

Authentication Sync to Trust Zone

<https://campus.barracuda.com/doc/28361/>

If you are running multiple authentication services on a Control Center, it can sometimes be useful to sync the authentication data of the users between these services.

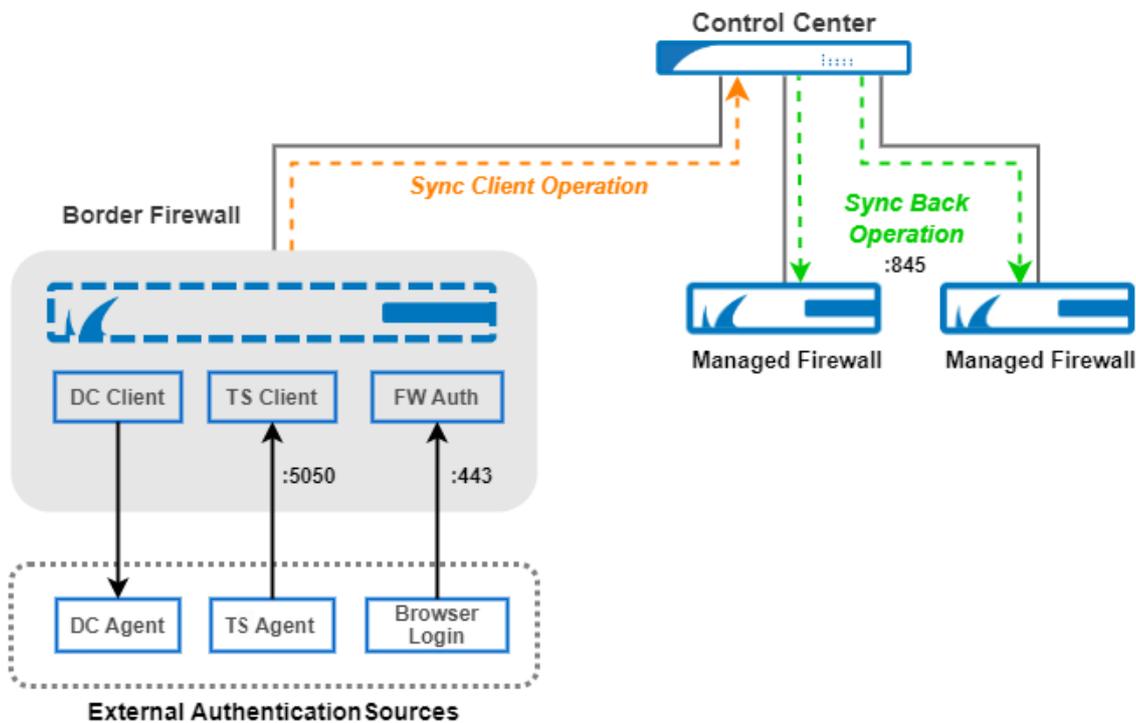
Authentication Sync to Trust Zone is a CC feature that distributes all authenticated user entries across managed boxes in the same non-policy trust zone. The service is supplied with data from the DC Agent, the TS Agent, or the firewall authentication service. The information from these services is collected on the box side and is interpreted accordingly before it is sent to the Control Center in a sync client operation. This central authentication data is then distributed to all boxes that are registered in the same authentication sync zone. This sync-back operation gets triggered every 10 seconds by default.

If a single box goes down during the distribution of the authentication data, the Control Center holds back every authentication entry to do a full sync after the box gets available again.

The Authentication Sync to Trust Zone service must be configured on the Control Center. The configuration requires switching to the advanced mode in Firewall Admin.

NOTE!

The Authentication Sync to Trust Zone is a stand-alone service and is not related to NAC/VPN policy trust zones or to any ranges or clusters.



Authentication Sync Zones on HA Pairs

If you are running an authentication sync zone on an HA pair, you must consider that the authentication database gets overwritten every second. This can lead to unexpected issues. To avoid these issues, you must ensure that certain settings are configured correctly for high availability-related policies, especially on firewalls that have been updated only over a longer period (see below).

How to Create a New Authentication Sync Zone

Creating a new authentication trust zone is not tied to a dedicated node in the configuration tree. To create a new authentication sync zone, simply add a single entry to a specific managed firewall. This entry will then be offered for selection on any other managed firewall.

Step 1. Create a New Authentication Sync Zone

This step is required only if an appropriate zone does not yet exist. It is therefore recommended to check the list of present sync zones for the Authentication Sync Zone before you perform the following steps.

1. Log into your Control Center.
2. Go to **CONFIGURATION > Configuration Tree > Multi-Range > your range > your cluster > Boxes > your_box > Properties**.

3. In the left menu, click **Operational**.
4. Click **Lock**.
5. In the section **Operational Settings**, for **Authentication Sync Zone**, click **Other**.
6. The drop-down menu item will be replaced with an edit field.
7. Enter the name you have chosen for your authentication sync zone into the edit field.

Operational Settings	
Disable Box	no
CC Activates Network	no
Detect Appl. Model Mismatch	no
ART Network Activation	yes
HA Firmware Update	Manual Failover
Disable Barracuda Activation	No
Collect Statistics	like-cluster
Went Operational	
Box->CC Access	Standard-CC-IP
Explicit CC IP	
CC->Box Access	Standard-Box-IP
Explicit Box IP	
Authentication Sync Zone	MyAuthSyncZone <input checked="" type="checkbox"/> Other
PAR File Retrieval Shared Key	

8. Click **Send Changes**.
9. Click **Activate**.

After creating a new authentication sync zone, the zone will be available for selection on other boxes.

Step 2. Add Another Firewall to an Existing Authentication Sync Trust Zone

You can now add another firewall to feed that sync zone with authentication data. For this, perform the following steps:

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > your range > your cluster > Boxes > your_box > Properties**.
2. In the left menu, click **Operational**.
3. Click **Lock**.
4. For **Authentication Sync Zone**, select the required sync zone from the list in the menu.

Operational Settings	
Disable Box	no
CC Activates Network	no
Detect Appl. Model Mismatch	no
ART Network Activation	yes
HA Firmware Update	Manual Failover
Disable Barracuda Activation	No
Collect Statistics	like-cluster
Went Operational	
Box->CC Access	Standard-CC-IP
Explicit CC IP	
CC->Box Access	Standard-Box-IP
Explicit Box IP	
Authentication Sync Zone	<input type="checkbox"/> Other
PAR File Retrieval Shared Key	Non-Policy-Trustzone - MyAuthSyncZone

5. Click **Send Changes**.
6. Click **Activate**.

Step 3. Provide Authentication Sync Data to the Authentication Sync Zone

You can now add the following authentication services to feed the authentication sync zone with data.

- **MSAD DC Clients** – For more information on how to configure MSAD DC Clients, see [How to Configure MSAD Authentication](#).
- **TS Agent Authentication** – For more information on how to configure TS Agent Authentication, see [How to Configure TS Agent Authentication](#).
- **Firewall Authentication** – For more information on how to configure Firewall Authentication, see [Firewall Authentication and Guest Access](#).
- Global/Non-Policy Trustzones

Ensure that you are running Firewall Admin in **Advanced Mode!**

Option #1: Add an MSAD Client Authentication Service

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > your range > your cluster > Boxes > your_box > Infrastructure Service**.
2. In the left menu, select **MSAD DC Client**.
3. Select the check box for **Authentication Sync to Trustzone**.

MSAD DC Client Settings

Activate Scheme

Auto Logout After [h]

Debug Log

Server Setting

Name	IP Address	TCP Port
SERV01	10.17.94.31	5049

Group Filter Patterns

Authentication Sync to Trustzone

This scheme is used for transparent user authentication against a MSAD.

4. Click **Send Changes**.
5. Click **Activate**.

Option #2: Add a TS Agent Authentication Service

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > your range > your cluster > Boxes > your_box > Infrastructure Service**.
2. In the left menu, select **TS Agent Authentication**.
3. Select the check box for **Authentication Sync to Trustzone**.

TS Agent Authentication Settings

Activate Scheme	Yes	<input type="checkbox"/>
Auto Logout After [d]	0	<input type="checkbox"/>
Always use SSL	Yes	<input type="checkbox"/>
Strip Domain Name	No	<input type="checkbox"/>
Authentication Sync to Trustzone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Log Level	Informational	<input type="checkbox"/>
TS Agent Certificates	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

Certificate Subject Altern... Certificate File

4. Click **Send Changes**.
5. Click **Activate**.

Option #3: Add Firewall Authentication

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > your range > your cluster > Boxes > your_box > Assigned Services > Firewall > Firewall Forwarding Settings**.
2. In the left menu, select **Authentication**.
3. Select the check box for **Authentication Sync to Trustzone**.

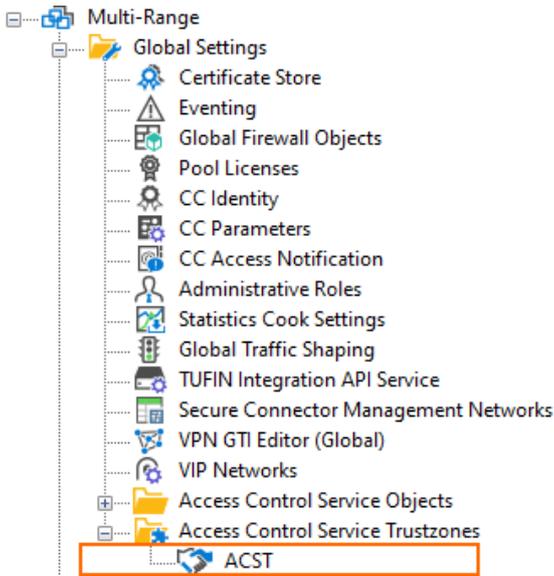
Metadirectory Authentication

Authentication Scheme	MS Active Directory	<input type="checkbox"/> Other
Listen IP	127.0.0.1	<input type="checkbox"/>
Request Timeout	10	<input type="checkbox"/>
User ACL Policy	deny-explicit	<input type="checkbox"/>
User ACL	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Group ACL Policy	deny-explicit	<input type="checkbox"/>
Group ACL	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Authentication Sync to Trustzone	<input checked="" type="checkbox"/>	<input type="checkbox"/>

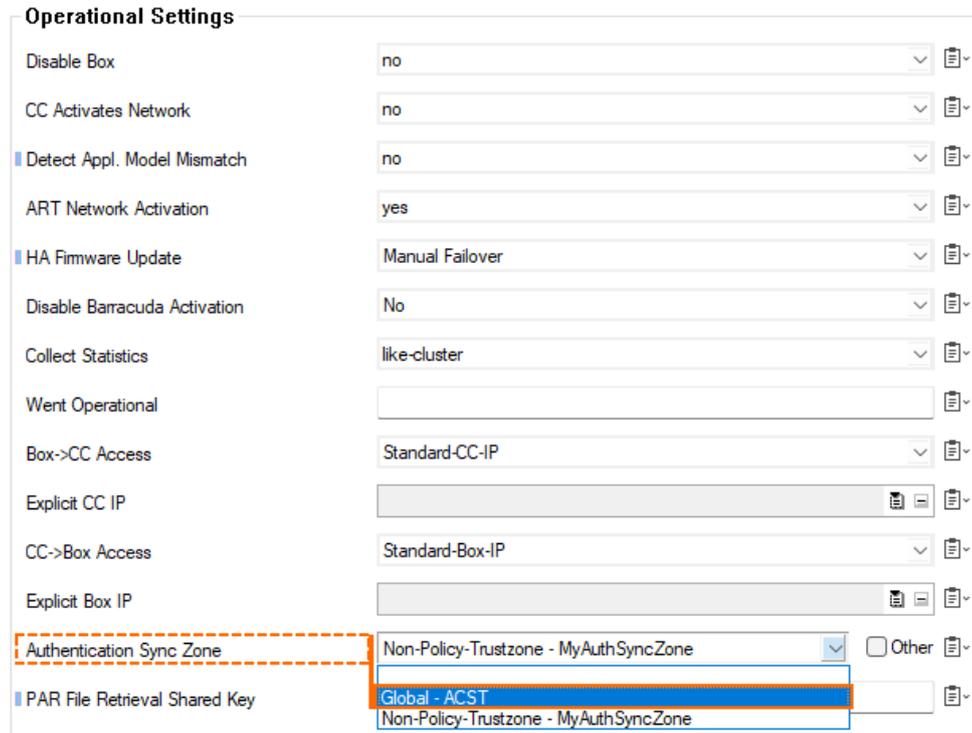
4. Click **Send Changes**.
5. Click **Activate**.

Option #4: Add a Global Trustzone

If you have configured a global **Access Control Service Trustzone**, this trusted zone will be displayed in the configuration at **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > Access Control Service Trustzones**:



This zone will also be available for selection in the menu list of authentication trust zones:



Additional Settings to Ensure for HA Pairs

Because in an HA setup, the active box overwrites the authentication database every second, running an authentication sync zone can lead to issues. To avoid these issues, ensure that the configuration for high availability-related policies matches the settings of the following screenshot.

Note that you must enable the advanced mode in Firewall Admin to access the related configuration section.

1. Log into your HA primary firewall.
2. Go to **CONFIGURATION > Configuration Tree > your_primary_firewall > Infrastructure Services > General Firewall Configuration**.
3. In the left menu, select **Operational**.
4. In the main view, scroll down to the last configuration section **High Availability Related Policies**.
5. Ensure that the value for **Enable Authentication Sync** is set to **Auto**.

High Availability Related Policies	
Allow Active-Active Mode	No
Enable Session Sync	Yes
Enable Authentication Sync	Auto
Log Synced Sessions	Yes

How to Remove an Authentication Sync Trust Zone

Removing an Authentication Sync Trust Zone is done by unregistering it. Perform the following steps to unregister from a sync zone:

1. Log into your Control Center.
2. Go to **CONFIGURATION > Configuration Tree > Multi-Range > your_range > your_cluster > Boxes > your_first_box > Properties**.
3. In the left menu, click **Operational**.
4. Click **Lock**.
5. Click the menu list for **Authentication Sync Zone**.
6. Select the first, empty line in the list.

Operational Settings

Disable Box	no	<input type="checkbox"/>
CC Activates Network	no	<input type="checkbox"/>
Detect Appl. Model Mismatch	no	<input type="checkbox"/>
ART Network Activation	yes	<input type="checkbox"/>
HA Firmware Update	Manual Failover	<input type="checkbox"/>
Disable Barracuda Activation	No	<input type="checkbox"/>
Collect Statistics	like-cluster	<input type="checkbox"/>
Went Operational		<input type="checkbox"/>
Box->CC Access	Standard-CC-IP	<input type="checkbox"/>
Explicit CC IP		<input type="checkbox"/>
CC->Box Access	Standard-Box-IP	<input type="checkbox"/>
Explicit Box IP		<input type="checkbox"/>
Authentication Sync Zone	<input type="text" value="Non-Policy-Trustzone - MyAuthSyncZone"/> <input type="checkbox"/> Other	<input type="checkbox"/>
PAR File Retrieval Shared Key	<input type="text" value="Global - ACST"/> <input type="text" value="Non-Policy-Trustzone - MyAuthSyncZone"/>	<input type="checkbox"/>

NOTE

Adding a firewall to an existing Authentication Sync Trust Zone links it to the zone you have created at the beginning.

When unregistering from such a sync zone, the existing last link that refers to the sync zone will cause the initial sync zone entry to be removed from the list.

Figures

1. authentication_synczone_diagram.png
2. auth_sync_zone_enter_sync_zone_name.png
3. auth_sync_zone_select_auth_sync_zone.png
4. auth_sync_zone_MSAD_DC_client_activate_sync_to_zone.png
5. auth_sync_zone_TS_agent_activate_sync_to_zone.png
6. auth_sync_zone_FW_auth_activate_sync_to_zone.png
7. auth_sync_zone_add_global_non_policy_trustzone.png
8. auth_sync_zone_select_global_ACST.png
9. auth_sync_zone_settings_for_HA_pairs.png
10. auth_sync_zone_remove_an_auth_sync_zone.png

© Barracuda Networks Inc., 2025 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.