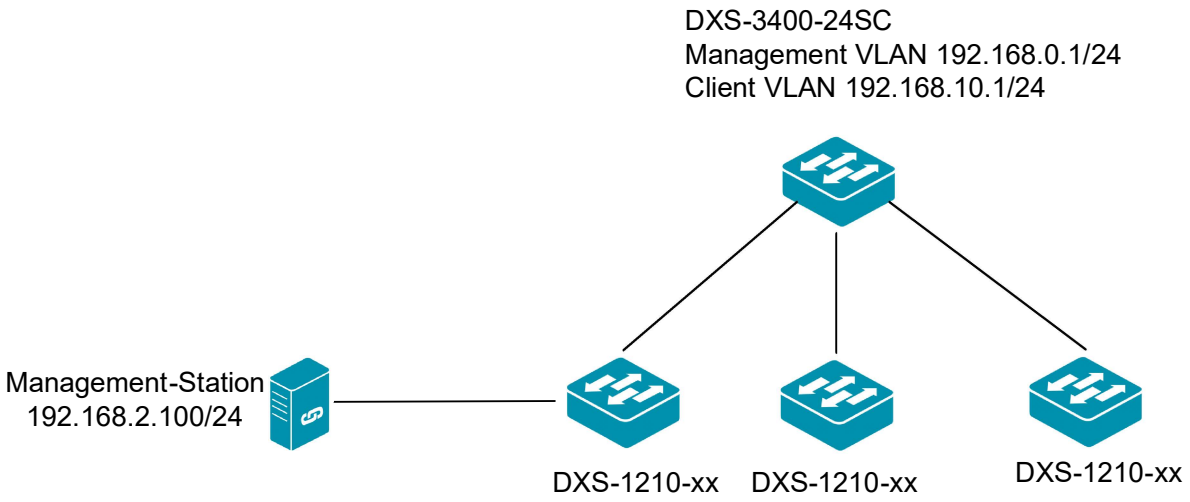
HowTo: Trusted Host ACL on DXS-3400 & DXS-1210

[Requirements]

1. DXS-3400-xx or DXS-1210-xx with latest firmware

[Topologie/Scenario]

There is a switched and routed company network.
Management-Access to the switches should only be allowed from Management VLAN Subnet 192.168.0.0/24 and from dedicated Management Host in Client VLAN 192.168.2.100.

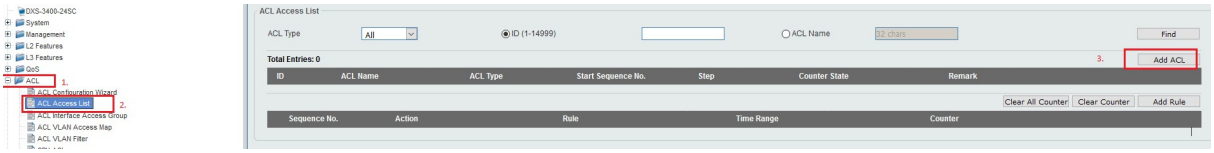


[preparation]

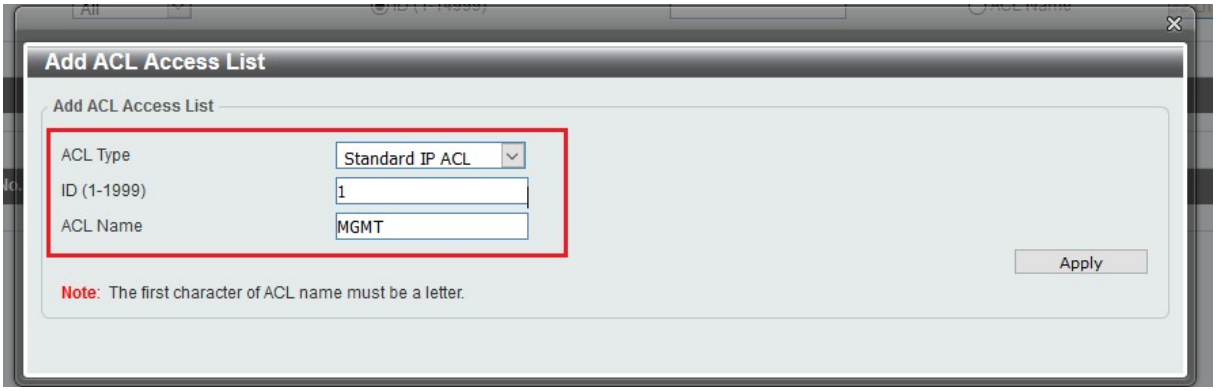
- ⇨ All VLANs and Routing is completely configured
- ⇨ Ensure to test the ACL f.e. with ping (icmp) before finally assigning it

[Creating the ACL]

1. navigate into the Sub-Menu “ACL > ACL Access List”
2. create a new ACL by “Add ACL”

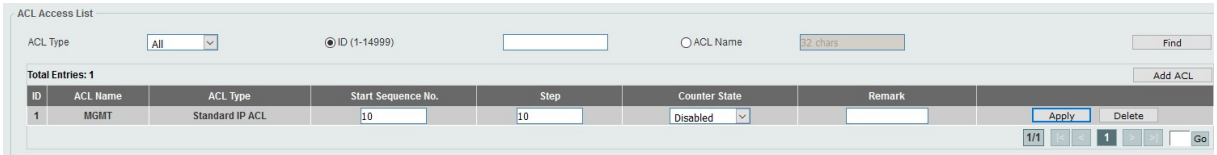


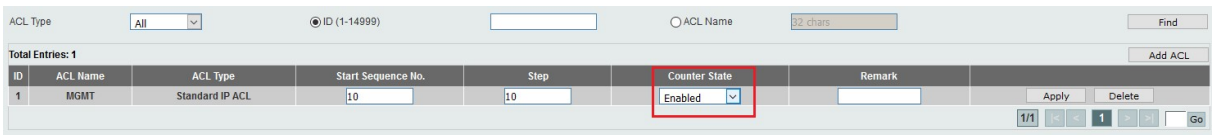
3. keep the Standard IP ACL
4. define the ACL ID
5. define the ACL Name
6. with APPLY you confirm your settings



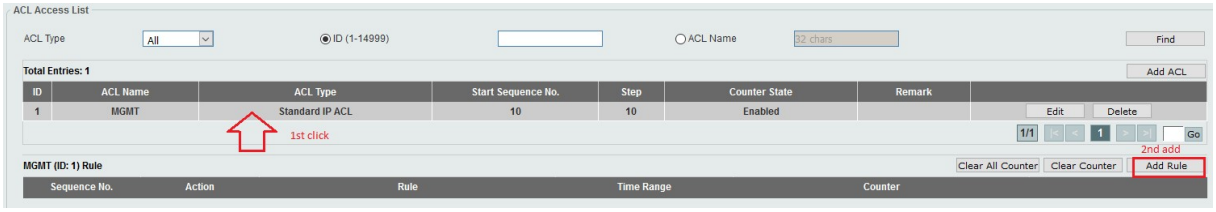
7. After confirming your settings, you’ll see the ACL

8. By pressing “EDIT” you can change the Sequence, Step and the Counter State
   - By default, you don’t need to change here anything, however you might want to enable the Counter only, so change this to “Enable”

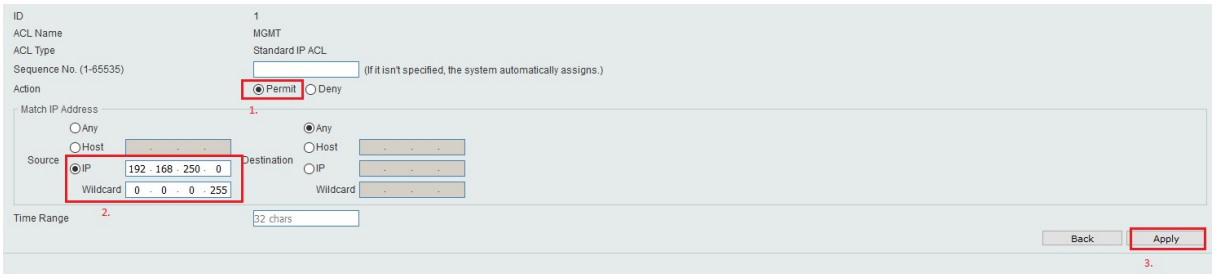


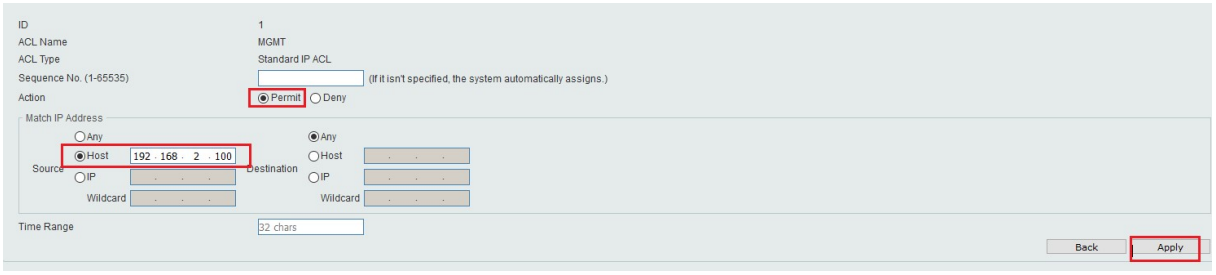


9. Klick anywhere into the defined ACL to select/specify it
    - Afterward you are able to create Rules for this ACL



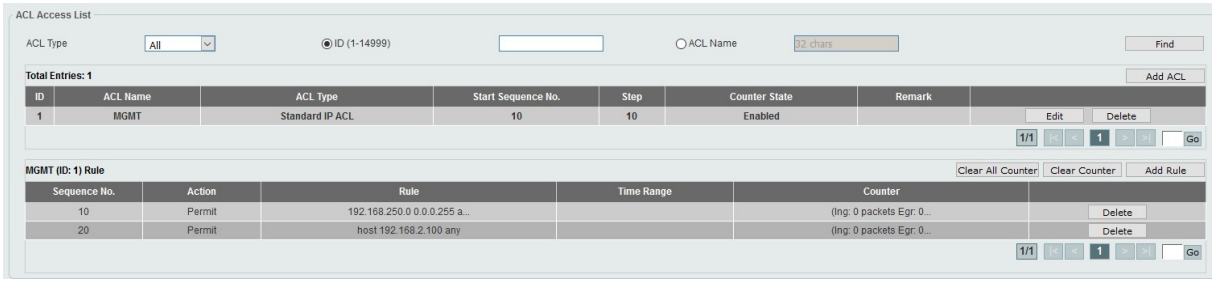
10. Now you can manually create Rules
    - Create a PERMIT rule for Management Subnet
        - be careful of the Subnet-Mask as a Wildcard
    - repeat the Rule-creation for all your Networks and Hosts



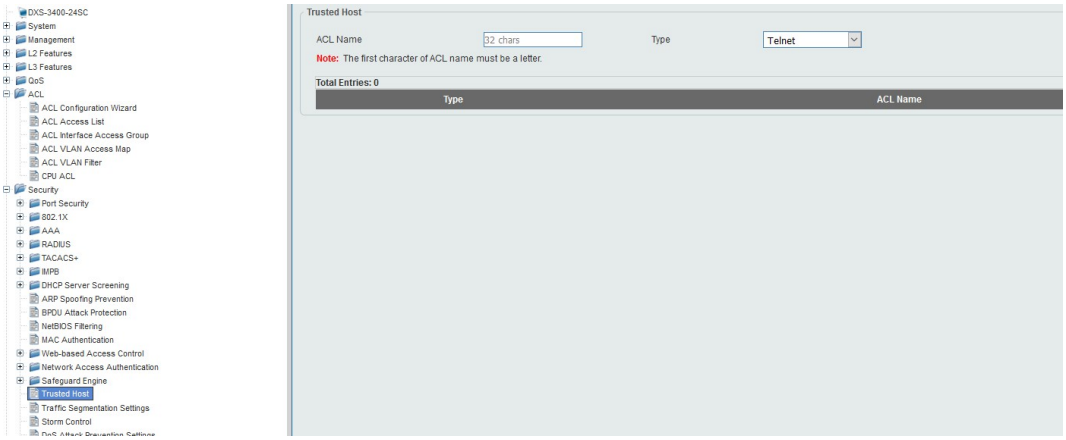


After you pressed “Apply” you can directly create a new Rule or Leave the Rule Creation by pressing “Back” now

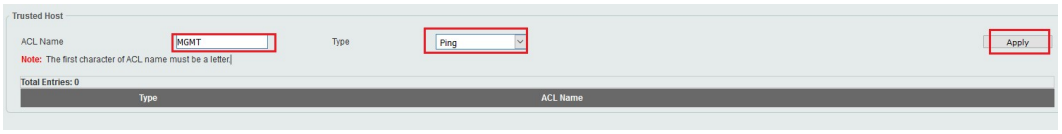
11. after finishing the ACL Rule Creation, you can check your settings again by selecting the ACL



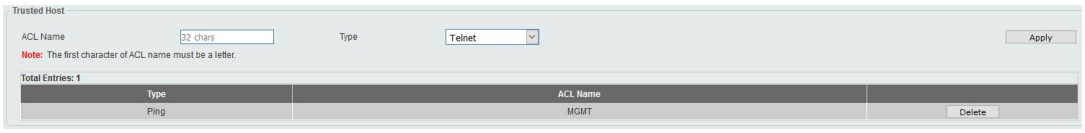
12. Navigate now to “Security > Trusted Host”



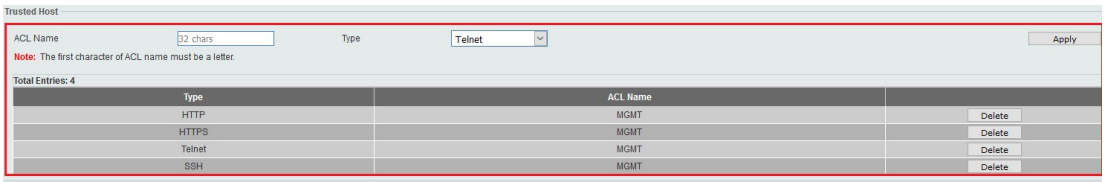
13. Here you now can assign the created ACL “MGMT” to different services
    - For Testing purposes, you should start with “PING”, to ensure you still can ping the device after assigning the ACL, otherwise you have to restart the Switch (or connect by console) and delete/reverse the ACL definitions.



14. After pressing APPLY now, the ACL immediately becomes active and should still grant/block your defined Access.



15. Now add all the Services you want to secure
16. In our example we want HTTP/HTTPS/Console and Telnet access only be available to the Hosts/Subnet defined in the ACL



If you now still have access to the device, the ACL is working correctly and you should save the configuration now.