

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
- \Rightarrow 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

| CL Type | Standard IP ACL | |
|------------|-----------------|-------|
| D (1-1999) | | |
| CL Name | MGMT | |
| | | Apply |

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

| NUL AUUSS L | | | | | | | |
|---------------|----------|-----------------|--------------------|------|---------------------|--------|------------------|
| ACL Type | All | ♥ ID (1-14999) | | | O ACL Name 32 chars | | Find |
| Total Entries | s: 1 | | | | | | Add ACL |
| ID | ACL Name | ACL Type | Start Sequence No. | Step | Counter State | Remark | |
| 1 | MGMT | Standard IP ACL | 10 | 10 | Disabled | | Edit Delete |
| | | | | | | | 1/1 < < 1 > > Go |

- 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"

| ACL Acce | ess List | | | | | | |
|-------------|-----------|-----------------|--------------------|------|---------------|----------|-------------------|
| ACL Typ | pe | All | ID (1-14999) | | O ACL Name | 32 chars | Find |
| Total En | ntries: 1 | | | | | | Add ACL |
| ID | ACL Name | ACL Type | Start Sequence No. | Step | Counter State | Remark | |
| 1 | MGMT | Standard IP ACL | 10 | 10 | Disabled 🖂 | | Apply Delete |
| | | | | | | | 1/1 < < 1 > > G |
| | | | | | | | |
| CL Type | | All | ID (1-14999) | | O ACL Name | 32 chars | Find |
| otal Entrie | s: 1 | | | | | | Add ACL |
| D A | ACL Name | ACL Type | Start Sequence No. | Step | Counter State | Remark | |
| 1 | MGMT | Standard IP ACL | 10 | 10 | Enabled 🔽 | | Apply Delete |
| | | | | | | | 1/1 K < 1 > > Go |



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

| ACL Access ACL Type | List | ✓ ● ID (1-145) | 99) | | O ACL Name | 32 chars | | Find |
|------------------------|-------------|-----------------|-----------|----------------|-------------|----------|--------|---------------------------------------|
| Total Entrie | es: 1 | | | | | | | Add A |
| ID | ACL Name | ACL Type | Start Seq | uence No. Step | Counter Sta | te | Remark | |
| 1 | MGMT | Standard IP ACL | 1 | 0 10 | Enabled | | | Edit Delete |
| | | 1st click | | | | | | 1/1 < < 1 > > 2nd ac |
| MGMT (ID: | 1) Rule | | | | | | [| Clear All Counter Clear Counter Add R |
| Sequ | ience No. 💋 | Action | Rule | Time Ra | nge | Coun | ter | |

10. Now you can manually create Rules

- Create a PERMIT rule for Management Subnet
 - be careful of the Subnet-Mask as a Wildcard
- o repeat the Rule-creation for all your Networks and Hosts

| ID | 1 |
|-------------------------------|--|
| ACL Name | MGMT |
| ACL Type | Standard IP ACL |
| Sequence No. (1-65535) | (If it isn't specified, the system automatically assigns.) |
| Action | Ceny |
| Match IP Address | 1. |
| OAny | |
| OHost | OHost |
| Source IP 192 - 168 - 250 - 0 | Destination OIP |
| Wildcard 0 - 0 - 0 - 255 | Wildcard |
| Time Range 2. | 32 chars |
| | Back Apply |
| | 3. |
| | |

| ID | 1 |
|--------------------------|--|
| ACL Name | MGMT |
| ACL Type | Standard IP ACL |
| Sequence No. (1-65535) | (If it isn't specified, the system automatically assigns.) |
| Action | Permit Deny |
| Match IP Address | |
| OAny | |
| Host 192 · 168 · 2 · 100 | OHost |
| Source OIP | estination of the second secon |
| Wildcard | Wildcard |
| Time Range | 22 chars |
| | Back Apply |
| | |

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

| CL Type | All | ID (1-14999) | | | O ACL Name 32 chars | | Find |
|------------------|----------|--------------------|--------------------|------------|---------------------|---------------------|--|
| otal Entries: 1 | | | | | | | Add ACL |
| ID ACL Nam | e | ACL Type | Start Sequence No. | Step | Counter State | Remark | |
| 1 MGMT | | Standard IP ACL | 10 | 10 | Enabled | | Edit Delete |
| | | | | | | | 1/1 < < 1 > > |
| GMT (ID: 1) Rule | | | | | | | Clear All Counter Clear Counter Add Rule |
| Sequence No. | Action | Rule | | Time Range | 9 | Counter | |
| | Permit | 192.168.250.0 0.0. | 0.255 a | | (Ing | g: O packets Egr: 0 | Delete |
| 10 | 1 errint | | | | | 2: 0 packets Egr: 0 | Delete |



12. Navigate now to "Security > Trusted Host"

| DXS-3400-24SC | / Trusted Host |
|---------------------------------|---|
| I System | |
| 🗉 📁 Management | ACL Name 32 chars Type Telnet |
| 1 C2 Features | |
| E C3 Features | Note: The first character of ACL name must be a letter. |
| 🕀 📁 QoS | Total Entries: 0 |
| E DACL | |
| ACL Configuration Wizard | Type ACL Name |
| ACL Access List | |
| ACL Interface Access Group | |
| ACL VLAN Access Map | |
| ACL VLAN Filter | |
| CPU ACL | |
| E Decurity | |
| Port Security | |
| 🕀 📁 802.1X | |
| 🗉 📁 AAA | |
| 🟵 📁 RADIUS | |
| E TACACS+ | |
| 🕑 📁 IMPB | |
| DHCP Server Screening | |
| ARP Spoofing Prevention | |
| BPDU Attack Protection | |
| NetBIOS Filtering | |
| MAC Authentication | |
| Web-based Access Control | |
| E Provide Access Authentication | |
| 🗉 🃁 Safeguard Engine | |
| Trusted Host | |
| Traffic Segmentation Settings | |
| - 📄 Storm Control | |
| Bos Attack Drevention Sattinge | |
| | |

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.

| Trusted Host | | |
|---|-----------|-------|
| ACL Name MGMT | Type Ping | Apply |
| Note: The first character of ACL name must be a letter. | | |
| | | |
| Total Entries: 0 | | |
| Total Entries: 0 Type | ACL Name | |

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

| ACL Name 32 chars | Туре | Teinet | Apply |
|---|------|----------|--------|
| Note: The first character of ACL name must be a letter. | | | |
| Total Entries: 1 | | | |
| Туре | | ACL Name | |
| Ping | | MGMT | Delete |

- 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

| Trusted Host | | | | | | |
|---|----------|--------|--|--|--|--|
| ACL Name 32 chars Type | Telnet | Apply | | | | |
| Note: The first character of ACL name must be a letter. | | | | | | |
| Total Entries: 4 | | | | | | |
| Туре | ACL Name | | | | | |
| HTTP | MGMT | Delete | | | | |
| HTTPS | MGMT | Delete | | | | |
| Telnet | MGMT | Delete | | | | |
| SSH | MGMT | Delete | | | | |

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

| Sive - XTools - | | 🙎 Lopped in as: Administrator, 👰 Lo |
|-------------------------------|--|-------------------------------------|
| Save Configuration 2. | figuration | |
| | Save Configuration File Path C:/config.cfg | Apply |
| E 2 Features E 2 Features | | 3. |