App User Guide

DMVPN

Version: 1.0.0

Date: 2016-06-06

Status: Confidential

Contents

Revision History

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Release Date	App Version	Doc Version	Details
2016-06-06	2.0.0	v.1.0.0	First Release

Chapter 1 Overview

DMVPN (Dynamic Multipoint VPN) is a kind of dynamic establishes VPN Tunnel technology. DMVPN uses the NHRP (Next Hop Resolution Protocol) technology to analyze the end address of VPN Tunnel in the Hub-And- Spoke under the network environment; and uses the Multipoint GRE Tunnel port to establish Multipoint GRE over IPSec VPN Tunnel. DMVPN is based on IPSec VPN and GRE VPN.

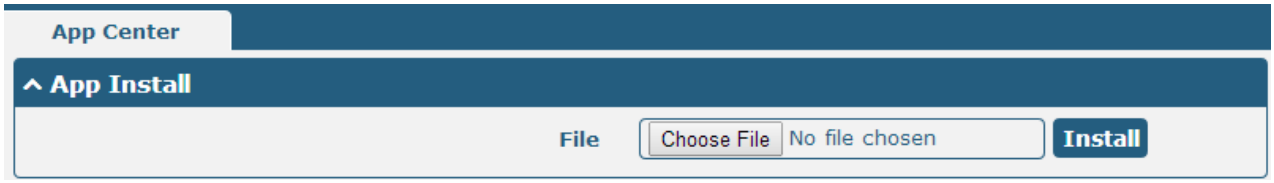
DMVPN is an App which needs to install into router in **System->App Center** unit.

Chapter 2 App Installation

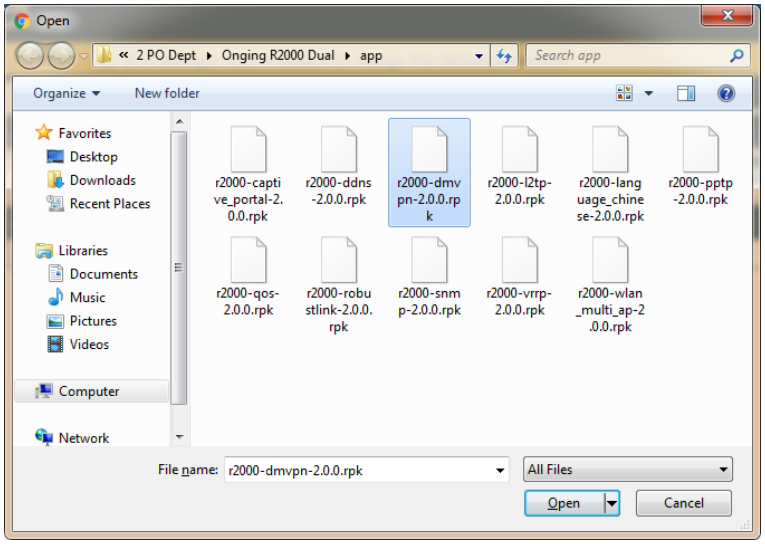
2.1 Installation

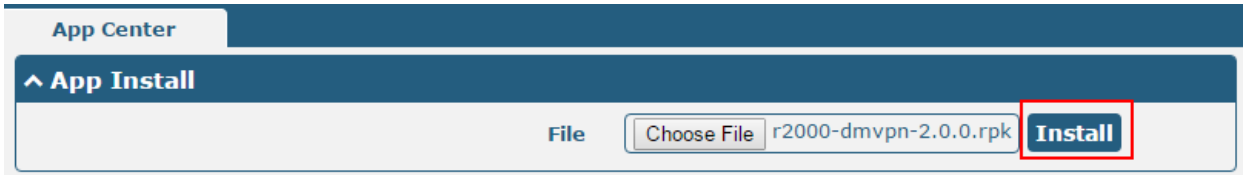
Path：**System->App**

1 Please place DMVPN App .rpk file (e.g. r2000-dmvpn-2.0.0.rpk) into a free disk of PC. And then log in router configuration page, go to **System->App** as the following screenshot show.

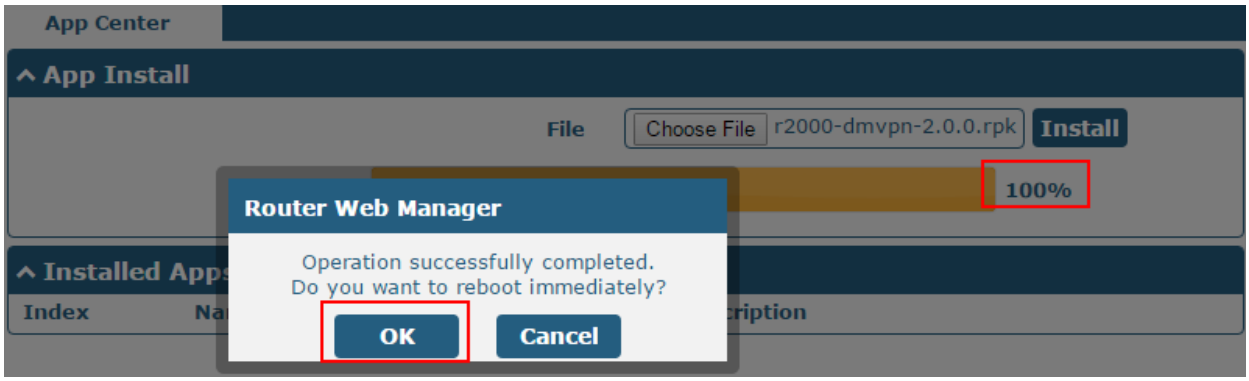


2 Click “Choose File” button, select DMVPN App .rpk file from the PC, then click “Install” button of router configuration page.

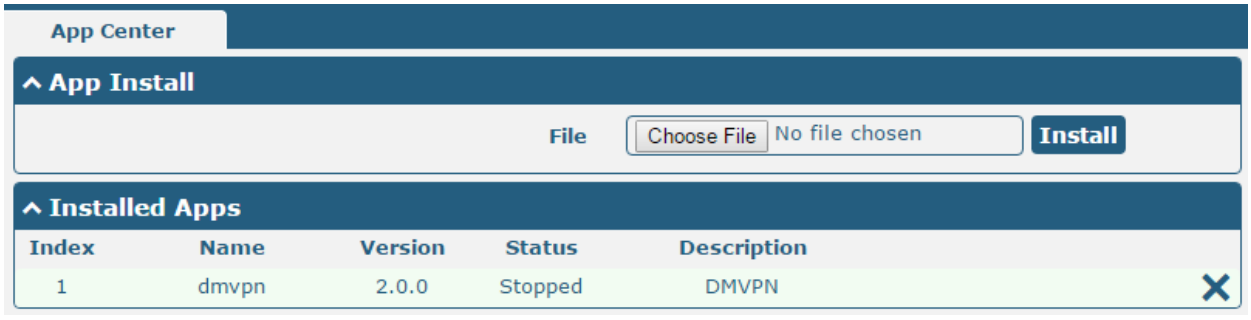


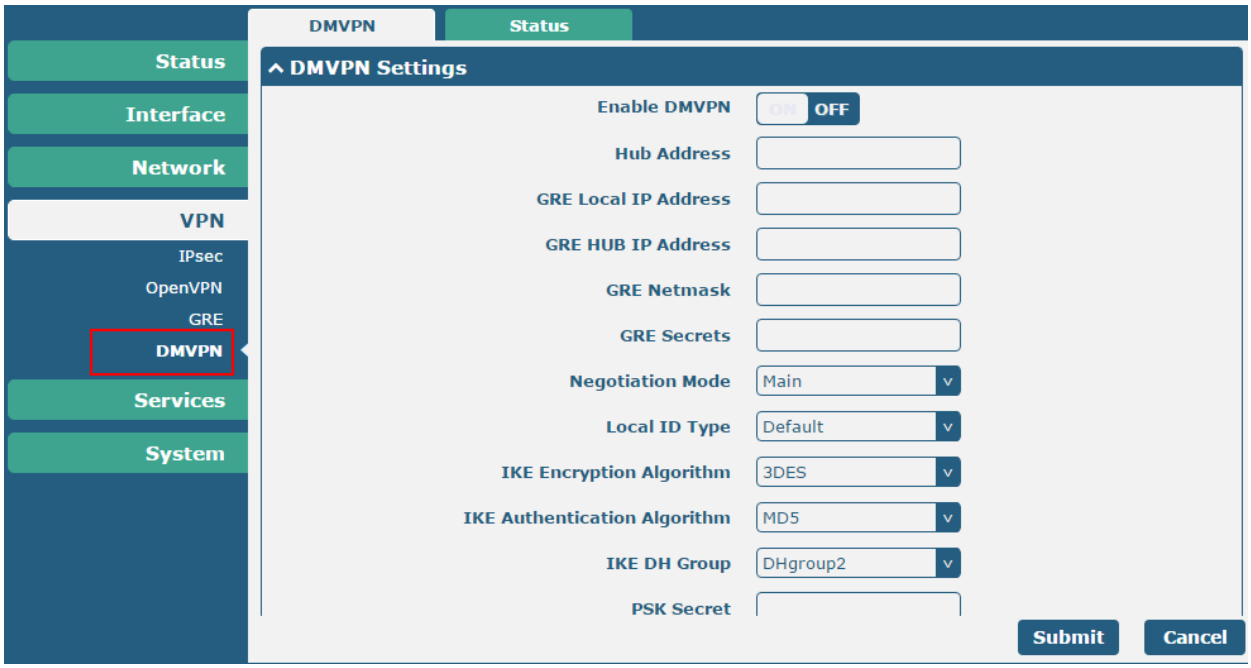


3 When the rate of installation progress reach 100%, the system will pop up a reboot router reminder window. Please click “OK” to make router reboot.



4 After router power on again, log in configuration page, DMVPN will be include in App Center’s “Installed Apps” list, and the function configuration will display in **VPN** part.

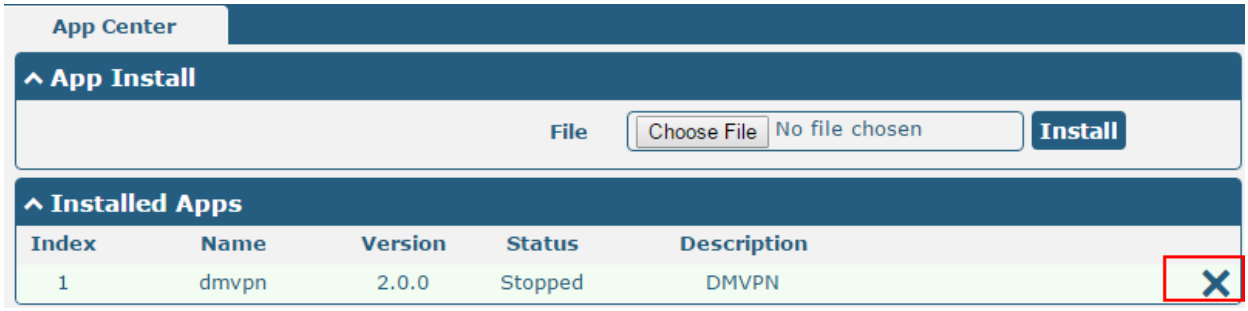




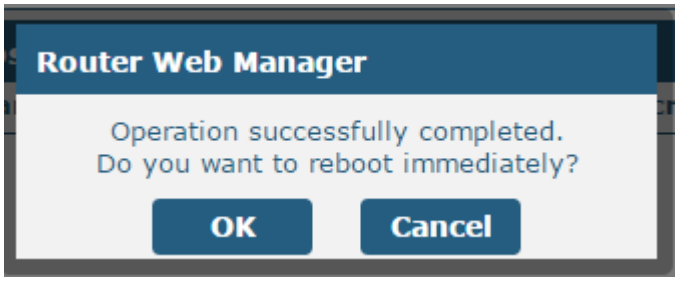
2.2 Uninstallation

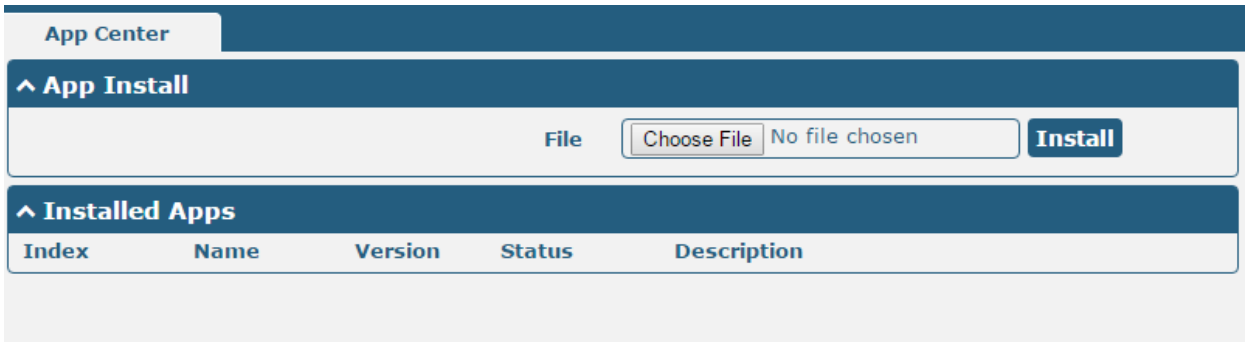
Path：**System->App Center**

1 Go to "**Installed Apps**", find DMVPN App and then click "✕".

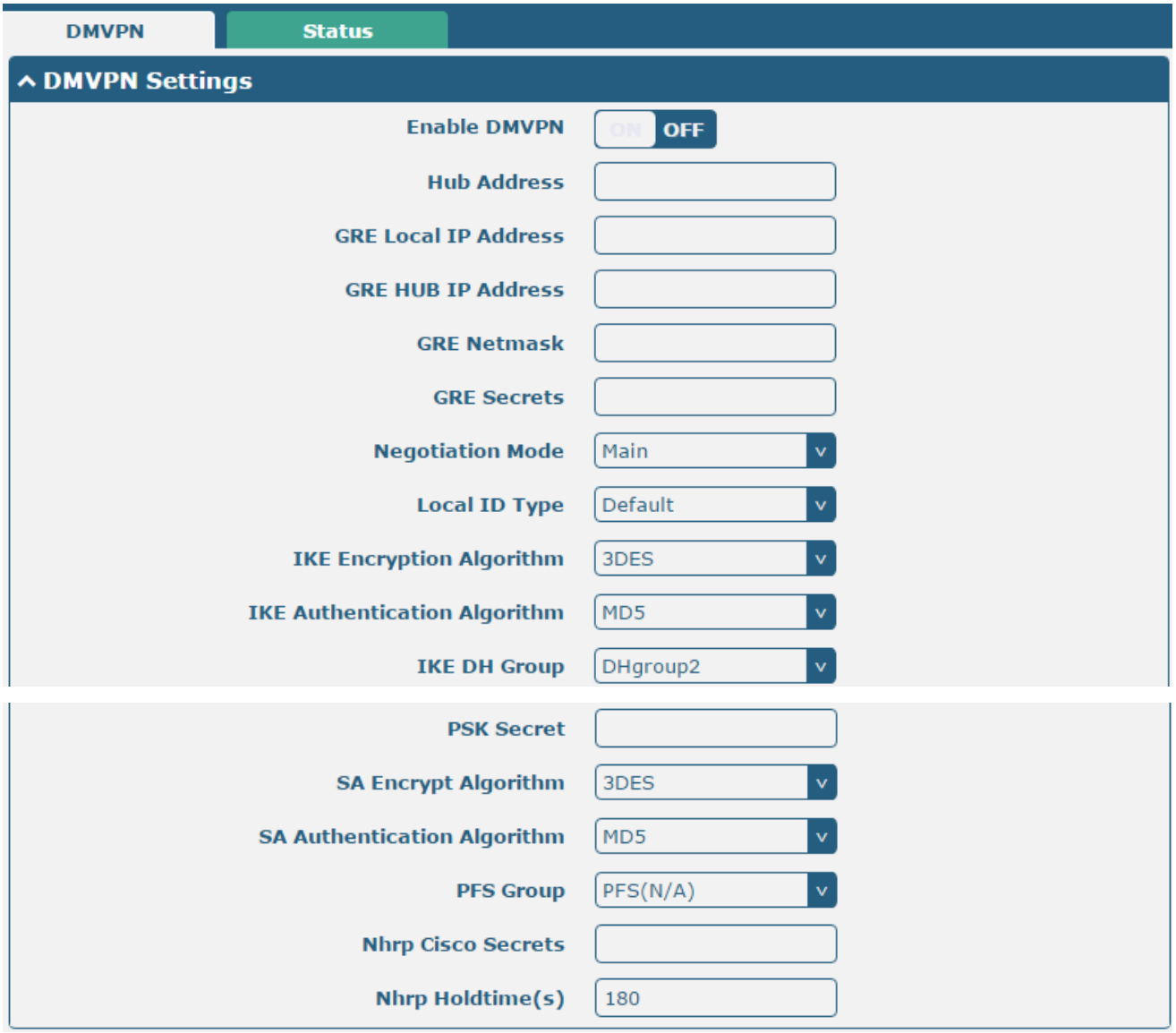


2 Click "OK" in the router reboot reminder pop up window. When router finish restart, DMVPN had been uninstalled.





Chapter 3 Parameters Description



DMVPN		
Item	Description	Default
Enable DMVPN	Click to enable DMVPN function.	OFF
Hub Address	DMVPN Hub's IP address or domain	Null
GRE Local IP address	GRE Local tunnel IP address	Null
GRE HUB IP address	GRE Hub tunnel IP address	Null
GRE Netmask	GRE tunnel Netmask	Null
GRE Secrets	GRE tunnel secret key	Null
Negotiation Mode	Select from "Main" and "aggressive" for the IKE negotiation mode in phase 1. If the IP address of one end of an IPSec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main

DMVPN		
Item	Description	Default
Local IP Type	Select from “ID”, “FQDN” and “User FQDN” for IKE negotiation. “Default” stands for “Router’s extern IP”. ID: Uses custom string as the ID in IKE negotiation. FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com. User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with an sign “@” for the local security gateway, e.g., test@robustel.com.	default
IKE Encryption Algorithm	Select from “DES”, “3DES” and “AES128” to be used in IKE negotiation. DES: Uses the DES algorithm in CBC mode and 56-bit key. 3DES: Uses the 3DES algorithm in CBC mode and 168-bit key. AES128: Uses the AES algorithm in CBC mode and 128-bit key.	3DES
IKE Authen Algorithm	Select from “MD5” and “SHA1”to be used in IKE negotiation. MD5: Uses HMAC-SHA1. SHA1: Uses HMAC-MD5.	MD5
IKE DH Group	Select from “MODP768_1”, “MODP1024_2” and “MODP1536_5”to be used in key negotiation phase 1. MODP768_1: Uses the 768-bit Diffie-Hellman group. MODP1024_2: Uses the 1024-bit Diffie-Hellman group. MODP1536_5: Uses the 1536-bit Diffie-Hellman group.	MODP1024_2
PSK Secrets	Enter Pre-shared Key	Null
SA Encrypt Algorithm	Select from “DES”, “3DES” and “AES128” to be used in IKE negotiation. DES: Uses the DES algorithm in CBC mode and 56-bit key. 3DES: Uses the 3DES algorithm in CBC mode and 168-bit key. AES128: Uses the AES algorithm in CBC mode and 128-bit key. Note: Higher security means more complex implementation and lower speed. DES is enough to meet general requirements. Use 3DES when high confidentiality and security are required.	3DES
SA Authentication Algorithm	Select from “AH_MD5_96” and “AH_ SHA1_96” when you select “AH” in “Protocol”; Select from “MD5” and “SHA1”to be used in IKE negotiation. MD5: Uses HMAC-SHA1. SHA1: Uses HMAC-MD5.	MD5
PFS Group	Select from “PFS_NULL”, “MODP768_1”, “MODP1024_2” and “MODP1536_5”. PFS_NULL: Disable PFS Group MODP768_1: Uses the 768-bit Diffie-Hellman group. MODP1024_2: Uses the 1024-bit Diffie-Hellman group. MODP1536_5: Uses the 1536-bit Diffie-Hellman group.	PES_NULL
Nhrp Cisco secret	Cisco Nhrp secret key	Null
Nhrp holdtime	The hold time of Nhrp protocol	60

Go to Status to check the DMVPN connection status.