

D-Link® Technical Support Setup Procedure

FAQ: How to configure DMZ

Release date: 9/07/2015

Model Support: DSL-2877AL

H/W: A1 , A2

S/W: 1.00.10TH

FAQ : How to configure DMZ

การตั้งค่า DMZ สามารถทำได้อย่างไร

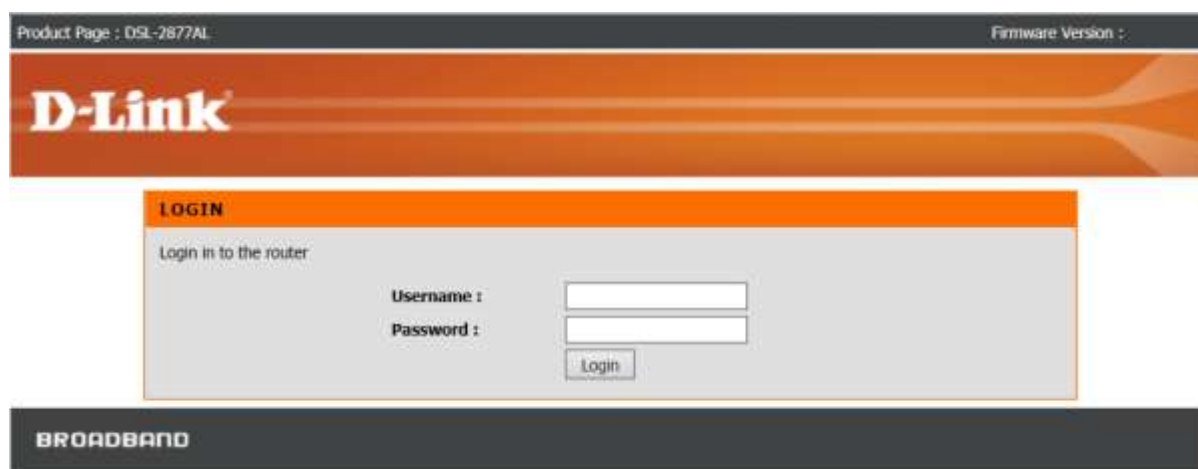
DMZ ควรทำเฉพาะเมื่อคุณมีอุปกรณ์ที่ไม่สามารถทำงานผ่านการตั้งค่าจากด้านหลังเราเตอร์ได้

Note: ในการตั้งค่า DMZ (Demilitarized Zone) นั้น คุณจะอนุญาตให้เราเตอร์ทำการ forward ทราฟฟิกในทุก ๆ กรณีจากอินเทอร์เน็ตไปยังอุปกรณ์ที่ระบุไว้ เปรียบเสมือนกับการปิดการทำงานของ firewall นั้นจะทำให้ อุปกรณ์ของคุณอยู่ในภาวะเสี่ยง ดังนั้นการเลือกทำในลักษณะนี้ให้ทำเป็นวิธีการสุดท้าย

ขั้นตอนที่ 1 : เปิดเว็บเบราว์เซอร์ของคุณ แล้วพิมพ์ <http://192.168.1.1> ในช่องของ Address Bar



ชื่อผู้ใช้งานที่มาจากโรงงานคือ admin แล้วใส่รหัสผ่านของคุณ ในกรณีรหัสผ่านไม่ได้มีการเปลี่ยนแปลง ให้ใช้ค่าที่มาจากโรงงานเป็น admin แล้วคลิก Login



ขั้นตอนที่ 2 : คลิกบนแท็บของ Advanced ที่อยู่ทางด้านบนแล้วคลิก DMZ จากเมนูที่อยู่ทางด้านซ้ายมือ

The screenshot shows the 'ADVANCED' tab of the DSL-2877AL router's web interface. The left sidebar contains a menu with 'DMZ' highlighted by a red arrow. The main content area is titled 'DMZ (EXPOSED HOST)' and includes a description of DMZ, a note about packet forwarding, and a 'DMZ (EXPOSED HOST) SETTINGS' section. The settings section includes options to enable or disable DMZ, select an interface (PVC0), enter an IP address, and set a time range (Begin time, End time, Begin day, End day). An 'Apply' button is at the bottom of the settings section. On the right, there is a 'Helpful Hints...' section with explanatory text about DMZ and a 'More...' link.

DSL-2877AL	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
Advanced Wireless	DMZ (EXPOSED HOST) DMZ (Exposed Host): From the Internet you can access to a client within the DMZ. This client is more vulnerable than the other clients in your LAN. It is strongly recommended to store any sensitive data behind the DMZ protected by a firewall. Note: Most of packets that from Internet will be forwarding to DMZ server except those packets that should forward to active virtual server, or access IAD's Telnet/FTP/remote administration http access service.				Helpful Hints... DMZ is short for Demilitarized Zone. A demilitarized zone is a network area (a subnetwork) that sits between your internal network and an external network, usually the Internet. The point of a DMZ is that connections from the internal and the external network to the DMZ are permitted, whereas connections from the DMZ are only permitted to the external network - hosts in the DMZ may not connect to the internal network. This allows the DMZ's hosts to provide services to the external network while protecting the internal network in case intruders compromise a host in the DMZ. For someone on the external network who wants to illegally connect to the internal network, the DMZ is a dead end. More...
Virtual Server	DMZ (EXPOSED HOST) SETTINGS				
Port Trigger	Enable DMZ : <input checked="" type="radio"/> Disable <input type="radio"/> Enable				
DMZ	Interface : PVC0				
Parental Control	IP Address : []				
IP & MAC Filtering	Time : <input checked="" type="radio"/> Disable <input type="radio"/> Enable				
DSL Line Settings	Begin time : 00 : 00				
Firewall	End time : 00 : 00				
DNS	Begin day : Sun				
Dynamic DNS	End day : Sun				
Network Tools	[Apply]				
Routing					
URL Redirect					
Internet Online					
Reboot					
Logout					

FAQ : How to configure DMZ

ขั้นตอนที่ 3 : คลิกเพื่อเปิดใช้งาน DMZ

- ตรวจสอบให้แน่ใจว่า ได้เลือกอินเตอร์เฟซของ WAN ที่เลือกไว้ ถูกต้องหรือไม่
- ใส่ค่า IP Address ของอุปกรณ์ที่ต้องการทำเป็น DMZ Host

The screenshot shows the web interface of a D-Link DSL-2877AL router. The navigation menu on the left includes: Advanced Wireless, Virtual Server, Port Trigger, DMZ, Parental Control, IP & MAC Filtering, DSL Line Settings, Firewall, DNS, Dynamic DNS, Network Tools, Routing, and URL Redirect. The main content area is titled 'DMZ (EXPOSED HOST)' and contains the following text:

DMZ (EXPOSED HOST)

DMZ (Exposed Host): From the Internet you can access to a client within the DMZ. This client is more vulnerable than the other clients in your LAN. It is strongly recommended to store any sensitive data behind the DMZ protected by a firewall.

Note: Most of packets that from Internet will be forwarding to DMZ server except those packets that should forward to active virtual server, or access IAD's Telnet/FTP/remote administration http access service.

DMZ (EXPOSED HOST) SETTINGS

Enable DMZ : Disable Enable

Interface : PVC0

IP Address : 192.168.1.2

Time : Disable Enable

Begin time : 00:00

End time : 00:00

Begin day : Sun

End day : Sun

Apply

Helpful Hints... DMZ is short for Demilitarized Zone. A demilitarized zone is a network area (a subnetwork) that sits between your internal network and an external network, usually the Internet. The point of a DMZ is that connections from the internal and the external network to the DMZ are permitted, whereas connections from the DMZ are only permitted to the external network - hosts in the DMZ may not connect to the internal network. This allows the DMZ's hosts to provide services to the external network while protecting the internal network in case intruders compromise a host in the DMZ. For someone on the external network who wants to illegally connect to the internal network, the DMZ is a dead end. More...

คลิก Apply

FAQ : How to configure DMZ

ตรวจสอบอุปกรณ์ที่ติดตั้ง (DMZ Client Device) ได้เปิดใช้งานและบันทึกใน DMZ Table เป็นที่เรียบร้อยแล้ว

Note: Most of packets that from Internet will be forwarding to DMZ server except those packets that should forward to active virtual server, or access IAD's Telnet/FTP/remote administration http access service.

DMZ (EXPOSED HOST) SETTINGS

Enable DMZ : Disable Enable

Interface : WAN

Service Num : 0

IP Address :

Time : Disable Enable

Begin time : 00 : 00

End time : 00 : 00

Begin day : Sun

End day : Sun

Apply

EXISTING DMZ

Status	Interface	IP Address	Time	Day	Remove	Edit
Active	PVC0	192.168.1.2			<input type="checkbox"/>	<input type="radio"/>

Remove Selected

network area (a subnetwork) that sits between your internal network and an external network, usually the Internet. The point of a DMZ is that connections from the internal and the external network to the DMZ are permitted, whereas connections from the DMZ are only permitted to the external network - hosts in the DMZ may not connect to the internal network. This allows the DMZ's hosts to provide services to the external network while protecting the internal network in case intruders compromise a host in the DMZ. For someone on the external network who wants to illegally connect to the internal network, the DMZ is a dead end.

More...

FAQ : How to configure DMZ

เลือก Remove แล้วคลิก Remove Selected เพื่อทำการลบรายการที่เลือกไว้ในตาราง DMZ เมื่อ IP Address นั้นมีการเปลี่ยนแปลง หรือไม่ได้ใช้แล้วเป็นเวลานาน

Enable DMZ : Disable Enable

Interface : WAN

Service Num : 0

IP Address :

Time : Disable Enable

Begin time : 00 : 00

End time : 00 : 00

Begin day : Sun

End day : Sun

Apply

Status	Interface	IP Address	Time	Day	Remove	Edit
Active	PVC0	192.168.1.2			<input checked="" type="checkbox"/>	<input type="checkbox"/>

Remove Selected

D-Link® Technical Support Setup Procedure

- **How do I enable the DMZ on my router?**

DMZ should only be used if you have a computer/device that cannot run Internet applications properly from behind the router.

Note: By enabling the DMZ (Demilitarized Zone) feature, you are allowing the router to forward all incoming traffic from the internet to the device specified, virtually disabling the routers "firewall protection". This may expose the device to a variety of security risks, so only use this option as a last resort.

Step 1: Open your Internet browser and enter `http://192.168.1.1` into the address bar.



Enter your login information. If you have not changed the default settings, the

- **Username** field is Admin and
- **Password** field should Admin. Click **Login**.



FAQ : How to configure DMZ

Step 2: Click on the **Advanced** Tab at the top and then click **DMZ** on the left side as shown.

The screenshot shows the D-Link DSL-2877AL web interface. At the top, there are tabs for SETUP, **ADVANCED**, MAINTENANCE, STATUS, and HELP. The left sidebar contains a menu with items: Advanced Wireless, Virtual Server, Port Trigger, **DMZ** (highlighted with a red arrow), Parental Control, IP & MAC Filtering, DSL Line Settings, Firewall, DNS, Dynamic DNS, Network Tools, Routing, and URL Redirect. Below the menu are 'Internet Online' status and 'Reboot' and 'Logout' buttons.

The main content area is titled **DMZ (EXPOSED HOST)** and contains the following text:

DMZ (Exposed Host): From the Internet you can access to a client within the DMZ. This client is more vulnerable than the other clients in your LAN. It is strongly recommended to store any sensitive data behind the DMZ protected by a firewall.

Note: Most of packets that from Internet will be forwarding to DMZ server except those packets that should forward to active virtual server, or access IAD's Telnet/FTP/remote administration http access service.

DMZ (EXPOSED HOST) SETTINGS

Enable DMZ : Disable Enable

Interface : PVC0

IP Address : [Empty text box]

Time : Disable Enable

Begin time : 00:00

End time : 00:00

Begin day : Sun

End day : Sun

[Apply button]

Helpful Hints..

DMZ is short for Demilitarized Zone.

A demilitarized zone is a network area (a subnetwork) that sits between your internal network and an external network, usually the Internet. The point of a DMZ is that connections from the internal and the external network to the DMZ are permitted, whereas connections from the DMZ are only permitted to the external network - hosts in the DMZ may not connect to the internal network. This allows the DMZ's hosts to provide services to the external network while protecting the internal network in case intruders compromise a host in the DMZ. For someone on the external network who wants to illegally connect to the internal network, the DMZ is a dead end.

[More...](#)

FAQ : How to configure DMZ

Step 3: Check Enable DMZ.

- Ensure the correct WAN **Interface** is selected.
- Enter the desired **DMZ Host IP Address** of the LAN device you want to place in the DMZ.

The screenshot shows the 'ADVANCED' tab of the DSL-2877AL web interface. The 'DMZ (EXPOSED HOST)' section is highlighted in orange. Below this, there is a descriptive paragraph about DMZ and a note. The 'DMZ (EXPOSED HOST) SETTINGS' section contains the following configuration:

- Enable DMZ: Disable Enable
- Interface: PVC0
- IP Address: 192.168.1.2
- Time: Disable Enable
- Begin time: 00:00
- End time: 00:00
- Begin day: Sun
- End day: Sun

A red arrow points to the 'Apply' button at the bottom of the settings section. On the right side, there is a 'Helpful Hints...' section with text explaining DMZ and a 'More...' link at the bottom.

Click **Apply** as shown.

FAQ : How to configure DMZ

Ensure DMZ Client Device Information is currently active and saved in the **DMZ** Table.

Note: Most of packets that from Internet will be forwarding to DMZ server except those packets that should forward to active virtual server, or access IAD's Telnet/FTP/remote administration http access service.

DMZ (EXPOSED HOST) SETTINGS

Enable DMZ : Disable Enable

Interface : WAN

Service Num : 0

IP Address :

Time : Disable Enable

Begin time : 00:00

End time : 00:00

Begin day : Sun

End day : Sun

Apply

EXISTING DMZ

Status	Interface	IP Address	Time	Day	Remove	Edit
Active	PVC0	192.168.1.2			<input type="checkbox"/>	<input type="radio"/>

Remove Selected

network area (a subnetwork) that sits between your internal network and an external network, usually the Internet. The point of a DMZ is that connections from the internal and the external network to the DMZ are permitted, whereas connections from the DMZ are only permitted to the external network - hosts in the DMZ may not connect to the internal network. This allows the DMZ's hosts to provide services to the external network while protecting the internal network in case intruders compromise a host in the DMZ. For someone on the external network who wants to illegally connect to the internal network, the DMZ is a dead end.

More...

Check on **Remove** and click **Remove Selected** to remove the selected rule in the **DMZ** Table when Local IP Address has been changed or is no longer available.

Enable DMZ : Disable Enable

Interface : WAN

Service Num : 0

IP Address :

Time : Disable Enable

Begin time : 00:00

End time : 00:00

Begin day : Sun

End day : Sun

Apply

EXISTING DMZ

Status	Interface	IP Address	Time	Day	Remove	Edit
Active	PVC0	192.168.1.2			<input checked="" type="checkbox"/>	<input type="radio"/>

Remove Selected

network area (a subnetwork) that sits between your internal network and the external network to the DMZ are permitted, whereas connections from the DMZ are only permitted to the external network - hosts in the DMZ may not connect to the internal network. This allows the DMZ's hosts to provide services to the external network while protecting the internal network in case intruders compromise a host in the DMZ. For someone on the external network who wants to illegally connect to the internal network, the DMZ is a dead end.

More...

FAQ : How to configure DMZ

ฝ่ายสนับสนุนทางด้านเทคนิค

Call Center หมายเลขโทรศัพท์ 02-6617997

ภาษาไทย : จันทร์ ถึง ศุกร์ เวลา 9.00 น. – 18.00 น.

Thai : Mon – Fri : Time 9.00 – 18.00.

ภาษาอังกฤษ : เสาร์ , อาทิตย์ , วันหยุดนชัตฤกษ์ และ วันธรรมดา หลัง 18.00 น.

English : Sat – Sun , Public Holiday and after 18.00 weekday.

Website : www.dlink.co.th

email: support@dlink.com.sg

Facebook : <http://www.facebook.com/DLinkThailandFans>

Nationwide D-Link Service Centres :

<p>Cham Issara Tower II 3rd Floor, Cham Issara Tower II 2922/138 New Perchburi Road Khwang Bangkapi, Khet Huay-Kwang, Bangkok 10320, Thailand</p> <p>Tel : +66 (0) 2308-2040 Fax : +66 (0) 2308-2024 Call Center : +66 (0) 2716-6669 Operating hours: Mondays till Friday 9am to 6pm</p>	<p>Pantip Plaza Branch 4th Fl. Pantip Plaza 604/2 Petchburi Road Room 439-440 Kwang Thanon Petchburi, Khet Ratchathewi Bangkok 10400, Thailand Tel : +66 (0) 2656 6037 Tel : +66 (0) 2656 6054 Fax : +66 (0) 2656 6042 Operating hours: Mondays till Sunday 10am to 7pm</p>	<p>Rayong Branch 217/24 Sukhumvit Road Tumbon Noen Phra, Amphoe Mueang Rayong Changwat Rayong 21000, Thailand</p> <p>Tel : +66 (0) 3880-0631-3 Fax : +66 (0) 3880-0634 Operating hours: Mondays till Sunday 9am to 6pm</p>
<p>Surat Thani Branch 412/8 Talat Mai Road Tumbon Talat, Amphoe Mueang Surat Thani Changwat Surat Thani 84000, Thailand</p> <p>Tel : +66 (0) 7721-7907-10 Fax : +66 (0) 7721-7910 Operating hours: Mondays till Friday 9am to 6pm</p>	<p>Phuket Branch 156/3 Phang Nga Road Tumbon Taratyai, Amphoe Mueang Phuket Changwat Phuket 83000, Thailand</p> <p>Tel : +66 (0) 7623-2906-9 Fax : +66 (0) 7623-2909 Operating hours: Mondays till Friday 9am to 6pm</p>	<p>Hat Yai Branch 48/106 Phadungpakdee Road Tumbon Hatyai, Amphoe Hatyai Changwat Songkhla 90110, Thailand</p> <p>Tel : +66 (0) 7435-4559-61 Fax : +66 (0) 7435-4561 Operating hours: Mondays till Friday 9am to 6pm</p>
<p>Chiang Mai Branch 2/1 Moo 3, Chiang Mai-Lampang Road Tumbon Chang Pueak, Amphoe Mueang Chiang Mai Changwat Chiang Mai 50300, Thailand</p> <p>Tel : +66 (0) 5340-9482-6 Fax : +66 (0) 5340-9486 Operating hours: Mondays till Friday 9am to 6pm</p>	<p>Phitsanulok Branch 117/7 Praongdam Road Tumbon Nai Musang, Amphoe Mueang Phitsanulok Changwat Phitsanulok 65000, Thailand</p> <p>Tel : +66 (0) 5521-2323-5 Fax : +66 (0) 5521-2326 Operating hours: Mondays till Friday 9am to 6pm</p>	

FAQ : How to configure DMZ