Pulse Secure Access
Initial Configuration User Records Synchronization
This document explains how to set up User records synchronization between different clusters or stand-alone units.

Active/Passive, Active/Active, Stand-alone nodes.

First cluster: Active 172.22.149.112 passive 172.22.149.111
Second cluster: Active 172.22.149.143 Passive 172.22.149.140

Configuration Steps:

Step 1:
Configure the first node 172.22.149.112.
Enable User Record Synchronization Under the Auth Server, choose Logical Auth Server Name. (This name should be the same across all nodes).

![User Record Synchronization](image)

Under the Authentication/Authorization Servers you should see the User Record Synchronization enabled with the Logical Auth Server Name.

<table>
<thead>
<tr>
<th>Authentication/Authorization Servers</th>
<th>Type</th>
<th>User Record Synchronization</th>
<th>Logical Auth Server Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators</td>
<td>Local Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory / Windows NT</td>
<td>✓</td>
<td>sync1</td>
</tr>
<tr>
<td>Local AD</td>
<td>Active Directory / Windows NT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Local</td>
<td>Local Authentication</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Step 2:

1. System Configuration >> User Record Synchronization Enable User Record Synchronization
2. Node name. (Example Node112)
3. Shared Secret (please note all nodes share the same secret).
4. Node Function Choose Client and Server
Step 3:

5. This Client add the IP address of the node to enable the creation of the Database.

Step 4:

6. This Server add the IP Address of the entire peer Servers allowing Changes to user records on this server to be copied to the peer servers configured here.

7. Client Nodes enable the IP address of all the client nodes which are allowed to access this server. This act as an access list (ACL) to allow the other unit access to this server data base.
Second node (The passive node) 172.22.149.111.

Step 1:
Enable User Record Synchronization Under the Auth Server, choose Logical Auth Server Name. (This name should be the same across all nodes).
Step 2:

1. System Configuration >> User Record Synchronization Enable User Record Synchronization
2. Node name. (Example Node111)
3. Shared Secret (please note All nodes share the same secret).
4. Node Function Choose Client and Server
Step 3:

5. This Client add the IP address of the node to enable the creation of the Database.

![User Record Synchronization](image)

Step 4:

6. This Server add the IP Address of the entire peer Servers allowing Changes to user records on this server to be copied to the peer servers configured here.

7. Client Nodes enable the IP address of all the client nodes which are allowed to access this server. This act as an access list (ACL) to allow the other unit access to this server data base.
Second cluster Active 172.22.149.140 Passive 172.22.149.143

Configure the 3rd Node 172.22.149.140.

Step 1:
Enable User Record Synchronization Under the Auth Server, choose Logical Auth Server Name. (This name should be the same across all nodes).
Step 2:

1. System Configuration >> User Record Synchronization Enable User Record Synchronization
2. Node name. (Example Node140)
3. Shared Secret (please note All nodes share the same secret).

Step 3:

5. This Client add the IP address of the node to enable the creation of the Database.
Step 4:

6. This Server add the IP Address of the entire peer Servers allowing Changes to user records on this server to be copied to the peer servers configured here.

7. Client Nodes enable the IP address of all the client nodes which are allowed to access this server. This act as an access list (ACL) to allow the other unit access to this server data base.
Configure the 4th Node 172.22.149.143.

**Step 1:**

Enable User Record Synchroniztion Under the Auth Server, choose Logical Auth Server Name. (This name should be the same across all nodes).
Step 2:

1. System Configuration >> User Record Synchronization Enable User Record Synchronization

2. Node name, (Example Node143)

3. Shared Secret (please note All nodes share the same secret).

4. Node Function Choose Client and Server

Step 3:

5. This Client add the IP address of the node to enable the creation of the Database.
Step 4:

6. This Server add the IP Address of the entire peer Servers allowing Changes to user records on this server to be copied to the peer servers configured here.

7. Client Nodes enable the IP address of all the client nodes which are allowed to access this server. This act as an access list (ACL) to allow the other unit access to this server data base.
### User Record Synchronization

Changes to user records received by this server will be copied to the peer servers.

#### Peer Servers

<table>
<thead>
<tr>
<th>Server Node Name</th>
<th>Internal Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node143</td>
<td>172.22.149.143</td>
</tr>
<tr>
<td>Node140</td>
<td>172.22.149.140</td>
</tr>
<tr>
<td>node111</td>
<td>172.22.149.111</td>
</tr>
<tr>
<td>node112</td>
<td>172.22.149.112</td>
</tr>
</tbody>
</table>

#### Client Nodes

Configure all the client nodes which are allowed to access this server.

<table>
<thead>
<tr>
<th>Client Node Name</th>
<th>Internal Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node140</td>
<td>172.22.149.140</td>
</tr>
<tr>
<td>node111</td>
<td>172.22.149.111</td>
</tr>
<tr>
<td>node112</td>
<td>172.22.149.112</td>
</tr>
</tbody>
</table>