

# **HowTo: Syslog Server**

## [Voraussetzungen]

1. DGS-1510-xx mit aktueller Firmware 1.21B05 und höher

## [Topologie]



## [Vorbereitung]

- ⇒ Der DGS-1510-xx hat im Auslieferungszustand die Standard IP 10.90.90.90/8
- ⇒ Bitte ändern Sie dies bei der Ersteinrichtung (Integration in Ihre bestehende Infrastruktur) des DGS-1510-xx in Ihrem Netzwerk, für die genaue Vorgehensweise der Einstellung der IP & des Benutzernamens schlagen Sie bitte im Handbuch (z.B.: <u>ftp://ftp.dlink.de/dgs/dgs-1510-20/documentation</u>) nach

## [Aufgabe]

Der DGS-1510-xx soll diverse Meldungen an einen externen Syslog-Server versenden.



#### 1. Anlegen eines "Diskriminators"

a. System -> System Log -> System Log Discriminator Settings

📲 Save 👻 🎇 Tools 👻 🐞 Wizard	🎱 Online Help 👻 English 💉	·				Logged in as: Ac	lministrator, <u>ശ</u> Logout
Fuzzy Search	System Log Discrimina	tor Settings					
DGS-1510-28P	Discriminator Log Settings						
System Information Settings	Discriminator Name	15 chars	]				
Peripheral Settings     Peripheral Settings     Peripheral Settings	Action	Drops V		□ PORT	STP		
E System Log			VOICE_VL				
System Log Discriminator Settings		JWAC	DHCPV6	STORM_CT	SSH		
System Log Server Settings			AAA				
System Attack Log     Ime and SNTP		DAI DOT1X	DP POE	SURVEILL BPDU_PRO	RADIUS		
Ime Range     Management		SAFEGUAR	CFG	FIRMWARE			
El 2 Features     El 2 Features     El 2 Features	Severity	0(Emergencies)	1(Alerts)	2(Critical)	3(Errors)		
E COS		4(Warnings)	5(Notifications)	6(Informational)	7(Debugging)		Apply
	Name	Action	Facil	ity List	Severity	Severity List	
monitoring     filler     Green							

b. Konfigurieren/Anlegen eines Discriminators

a. Discriminator Name = definiert den Namen Ihres Desriminators (frei wählbar, z.B. ALL)

b. Action = Includes / Excludes, definiert welche Events gemeldet oder nicht gemeldet werden sollen

c. Severity = Includes / Excludes, definiert welche Events mit welchem Schweregread (Severity) verarbeitet werden sollen d. Apply = Übernehmen der Einstellungen

📲 Save 🔻 🐒 Tools 🔻 📫 Wizard 🔹 Online Help 👻 English ~ 🤦 Logged in as: Administrator, ... 🧏 Logout System Log Discriminator Settings DGS-1510-28P Discriminator Log Settings System System Inform Discriminator Name ALL nation Setting Peripheral Settings Action Includes ~ ✓ PORT
 ✓ FDB
 ✓ PORTSEC SYS STACKING STP PoE
 System Log System Log
System Log Settings
System Log Discriminator St
System Log Discriminator St
System Log Server Settings
System Log
System Log
System Attack Log ACL
JWAC
CLI ✓ WAC ✓ SSH ✓ ERPS QOS ✓ DHCPV6 ✓ WEB SNMP DDM DAI DOT1X DEVICE
 RADIUS
 MAC AAA DoS System Artacl
System Artacl
Time and SNTP
Time and SNTP
Time Range
Time Range
Time Range
Time Construction
Time Constru BPDU\_PRO POE SAFEGUAR CFG FIRMWARE Includes ~ Severity O(Emergencie
 4(Warnings) ✓ 1(Alerts)
 ✓ 5(Notification 2(Critical) 6(Information ✓ 3(Errors)
 ✓ 7(Debugging) Apply 🖶 🚝 Security Cooling
 OAM
 Monitor Action Facility List Severity Severity List 🌒 Online Help 👻 English Save 👻 🎇 Tools 👻 🐝 Wizard ~ 🔵 Logged in as: Administrator, ... 🙋 Logout System Log Discrimin ator Settings DGS-1510-28P
 System
 System Information
 Peripheral Settings Discriminator Log Settings Discriminator Name 15 char rmation Settings Drops ~ Action Port Configuration PORT

FDB

PORTSEC

STORM\_CT... Port Configuration
 Port Configuration
 Port
 System Log
 System Log Settings
 System Log Settings
 System Log Setter Settings
 System Log Setter Settings
 System Log Setter Settings
 System Attack Log
 System Attack Log SYS STACKING STP LAC ACL JWAC WAC DHCPV6 ERPS WEB SNMP DoS DOT1X BPDU\_PRO. MAC POE Drops ~ Severity 1(Alerts) 5(Notifications) 2(Critical) 6(Informational 3(Errors) 0(Emergencies Apply 4(Warnings)

SYS, STACKING, PORT, ST.

0,1,2,3,4,5,6,7

Delete

Action



#### 2. Anlegen Syslog Server (Host) a. System -> System Log -> System Log Server Settings

Fuzzy Search	System Log Server Setti	ngs				
DOS-1510-28P     System Information Settings     System Information Settings     Peripheral Settings     Poice     System Log     System Log     System Log     System Log     System Log	Log Server () Host IPv4 Address UDP Port (1024-65535) Facility	514 23	<ul> <li>Image: A start of the start of</li></ul>	O Host IPv6 Address Severity Discriminator Name	2013::1 4(Warnings) 15 chars	Apply
System Log Server Schuper      System Xtack Log      System Xtack Log      Management      L S reatures      AcL      Socurity      OAM      Moning      Green	Total Entries: 0 Server IP	Severity	Facility	Discrim	inator Name	UDP Port

#### b. Konfigurieren/Anlegen eines Syslog Host (Server)

- a. IPv4/IPv6 Adresse = definiert die zu verwendende IP Adresse
- b. Severity = Includes / Excludes, definiert welche Events mit
- welchem Schweregread (Severity) verarbeitet werden sollen
- c. Discriminator Name = der unter Punkt 1 angelegte Discriminator
- d. Apply = Übernehmen der Einstellungen

📲 Save 👻 🌋 Tools 👻 📫 Wizard	Online Help    English	×			Logged in as: Administrator,	<u> Log</u> ou
Fuzzy Search	System Log Server Set	tings				
DGS-1510-28P	Log Server					
😑 🎾 System						
- 📄 System Information Settings	<ul> <li>Host IPv4 Address</li> </ul>	192 · 168 · 10 · 100	<ul> <li>Host IPv6 Address</li> </ul>	2013::1		
Peripheral Settings	UDP Port (1024-65535)	514	Severity	7(Debugging)		
Fort Configuration				-(		
🕀 📁 PoE	Facility	23 🗸	Discriminator Name	ALL		
E Distem Log					A	Apply
System Log Settings						
System Log Discriminator Settings	Total Entries: 0					
System Log Server Settings	Server ID	Severity Ea	cility Disc	riminator Name	LIDP Port	
System Log	Servern	July 14	Disci			
System Attack Log						
Ime and SNTP      The Dense						
Inne Range						
Fuzzy Search	System Log Server Set	tings				
i may ocurun						
DGS-1510-28P	Log Server					
System	C Liest IDud Address		C Linet IDvP Address	2012:1		
System Information Settings	Host IFV4 Address		Host IFV6 Address	20131		
Peripheral Settings	UDP Port (1024-65535)	514	Severity	4(Warnings)		
Port Configuration	Eacility	23	Discriminator Name	15 chars		
E Sustam Lon	T denty	23	Dischinitator Name	13 Gildia		
System Log					A	Apply
System Log Discriminator Settings	E LIE LE L					
System Log Server Settings	Total Entries: 1					
System Log	Server IP	Severity Fa	cility Disc	riminator Name	UDP Port	
System Attack Log	192.168.10.100	Debugging	23	ALL	514 E	elete
Ime and SNTP						
🔤 Time Range						
🗉 🎬 Management						
E I 2 Features						



### 3. Anpassen der System Log Settings

a. System -> System Log -> System Log Settings

💾 Save 🔻 🌋 Tools 🔻 🐠 Wizard	🌒 Online Help 👻 English 💽	×	🙎 Logged in as: Administrator, 💯 Logout
Fuzzy Search	System Log Settings		
DGS-1510-28P	Global State		
System Information Settings	Source Interface State Type	Enabled         V           VLAN         VID (1-4094)         1	Apply
Port Configuration     PoE     System Lon	Buffer Log Settings		
Ting System Log Settings	Buffer Log State	Enabled V	
System Log Server Settings	Discriminator Name	15 chars	
Gradin Autor Log     Time and SNTP     ST Time Range	Write Delay (0-65535)	300 sec 🗌 Infinite	Apply
Management     Management	Console Log Settings		
	Console Log State	Disabled	
<ul> <li>■ 200S</li> <li>■ 200S</li> <li>■ 200S</li> </ul>	Severity	4(Warnings)	
Security     Security	Discriminator Name	15 chars	Apply
Monitoring     Green			



- b. Konfigurieren des Buffer Log State
  - a. Enabled/Disabled = aktivieren/deaktivieren der Funktion
  - b. Severity = 0-7 definiert welche Events mit welchem Schweregread (Severity) verarbeitet werden sollen
  - c. Discriminator Name = der unter Punkt 1 angelegte Discriminator
  - d. Apply = Übernehmen der Einstellungen

#### 4. Speichern der Konfiguration

- a. Save -> Save Configuration
- b. File Path = vorgegebene Daten für die Konfigurationsdatei
- c. Apply = Übernehmen und Speichern

Save - XTools - Wizard	Online Help + English V	S Logged in as: Administrator, 👰 Logout
Fuzzy Search	Save Configuration	
□ DG5-1510-28P     □ DG5-1510-28P     □ DG5-1510-28P     □ DG5-1510-28P     □ DG 28     □ ACL     □ Security	Ete Path C/config.cfg	Apply



## TEST am Syslog-Server

Thtp Server Thtp Client DHCP server Syslog server Log viewer

text	from	date
<190>Jul 20 13:55:21 192.168.10.6 INFO: Configuration saved to flash by console (Username: admin)	192.168.10.6	20/07 13:55:22.705
<190>Jul 20 13:55:25 192.168.10.6 INFO: Port eth1/0/14 link down	192.168.10.6	20/07 13:55:26.730
<190>Jul 20 13:55:31 192.168.10.6 INFO: Port eth1/0/14 link up, 1000Mbps FULL duplex	192.168.10.6	20/07 13:55:32.751
<190>Jul 20 13:55:45 192.168.10.6 INFO: RADIUS server 192.168.10.100 assigned VID: 2 to port E	192.168.10.6	20/07 13:55:46.791
<190>Jul 20 13:55:45 192.168.10.6 INFO: MAC-based Access Control host login success (MAC: 00	192.168.10.6	20/07 13:55:46.791