

Så här använder du B593 Router!

B593 Router Onlinehjälp



Huawei Technologies Co., Ltd.

Adress: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129,
People's Republic of China

Webbplats: www.huawei.com

E-post: terminal@huawei.com

Upphovsrätt © Huawei Technologies Co., Ltd. 2011. Med ensamrätt.

Ingen del av detta dokument får reproduceras eller överföras i någon form eller på något sätt utan föregående skriftligt medgivande från Huawei Technologies Co., Ltd.

Varumärken och behörigheter



och andra Huawei-varumärken tillhör Huawei Technologies Co., Ltd.

Alla andra varumärken och varunamn som nämns i detta dokument tillhör sina respektive ägare.

Observera

De inköpta produkterna, tjänsterna och funktionerna fastställs av kontraktet mellan Huawei och kunden. Produkterna, tjänsterna och funktionerna som beskrivs i det här dokumentet, eller delar av dem, kan ligga utanför inköpets eller användningens omfattning. Såvida inte annat anges i kontraktet anges påståenden, information och rekommendationer i det här dokumentet i "BEFINTLIGT SKICK" utan någon som helst garanti eller löften av något slag, varken uttryckliga eller underförstådda.

Informationen i detta dokument kan ändras utan föregående varning. Målsättningen när dokumentet skapades var att dess innehåll ska vara korrekt. Dock kan inga påståenden, ingen information och inga rekommendationer i dokumentet garanteras på något sätt, varken uttryckligen eller underförstått.

Huawei Technologies Co., Ltd.

Adress: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Webbplats: <http://www.huawei.com>

E-post: terminal@huawei.com

Innehåll

1 Komma igång	1
1.1 Använda routern	1
1.2 Konfigurationskrav för datorn	1
1.3 Logga in på webbhanteringsidan	2
2 Status	3
2.1 Internet	3
2.1.1 Status	3
2.1.2 Statistik	3
2.2 LAN	3
2.2.1 Status	3
2.2.2 Statistik	4
2.3 WiFi	4
2.3.1 Status	4
2.3.2 Statistik	4
3 Allmänna inställningar	5
3.1 SIM-inställningar	5
3.1.1 Visa SIM-kortets status	5
3.1.2 Aktivera verifiering av PIN-kod	5
3.1.3 Inaktivera verifiering av PIN-kod	6
3.1.4 Verifiera PIN-koden	6
3.1.5 Byta PIN-kod	6
3.1.6 Ställa in automatisk verifiering av PIN-koden	7
3.1.7 Verifiera PUK-koden	7
3.2 Internetinställningar	7
3.2.1 Välja ett nätverksnät	7
3.2.2 Välja ett anslutningsnät	8
3.2.3 Välja data-APN	8
3.2.4 Skapa en APN-profil	9
3.2.5 Ändra en APN-profil	9
3.2.6 Ta bort en APN-profil	9
3.3 DHCP-inställningar	10
3.3.1 Inställningar för LAN-värd	10




3.3.2 DHCP-inställningar	10
3.4 WiFi-inställningar	11
3.4.1 Allmänna inställningar	11
3.4.2 Gränssnittprofil	13
3.5 WiFi WPS	15
3.5.1 WPS-inställningar	15
3.6 WiFi med multi-SSID	15
3.6.1 SSID-lista	15
3.7 Åtkomstbegränsning för WiFi	16
3.7.1 WiFi MAC-kontroll	16
3.7.2 Ställin lista	17
3.8 Internet-MTU	18
3.9 Inställningar för routning	18
3.9.1 Dynamisk routning	18
3.9.2 Statisk routning	19
4 Säkerhetsinställningar	20
4.1 Brandvägg allmänt	20
4.1.1 Brandväggens nivå	20
4.2 MAC-filer	21
4.2.1 MAC-vitlista	21
4.2.2 MAC-svartlista	22
4.3 IP-filer	23
4.3.1 IP-vitlista	23
4.3.2 IP-svartlista	24
4.4 URL-filer	26
4.4.1 URL-vitlista	26
4.4.2 URL-svartlista	27
4.5 Åtkomstkontroll för tjänst	28
4.5.1 Åtkomstkontrollista	28
5 NAT-inställningar	29
5.1 DMZ-inställningar	29
5.1.1 DMZ	29
5.2 Portmappning	29
5.2.1 Portmappning	29
5.3 UPnP	31
5.3.1 UPnP-portmappning	31
5.4 SIP ALG	32
6 USB-hantering	33
6.1 Serverinställningar	33
6.1.1 Näverksservrar	33
6.1.2 USB-lagring	33

6.2 Användarinställningar	33
6.2.1 Användarlista	34
6.3 FTP-hämtning	35
6.3.1 Hämtningshistorik	35
7 System	36
7.1 Enhetsinformation	36
7.2 Återställa	36
7.2.1 Starta om	36
7.2.2 Återställ	36
7.3 Säkerhetskopiering och uppdatering	37
7.3.1 Säkerhetskopiera	37
7.3.2 Uppdatera	37
7.4 Uppgradera	38
7.4.1 Lokal uppgradering	38
7.4.2 HTTP-uppgradering	38
7.5 Lösenordsändring	39
7.6 Datum och tid	39
7.6.1 Inställningar	39
7.7 Diagnos	40
7.7.1 Ping	40
7.7.2 Traceroute	40
7.7.3 Systemkontroll	41
7.8 Loggning	41
8 Frågor och svar	42
9 Akronym och förkortningar	43

1 Komma igång

1.1 Använda routern

I det här dokumentet kallas kundutrustningen (CPE, Customer Premises Equipment) för routern. Studera följande säkerhetssymboler noggrant för att säkerställa att du använder routern på ett korrekt och säkert sätt:

-  Anger ytterligare information om ämnet.
-  Alternativa metoder eller en genväg för en åtgärd.
-  Varnar för potentiella problem eller uppgifter som måste anges.

1.2 Konfigurationskrav för datorn

Datorn måste uppfylla routerns krav. Annars försämrans prestandan.

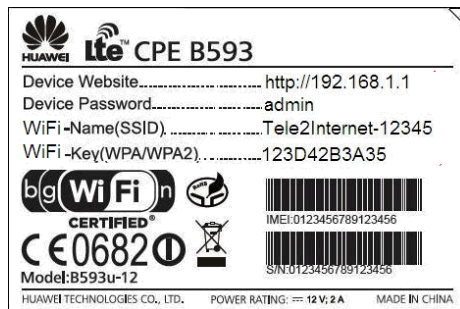
Objekt	Krav
Processor	Pentium 500 MHz eller snabbare
Minne	Minst 128 MB RAM
Hårddisk	50 MB ledigt utrymme
Operativsystem	<ul style="list-style-type: none">• Microsoft: Windows XP, Windows Vista eller Windows 7• Mac: Mac OS X
Bildskärmsupplösning	Minst 1 024 x 768 bildpunkter
Webbläsare	<ul style="list-style-type: none">• Internet Explorer 7.0 eller senare• Firefox 3.5 eller senare• Opera 10 eller senare• Safari 5 eller senare• Chrome 9 eller senare

1.3 Logga in på webbhanteringsidan

Via webbläsaren når du webbhanteringsidan där du konfigurerar och hanterar routern.

Så här loggar du in på webbhanteringsidan via Windows XP och Internet Explorer 7.0.

1. Anslut routern.
2. Ange din dators IP-adress i samma nätverkssegment som routern.



Routerens standard-IP-adress är 192.168.1.1 och nätmasken är 255.255.255.0. Du rekommenderas att ange IP-adress och DNS (Domain Name System) automatiskt.

3. Starta Internet Explorer, ange <http://192.168.1.1> i adressfältet och tryck på **Retur**.
4. Ange lösenordet och klicka på **Logga in**. När lösenordet har verifierats kan du logga in på webbhanteringsidan.

----Slut

2 Status

2.1 Internet

2.1.1 Status

Gör så här om du vill visa anslutningsstatusen för WAN (Wide Area Network):

1. Välj **Status > Internet**.
2. Visa WAN-anslutningsstatusen.

----Slut

2.1.2 Statistik

Gör så här om du vill visa statistik för WAN-porten:

1. Välj **Status > Internet**.
2. Visa statistiken för WAN-porten, till exempel upplänk- och nedlänkhastighet, upplänk- och nedlänksvolym och tid online.

----Slut

2.2 LAN

2.2.1 Status

Gör så här om du vill visa anslutningsstatus för LAN (Local Area Network):

1. Välj **Status > LAN**.
2. Visa status för LAN-anslutningen, till exempel IP-adress, MAC-adress (Media Access Control), DHCP-server (Dynamic Host Configuration Protocol) och LAN-portar (LAN1, LAN2, LAN3 och LAN4).

----Slut

2.2.2 Statistik

Gör så här om du vill visa statistik för LAN-portarna:

1. Väj **Status > LAN**.
2. Visa statistik för LAN-portarna, till exempel total trafikvolym, antal paket, antal paket med fel och antalet ignorerade paket som har överförts och tagits emot via portarna LAN1 till LAN4.

----Slut

2.3 WiFi

2.3.1 Status

Gör så här om du vill visa anslutningsstatus för WiFi:

1. Väj **Status > WiFi**.
2. Visa anslutningsstatus för WiFi, till exempel SSID, IP-adress, MAC-adress, broadcast-läge och trådlöst krypteringsläge.

----Slut

2.3.2 Statistik

Gör så här om du vill visa statistik för WiFi-portarna:

1. Väj **Status > WiFi**.
2. Visa statistik för WiFi-portarna, till exempel total trafikvolym, antal paket, antal paket med fel och antalet ignorerade paket som har överförts och tagits emot via WiFi-portarna.

----Slut

3 Allmänna inställningar

3.1 SIM-inställningar

På inställningssidan för SIM-kortet kan du hantera PIN-koden på följande sätt:

- Aktivera och inaktivera verifiering av PIN-koden
- Verifiera PIN-koden
- Byta PIN-kod
- Ställa in automatisk verifiering av PIN-koden

3.1.1 Visa SIM-kortets status

Gör så här om du vill visa SIM-kortets status:

1. Välj **Allmänna inställningar > SIM-inställningar**.
Sidan **PIN-hantering** visas.
2. SIM-kortets status visas till höger om rutan **SIM-kortstatus**.
----Slut

3.1.2 Aktivera verifiering av PIN-kod

Gör så här för att aktivera verifieringen av PIN-koden:

1. Välj **Allmänna inställningar > SIM-inställningar**.
Sidan **PIN-hantering** visas.
2. Ange **Aktivera för PIN-verifiering**.
3. Ange PIN-koden (fyra till åtta siffror) i rutan **Ange PIN-kod**.
4. Klicka på **Spara**.
----Slut

3.1.3 Inaktivera verifiering av PIN-kod

Gör så här för att inaktivera verifieringen av PIN-koden:

1. Välj **Allmänna inställningar > SIM-inställningar**.
Sidan **PIN-hantering** visas.
2. Ange **Inaktivera** för **PIN-verifiering**.
3. Ange PIN-koden (fyra till åtta siffror) i rutan **Ange PIN-kod**.
4. Klicka på **Spara**.

----Slut

3.1.4 Verifiera PIN-koden

Om verifiering av PIN-koden har aktiverats och PIN-koden inte har verifierats så krävs verifiering. Gör så här för att verifiera PIN-koden:

1. Välj **Allmänna inställningar > SIM-inställningar**.
Sidan **PIN-hantering** visas.
2. Ange PIN-koden (fyra till åtta siffror) i rutan **Verifiera PIN**.
3. Klicka på **Spara**.

----Slut

3.1.5 Byta PIN-kod

Du kan bara byta PIN-kod när verifiering av PIN-koden har aktiverats och PIN-koden har verifierats.

Gör så här för att byta PIN-kod:

1. Välj **Allmänna inställningar > SIM-inställningar**.
Sidan **PIN-hantering** visas.
2. Ange **Aktivera** för **PIN-verifiering**.
3. Ange **Aktivera** för **Ändring**.
4. Ange den aktuella PIN-koden (fyra till åtta siffror) i rutan **PIN-kod**.
5. Ange en ny PIN-kod (fyra till åtta siffror) i rutan **Ny PIN**.
6. Upprepa den nya PIN-koden i rutan **Bekräfta PIN**.
7. Klicka på **Spara**.

----Slut

3.1.6 Ställa in automatisk verifiering av PIN-koden

Du kan aktivera och inaktivera automatisk verifiering av PIN-koden. Om automatisk verifiering har aktiverats verifierar routern automatiskt PIN-koden efter en omstart. Funktionen kan bara aktiveras om verifiering av PIN-koden har aktiverats och PIN-koden har verifierats.

Gör så här för att aktivera automatisk verifiering av PIN-koden:

1. Välj **Allmänna inställningar > SIM-inställningar**.

Sidan **PIN-hantering** visas.

2. Ange **Aktivera för PIN-verifiering**.
3. Ange **Aktivera för Spara min PIN-kod**.
4. Klicka på **Spara**.

----Slut

3.1.7 Verifiera PUK-koden

Om verifiering av PIN-koden har aktiverats och PIN-koden inte kan verifieras med tre på varandra följande försök kommer PIN-koden att låsas. I så fall måste du verifiera PUK-koden och sedan byta PIN-kod för att låsa upp PIN-koden.

Gör så här för att verifiera PUK-koden:

1. Välj **Allmänna inställningar > SIM-inställningar**.

Sidan **PIN-hantering** visas.

2. Ange PUK-koden i rutan **PUK-kod**.
3. Ange en ny PIN-kod i rutan **Ny PIN**.
4. Upprepa den nya PIN-koden i rutan **Bekräfta PIN**.
5. Klicka på **Spara**.

----Slut

3.2 Internetinställningar

På den här sidan konfigurerar du Internetrelaterade inställningar.

3.2.1 Välja ett nätverksläge

Du kan välja ett nätverksläge så att routern får åtkomst till olika nätverk. **Nätverksläge** kan ha inställningarna **AUTO**, **Endast 4G**, **Endast 3G** och **Endast 2G**.

Gör så här för att välja ett nätverksläge:

1. Sätt in ett giltigt SIM-kort i routern och kontrollera att antennen fungerar.
2. Starta routern och logga in som administratör via webbgränssnittet.

3. Välj **Allmänna inställningar > Internetinställningar**.

Sidan **Internetinställningar** visas.

4. Ange något av värdena i följande tabell för **Nätverksläge**:

Parametervärde	Beskrivning
AUTO	Routern väljer läge automatiskt i ordningen 4G-nätverk, 3G-nätverk och 2G-nätverk.
Endast 4G	Routern ansluter till 4G-nätverket.
Endast 3G	Routern ansluter till 3G-nätverket.
Endast 2G	Routern ansluter till 2G-nätverket.

5. Klicka på **Spara**.

----Slut

3.2.2 Välja ett anslutningsläge

På den här sidan väljer du läge för nätverksanslutning. **Alltid på** anger att anslutningen alltid är aktiv. Om förhållandena till åter ansluter routern alltid till Internet. **Manuell** anger att du kan ansluta eller koppla bort routern manuellt från Internet.

Gör så här för att välja ett anslutningsläge:

1. Välj **Allmänna inställningar > Internetinställningar**. Sidan **Internetinställningar** visas.

2. Ange något av värdena i följande tabell för **Anslutningsläge**:

Parametervärde	Beskrivning
Alltid på	Om nätverket har kopplats bort ansluter routern automatiskt till nätverket.
Manuellt	Routern kopplar bort från Internet när den startas. Du kan ansluta till eller koppla bort från Internet manuellt.

3. Klicka på **Spara**.

----Slut

3.2.3 Välja data-APN

Du kan ange en grupp med uppringningsparametrar för ett data-APN (Access Point Name, namn på åkomstpunkt) så att routern ansluter till Internet.

Gör så här för att ställa in uppringningsparametrarna:

1. Välj **Allmänna inställningar > Internetinställningar**.

Sidan **Internetinställningar** visas.

2. Ställ först in **Data-APN** och sedan en grupp med uppringningsparametrar som motsvarar detta data-APN.
3. Klicka på **Spara**.
----Slut

3.2.4 Skapa en APN-profil

Gör så här för att skapa en grupp med uppringningsparametrar för APN:

1. Välj **Allmänna inställningar > Internetinställningar**.
Sidan **Internetinställningar** visas.
2. Klicka på **Redigera APN-profil** på sidan **Internetinställningar**.
Sidan **APN-profil** visas.
3. Klicka på **Lägg till APN-profil**.
4. Ange **APN**, **Uppringningsnummer**, **Användarnamn** och **Lösenord** på sidan som visas.
5. Ställ in **Autentisering** på **AUTO**, **PAP** eller **CHAP**.
6. Klicka på **Spara**.
----Slut

3.2.5 Ändra en APN-profil

Gör så här för att ändra APN-uppringningsparametrarna:

1. Välj **Allmänna inställningar > Internetinställningar**.
Sidan **Internetinställningar** visas.
2. Klicka på **Redigera APN-profil** på sidan **Internetinställningar**.
Sidan **APN-profil** visas.
3. Klicka på **Redigera** i den **APN-profil**-post som ska ändras.
4. Ändra **APN**, **Uppringningsnummer**, **Användarnamn** och **Lösenord** på sidan som visas.
5. Ställ in **Autentisering** på **AUTO**, **PAP** eller **CHAP**.
6. Klicka på **Spara**.
----Slut

3.2.6 Ta bort en APN-profil

Gör så här för att ta bort befintliga APN-uppringningsparametrar:

1. Välj **Allmänna inställningar > Internetinställningar**.
Sidan **Internetinställningar** visas.
2. Klicka på **Redigera APN-profil** på sidan **Internetinställningar**.

Sidan **APN-profil** visas.

3. Klicka på **Ta bort** i den **APN-profil**-post som ska tas bort. Ett meddelande visas.
4. Klicka på **OK**.

----Slut

3.3 DHCP-inställningar

Ett LAN är ett gemensamt kommunikationssystem inom ett begränsat område som har fler än en ansluten enhet.

Med korrekta LAN-inställningar kan nätverksenheter, till exempel datorer, dela kommunikation i LAN:et via routern.

3.3.1 Inställningar för LAN-värd

Som standard är IP-adressen 192.168.1.1 med nätmasken 255.255.255.0. Du kan ändra IP-adressen till en annan individuell IP-adress som är enkelt att komma ihåg, och se till att IP-adressen är unik i ditt nätverk. Om du ändrar routerns IP-adress måste du ansluta till det webbaserade verktyget via den nya IP-adressen.

Gör så här för att ändra routerns IP-adress och nätmask:

1. Välj **Allmänna inställningar > DHCP-inställningar**.

Sidan **DHCP-inställningar** visas.

2. Ställ in **IP-adress**.
3. Ställ in **Nätmask**.
4. Markera kryssrutan **Aktivera** efter **DHCP-server**.
5. Klicka på **Spara**.

----Slut

3.3.2 DHCP-inställningar

Med DHCP kan enskilda klienter TCP/IP-konfigureras automatiskt vid start från en server.

Du kan konfigurera routern som en DHCP-server eller inaktivera den när routern arbetar i routing-läge.

När routern är konfigurerad som en DHCP-server tillhandahåller den automatiskt TCP/IP-konfigurationen för LAN-klienterna som stöder DHCP-klientfunktionen. Om DHCP-servertjänster har inaktiverats måste du ha en annan DHCP-server i ditt LAN, eller också måste varje klient konfigureras manuellt.

Gör så här för att konfigurera DHCP-inställningar:

1. Välj **Allmänna inställningar > DHCP-inställningar**. Sidan **DHCP-inställningar** visas.
2. Markera kryssrutan **Aktivera** efter **DHCP-server**.
3. Ställ in **Start-IP-adress**.

☰ IP-adressen måste vara en annan än den IP-adress som har angetts på sidan **Inställningar för LAN-värd**, men den måste finnas i samma nätverkssegment.

4. Ställ in **Slut-IP-adress**.

☰ IP-adressen måste vara en annan än den IP-adress som har angetts på sidan **Inställningar för LAN-värd**, men den måste finnas i samma nätverkssegment. Slut-IP-adressen måste vara lägre eller lika med start-IP-adressen.

5. Ställ in **Lånetid**.

☰ Parametern kan vara från 1 till 10 080 minuter.

6. Klicka på **Spara**.

----Slut

I enhetslistan finns information om de aktiva enheterna.

Gör så här för att visa enhetslistan:

1. Välj **Allmänna inställningar > DHCP-inställningar**. Klicka på **Ansluten enhet**. Sidan **Anslutna enheter** visas.
2. Visa enhetslistan. I listan visas **Datornamn**, **MAC-adress**, **IP-adress** och **Lånetid**. **Lånetid** anger den återstående lånetiden för den dynamiska DHCP-servern. Om det finns en bunden statisk IP-adress visas **Lånetid** och **Datornamn** som **N/A** och **Okänd**.

----Slut

3.4 WiFi-inställningar

3.4.1 Allmänna inställningar

De grundläggande WiFi-inställningarna påverkar WiFi-prestandan. Inställningarna hjälper dig att uppnå maximal hastighet via optimal åtkomstprestanda.

Gör så här för att konfigurera grundläggande WiFi-inställningar:

1. Välj **Allmänna inställningar > WiFi-inställningar**.

Sidan **WiFi-inställningar** visas.


2. Markera kryssrutan **Aktivera** efter **Aktivera WiFi**.
3. Ange något av värdena i följande tabell för **Läge**:

Parametervärde	Beskrivning
802.11b/g/n	WiFi-stationen kan ansluta till routern i läget 802.11b, 802.11g eller 802.11n. Om stationen ansluter till routern i 802.11n-läge krävs krypteringssättet AES.
802.11b/g	WiFi-stationen kan ansluta till routern i läget 802.11b eller 802.11g.
802.11b	WiFi-stationen kan ansluta till routern i läget 802.11b.
802.11g	WiFi-stationen kan ansluta till routern i läget 802.11g.
802.11n	WiFi-stationen kan ansluta till routern i läget 802.11n.


4. Ställ in **Landskod**.

 **Kanal** kan variera beroende på vilket land som väljs.


5. Ställ in **Kanal**.

 **Auto** anger att kanalen med bäst signalkvalitet väljs.
Värdet **1** till **13** anger kanalen.


6. Ställ in **802.11n bandbredd**.

 Om parametern har värdet **20 MHz** fungerar 802.11n enbart med bandbredden 20 MHz.
Om parametern har värdet **20/40 MHz** fungerar 802.11n med bandbredden 20 MHz eller 40 MHz.
Om **Läge** har inställningen **802.11b** eller **802.11g** behöver inte den här parametern ställas in.

7. Ställ in **Hastighet**.

 **Hastighet** varierar beroende på vilket läge som har valts.
Om **Hastighet** har inställningen **Auto** ansluter WiFi-stationen till routern via den kanal som har bäst signalkvalitet.
Om hastigheten har angetts ansluter stationen till routern med en angiven hastighet.
Om kanalförhållandena inte uppfyller kravet på överkas anslutningens prestanda.

8. Ställ in **Energiöverföring**.

 Om parametern har inställningen **90% (rekommenderas)** överför WiFi-stationen med optimal effekt.
Om parametern har inställningen **100%** överför WiFi-stationen med full effekt.
Om parametern har inställningen **80%**, **60%**, **30%** eller **5%** överför WiFi-stationen

med låg effekt. WiFi-stationer som ligger långt från routern kanske inte kan få åtkomst till den.

9. Klicka på **Spara**.

----Slut

3.4.2 Gränssnittsprofil

När du konfigurerar routern på sidan **Gränssnittsprofil** ansluter WiFi-stationen till routern enligt de förinställda reglerna, vilket förbättrar åtkomstsäkerheten.

Gör så här om du vill konfigurera routern på sidan **Gränssnittsprofil**:

1. Välj **Allmänna inställningar > WiFi-inställningar**.

Sidan **WiFi-inställningar** visas.

2. Ställ in **SSID**.



Parametern får innehålla 1 till 32 ASCII-tecken.

WiFi-stationen ansluter till routern med det uppsökta SSID:t.

3. Ställ in **Maximalt antal godkända enheter**.



Parametern anger det maximala antalet WiFi-stationer som kan ansluta till routern.

Högst 32 stationer kan ansluta till routern.

4. Markera kryssrutan **Aktivera** efter **Djup broadcast**.

SSID döljs. I det här fallet kan inte stationen identifiera WiFi-information om routern.

5. Markera kryssrutan **Aktivera** efter **AP-isolering**. Stationerna kan ansluta till routern men kan inte kommunicera med varandra.

6. Ställ in **Säkerhet**.



Om parametern har inställningen **INGEN (rekommenderas inte)** ansluter WiFi-stationen direkt till routern. Det leder till säkerhetsrisker.

Om parametern har värdet **WEP** ansluter WiFi-stationen till routern i ett webbaserat krypteringsläge.

Om parametern har värdet **WPA-PSK** ansluter WiFi-stationen till routern i WPA-PSK-krypteringsläge.

Om parametern har värdet **WPA2-PSK (rekommenderas)** ansluter WiFi-stationen till routern i WPA2-PSK-krypteringsläge. Läget rekommenderas på grund av sin höga säkerhetsnivå.

Om parametern har värdet **WPA-PSK+WPA2-PSK** ansluter WiFi-stationen till routern i WPA-PSK eller WPA2-PSK-krypteringsläge.

7. Ställ in krypteringsläget.

Om...	Har inställningen	Beskrivning
WEP	GRUNDLÄGGANDE autentisering	<ul style="list-style-type: none"> • Gemensam autentisering: Stationen ansluter till routern i gemensamt autentiseringsläge. • Öppen autentisering: Stationen ansluter till routern i öppet autentiseringsläge. • Båda autentiseringarna: Stationen ansluter till routern i gemensamt eller öppet autentiseringsläge.
	Krypteringsnyckelns längd	<ul style="list-style-type: none"> • 128 bitar: Högst 13 ASCII-tecken eller 26 HEX-tecken kan anges i rutorna Nyckel 1 till Nyckel 4. • 64 bitar: Högst 5 ASCII-tecken eller 10 HEX-tecken kan anges i rutorna Nyckel 1 till Nyckel 4.
	Aktuellt nyckelindex	Kan ställas in till 1, 2, 3 eller 4 . När ett nyckelindex har valts aktiveras motsvarande nyckel.
WPA-PSK	WPA i förväg delad nyckel (PSK)	Högst 8 till 63 ASCII-tecken eller 8 till 64 HEX-tecken kan anges.
	WPA-kryptering	Kan ställas in till TKIP+AES, AES eller TKIP .
WPA2-PSK (rekommenderas)	WPA i förväg delad nyckel (PSK)	Högst 8 till 63 ASCII-tecken eller 8 till 64 HEX-tecken kan anges.
	WPA-kryptering	Kan ställas in till TKIP+AES, AES eller TKIP .
WPA-PSK + WPA2-PSK	WPA i förväg delad nyckel (PSK)	Högst 8 till 63 ASCII-tecken eller 8 till 64 HEX-tecken kan anges.
	WPA-kryptering	Kan ställas in till TKIP+AES, AES eller TKIP .

8. Klicka på **Spara**.

----Slut

3.5 WiFi WPS

3.5.1 WPS-inställningar

Med WPS (WiFi Protected Setup) lägger du enkelt till en trådlös klient i nätverket, utan att behöva konfigurera trådlösa inställningar som SSID, säkerhetsläge och lösenfras. Du kan lägga till en trådlös klient med tryckknappen eller med PIN-koden.

Om du ändrar PIN-koden kan du klicka på routerns WPS-knapp och klientens WPS-knapp för att ansluta till nätverket. Om du ändrar tryckknappen kan du inte använda PIN-knappen för att lägga till samtidigt.

Gör så här för att konfigurera WiFi WPS-inställningar:

1. Välj **Allmänna inställningar > WiFi WPS**.

Sidan **WiFi WPS** visas.

2. Markera kryssrutan **Aktivera** efter **WPS**.
3. Ställ in **WPS-läge**.



Om parametern har värdet **PBC** kan stationen ansluta till routern när du har tryckt på WPS-knappen först på stationen och sedan på routern.

Om parametern har värdet **Router-PIN-kod** kan stationen ansluta till routern när rätt PIN-kod har angetts.

Endast WPA- och WPA2-kryptering stöds.

4. Klicka på **Spara**.

----Slut

3.6 WiFi med multi-SSID

Högst fyra SSID kan användas för den här funktionen. Du kan ställa in parametrar för fyra SSID, till exempel konfigurera olika hastigheter och lägen. Som standard är det SSID som har index 1 aktiverat och kan inte inaktiveras, och de SSID som har index 2, 3 och 4 är inaktiverade.

3.6.1 SSID-lista

På sidan **SSID-lista** visas information om de fyra SSID som ska konfigureras. Gör så här för att konfigurera ett SSID:

1. Välj **Allmänna inställningar > WiFi med multi-SSID**.

Sidan **SSID-lista** visas.

2. Välj ett SSID att konfigurera och klicka på **Redigera**.
3. Markera kryssrutan **Aktivera** efter **Aktivera SSID**.
4. Ställ in **SSID**.

SSID får innehålla 1 till 32 ASCII-tecken. SSID får inte innehålla följande specialtecken: '/', '!', '=', '!', '\', '&'.

5. Ställ in **Maximalt antal godkända enheter**.

Antalet åtkomstenheter ska vara ett heltal mellan 1 och 32.

6. Markera kryssrutan **Aktivera efter Döj broadcast**.

Ställ in **AP-isolering**. Om kryssrutan **Aktivera** har markerats kan stationerna ansluta till routern, men de kan inte kommunicera med varandra. Om kryssrutan inte har markerats kan stationerna ansluta till routern på samma gång och kommunicera med varandra.

8. Ställ in **Säkerhet**. Om **Läge** har inställningen **802.11n** på sidan **Allmänna inställningar** kan **Säkerhet** bara få värdet **WPA-PSK**, **WPA2-PSK** eller motsvarande krypteringsläge.

Om **Säkerhet** har inställningen **WPA-PSK**, **WPA2-PSK** eller **WPA-PSK+WPA2-PSK** ställer du in **WPA i förväg delad nyckel (PSK)** och **WPA-kryptering**.

Den i förväg delade nyckeln (PSK) för WPA måste bestå av 8 till 63 ASCII-tecken eller 64 HEX-tecken.

Om **Säkerhet** har inställningen **WEP** ställer du in **GRUNDLÄGGANDE autentisering**, Krypteringsnyckelns **längd** och **Aktuellt nyckelindex**, och konfigurerar motsvarande nycklar.

Om **Krypteringsnyckelns längd** har inställningen **128 bitar** ska den i förväg delad nyckeln (PSK) för WPA innehålla 8 till 63 ASCII-tecken eller 64 HEX-tecken.

Om **Krypteringsnyckelns längd** har inställningen **64 bitar** måste 64-bitarskrypteringsnyckeln innehålla 5 ASCII-tecken eller 10 HEX-tecken.

9. Klicka på **Spara**.

----Slut

3.7 Åtkomstbegränsning för WiFi

3.7.1 WiFi MAC-kontroll

Med den här funktionen hanterar du åtkomsten till routern. Du kan ställa in regler för åtkomstbegränsning för varje SSID.

MAC-åtkomsten till varje SSID kan ställas in som **Inaktivera**, **Svartlista** eller **Vitlista**.

- Om **SSID1 MAC-åtkomst** har inställningen **Inaktivera** aktiveras inte åtkomstbegränsningen.
- Om **SSID1 MAC-åtkomst** har inställningen **Svartlista** kan endast enheter som inte finns i svartlistan ansluta till SSID:t.
- Om **SSID1 MAC-åtkomst** har inställningen **Vitlista** kan endast enheter som finns i vitlistan ansluta till SSID:t.

Gör så här för att konfigurera inställningarna för WiFi MAC-kontroll:

1. Välj **Allmänna inställningar > Åtkomstbegränsning för WiFi**.

Sidan **WiFi MAC-kontroll** visas.

2. Ställ in **SSID1 MAC-åtkomst**.
3. Ställ in **SSID2 MAC-åtkomst**.
4. Ställ in **SSID3 MAC-åtkomst**.
5. Ställ in **SSID4 MAC-åtkomst**.
6. Klicka på **Spara**.

----Slut

3.7.2 Ställ in lista

Med den här funktionen kan du ställa in regler för SSID-åtkomst baserat på MAC-adresser. Ställ in ett SSID som motsvarar en MAC-adress.

Gör så här om du vill lägga till ett objekt i inställningslistan:

1. Välj **Allmänna inställningar > Åtkomstbegränsning för WiFi**.

Sidan **WiFi MAC-lista** visas.

2. Klicka på **Ställ in lista**. Sidan **WiFi-åtkomstlista** visas.
3. Klicka på **Lägg till objekt**.
4. Ställ in **MAC**.
5. Aktivera MAC-adressen för SSID1 genom att markera kryssrutan **Aktivera** efter **För SSID1**. Åtgärderna för SSID2, SSID3 och SSID4 är desamma som för SSID1.
6. Klicka på **Spara**.

----Slut

Gör så här om du vill ändra ett objekt i inställningslistan:

1. Välj **Allmänna inställningar > Åtkomstbegränsning för WiFi**.

Sidan **WiFi MAC-lista** visas.

2. Klicka på **Ställ in lista**. Sidan **WiFi-åtkomstlista** visas.
3. Klicka på **Redigera** i posten för det objekt som ska ändras.
4. Ställ in **MAC** på sidan som visas.
5. Aktivera MAC-adressen för SSID1 genom att markera kryssrutan **Aktivera** efter **För SSID1**. Åtgärderna för SSID2, SSID3 och SSID4 är desamma som för SSID1.
6. Klicka på **Spara**.

----Slut

Gör så här om du vill ta bort ett objekt från inställningslistan:

1. Välj **Allmänna inställningar > Åtkomstbegränsning för WiFi**.

Sidan **WiFi MAC-lista** visas.

2. Klicka på **Ställ in lista**. Sidan **WiFi-åtkomstlista** visas.
3. Klicka på **Ta bort** i posten för det objekt som ska tas bort. Ett meddelande visas.
4. Klicka på **OK**.

----Slut

Gör så här om du vill ta bort alla objekt från inställningslistan:

1. Välj **Allmänna inställningar > Åtkomstbegränsning för WiFi**.

Sidan **WiFi MAC-lista** visas.

2. Klicka på **Ställ in lista**. Sidan **WiFi-åtkomstlista** visas.
3. Klicka på **Ta bort alla**. Ett meddelande visas.
4. Klicka på **OK**.

----Slut

3.8 Internet-MTU

En MTU (Maximum Transmission Unit) definieras som den maximala paketstorleken (i byte) i ett kommunikationsprotokollager. Den gäller för kommunikationsportar, till exempel gränssnittskort för nätverk och seriella portar.

Gör så här för att konfigurera MTU:

1. Välj **Allmänna inställningar > Internet-MTU**.

Sidan **Internet-MTU** visas.

2. Ställ in ett värde mellan 576 och 1 500 för **MTU**.
3. Klicka på **Spara**.

----Slut

3.9 Inställningar för routning

3.9.1 Dynamisk routning

Den här funktionen är aktiv när kaskadkopplade routrar som följer RIP (Routing Information Protocol) används i intranätet. På den här sidan aktiverar och inaktiverar du RIP och ställer in RIP-version samt RIP-driftläge.

Gör så här för att konfigurera inställningar för dynamisk routning:

1. Välj **Allmänna inställningar > Inställningar för routning**.

Sidan **Inställningar för routning** visas.

2. Klicka på **Inställningar** till höger ovan **Dynamisk routning**-fliken.
Inmatningsrutan för konfigurationer visas.
3. Markera kryssrutan **Aktivera** efter **Aktivera RIP**.
4. Ställ in **Åtgärd**. Om du anger inställningen **Aktiv** meddelar routern aktivt de omgivande routrarna om ruttändringar. Om du anger inställningen **Passive** ändras rutterna passivt.
5. Ställ in **Version** som **RIP v1**, **RIP v2** eller **RIP v1/RIP v2**.
6. Klicka på **Spara**.
----Slut

3.9.2 Statisk routning

Funktionerna för statisk routning liknar funktionerna för dynamisk routning. Skillnaden är att ruttinställningarna läggs till manuellt för att säkerställa att de är konsekventa och att rutterna kan nås.

- Om den kaskadkopplade routern har en fast IP-adress rekommenderas statisk routning.
- Om den kaskadkopplade routern har en IP-adress som kan ändras rekommenderas dynamisk routning.

Gör så här för att konfigurera inställningar för statisk routning:

1. Välj **Allmänna inställningar > Inställningar för routning**. Sidan **Statisk routning** visas.
2. Klicka på **Lägg till objekt** till höger ovan **Statisk routning**-fliken.
Inmatningsrutan för konfigurationer visas.
3. Ställ in **Mål-IP-adress**.
4. Ställ in **Nätmask**.
5. Ställ in **Router-IP-adress**. Den här IP-adressen kommer från routern och används för överföring till de kaskadkopplade enheterna. Den måste vara tillgänglig.
6. Klicka på **Spara**.
----Slut

4 Säkerhetsinställningar

4.1 Brandvägg allmänt

4.1.1 Brandväggens nivå

På den här sidan får du anvisningar om hur du ställer in brandväggens nivå. Om **Brandväggens nivå** har inställningen **Anpassat** kan konfigurationen ändras.

Gör så här för att konfigurera brandväggens nivå.

1. Välj **Säkerhetsinställningar > Brandvägg allmänt**.

Sidan **Brandvägg allmänt** visas.

2. Ange något av värdena i följande tabell för **Brandväggens nivå**.

Parametervärde	Beskrivning
Avaktivera	Brandväggen inaktiveras.
Hög	MAC-filtrering , IP-filtrering och URL-filtrering får inställningen Vitlista .
Medel	MAC-filtrering och IP-filtrering får inställningen Vitlista . URL-filtrering får inställningen Svartlista .
Låg	MAC-filtrering , IP-filtrering och URL-filtrering får inställningen Svartlista .
Anpassat	MAC-filtrering , IP-filtrering och URL-filtrering kan anpassas.

3. Klicka på **Spara**.

----Slut

Gör så här för att ställa in filtreringsfunktionerna för brandväggen:

1. Välj **Säkerhetsinställningar > Brandvägg allmänt**.

Sidan **Brandvägg allmänt** visas.

2. Ställ in **Anpassat för Brandväggens nivå**.
3. Ställ in **MAC-filtrering**.
4. Ställ in **IP-filtrering**.
5. Ställ in **URL-filtrering**.
6. Klicka på **Spara**.

----Slut

4.2 MAC-filter

Data filtreras efter MAC-adress. På den här sidan konfigurerar du enbart regler för MAC-filtrering.

4.2.1 MAC-vitlista

Gör så här för att lägga till en regel för MAC-vitlista:

1. Vaj **Säkerhetsinställningar > MAC-filter**.

Sidan **MAC-filter** visas.

2. Ställ in **Vitlista för MAC-filtreringsläge**.
3. Klicka på **Lägg till objekt**.
4. Ställ in **MAC** på sidan som visas.
5. Klicka på **Spara**.

----Slut

Gör så här för att ändra en regel för MAC-vitlista:

1. Vaj **Säkerhetsinställningar > MAC-filter**.

Sidan **MAC-filter** visas.

2. Ställ in **Vitlista för MAC-filtreringsläge**.
3. Klicka på **Redigera** i posten för den regel som ska ändras.
4. Ställ in **MAC** på sidan som visas.
5. Klicka på **Spara**.

----Slut

Gör så här för att ta bort en regel för MAC-vitlista:

1. Vaj **Säkerhetsinställningar > MAC-filter**.

Sidan **MAC-filter** visas.

2. Ställ in **Vitlista** för **MAC-filtreringsläge**.
3. Klicka på **Ta bort** i posten för den regel som ska tas bort. Ett meddelande visas.
4. Klicka på **OK**.

----Slut

Gör så här för att ta bort alla regler för MAC-vitlista:

1. Välj **Säkerhetsinställningar > MAC-filter**.
Sidan **MAC-filter** visas.
2. Ställ in **Vitlista** för **MAC-filtreringsläge**.
3. Klicka på **Ta bort alla**. Ett meddelande visas.
4. Klicka på **OK**.

----Slut

4.2.2 MAC-svartlista

Gör så här för att lägga till en regel för MAC-svartlista:

1. Välj **Säkerhetsinställningar > MAC-filter**.
Sidan **MAC-filter** visas.
2. Ställ in **Svartlista** för **MAC-filtreringsläge**.
3. Klicka på **Lägg till objekt**.
4. Ställ in **MAC** på sidan som visas.
5. Klicka på **Spara**.

----Slut

Gör så här för att ändra en regel för MAC-svartlista:

1. Välj **Säkerhetsinställningar > MAC-filter**.
Sidan **MAC-filter** visas.
2. Ställ in **Svartlista** för **MAC-filtreringsläge**.
3. Klicka på **Redigera** i posten för den regel som ska ändras.
4. Ställ in **MAC** på sidan som visas.
5. Klicka på **Spara**.

----Slut

Gör så här för att ta bort en regel för MAC-svartlista:

1. Välj **Säkerhetsinställningar > MAC-filter**.

Sidan **MAC-filter** visas.

2. Ställ in **Svartlista för MAC-filtreringsläge**.
3. Klicka på **Ta bort** i posten för den regel som ska tas bort. Ett meddelande visas.
4. Klicka på **OK**.

----Slut

Gör så här för att ta bort alla regler för MAC-svartlista:

1. Välj **S äkerhetsinställningar > MAC-filter**.
- Sidan **MAC-filter** visas.
2. Ställ in **Svartlista för MAC-filtreringsläge**.
 3. Klicka på **Ta bort alla**. Ett meddelande visas.
 4. Klicka på **OK**.

----Slut

4.3 IP-filter

Data filtreras efter IP-adress. På den här sidan konfigurerar du enbart regler för IP-filtrering.

4.3.1 IP-vitlista

Gör så här för att lägga till en regel för IP-vitlista:

1. Välj **S äkerhetsinställningar > IP-filter**.
- Sidan **IP-filter** visas.
2. Ställ in **Vitlista för IP-filtreringsläge**.
 3. Klicka på **L ägg till objekt**.
 4. Ställ in **Programnamn**.
 5. Ställ in **Protokoll**.
 6. Ange IP-adressen eller IP-adressegmentet som ska filtreras i rutan **K älladressintervall**.
 7. Ange portnumret eller portnummersegmentet som ska filtreras i **Intervall för k ällportnummer**.
 8. Ange IP-adressen eller IP-adressegmentet som ska filtreras i rutan **Intervall för m åadress**.
 9. Ange portnumret eller portnummersegmentet som ska filtreras i **Intervall för m åportnummer**.
 10. Klicka på **Spara**.

----Slut

Gör så här för att ändra en regel för IP-vitlista:

1. Välj **S äkerhetsinställningar > IP-filter**.

Sidan **IP-filter** visas.

2. Ställ in **Vitlista för IP-filtreringsläge**.
3. Klicka på **Redigera** i posten för den regel som ska ändras.
4. Ställ in **Programnamn**.
5. Ställ in **Protokoll**.
6. Ange IP-adressen eller IP-adressegmentet som ska filtreras i rutan **Källadressintervall**.
7. Ange portnumret eller portnummersegmentet som ska filtreras i **Intervall för källportnummer**.
8. Ange IP-adressen eller IP-adressegmentet som ska filtreras i rutan **Intervall för måladress**.
9. Ange portnumret eller portnummersegmentet som ska filtreras i **Intervall för målportnummer**.
10. Klicka på **Spara**.

----Slut

Gör så här för att ta bort en regel för IP-vitlista:

1. Välj **Säkerhetsinställningar > IP-filter**.

Sidan **IP-filter** visas.

2. Ställ in **Vitlista för IP-filtreringsläge**.
3. Klicka på **Ta bort** i posten för den regel som ska tas bort. Ett meddelande visas.
4. Klicka på **OK**.

----Slut

Gör så här för att ta bort alla regler för IP-vitlista:

1. Välj **Säkerhetsinställningar > IP-filter**.

Sidan **IP-filter** visas.

2. Ställ in **Vitlista för IP-filtreringsläge**.
3. Klicka på **Ta bort alla**. Ett meddelande visas.
4. Klicka på **OK**.

----Slut

4.3.2 IP-svartlista

Om **IP-filtrering** har inställningen **Svartlista** på sidan **Brandvägg allmänt** är IP-adresserna i IP-svartlistan de enda adresser som det inte går att få åtkomst till.

Gör så här för att lägga till en regel för IP-svartlista:

1. Välj **Säkerhetsinställningar > IP-filter**.

Sidan **IP-filter** visas.

2. Ställ in **Svartlista för IP-filtreringsläge**.
3. Klicka på **Lägg till objekt**.
4. Ställ in **Programnamn**.
5. Ställ in **Protokoll**.
6. Ange IP-adressen eller IP-adressegmentet som ska filtreras i rutan **Källadressintervall**.
7. Ange portnumret eller portnummersegmentet som ska filtreras i **Intervall för källportnummer**.
8. Ange IP-adressen eller IP-adressegmentet som ska filtreras i rutan **Intervall för måladdress**.
9. Ange portnumret eller portnummersegmentet som ska filtreras i **Intervall för målportnummer**.
10. Klicka på **Spara**.

----Slut

Gör så här för att ändra en regel för IP-svartlista:

1. Välj **Säkerhetsinställningar > IP-filter**.

Sidan **IP-filter** visas.

2. Ställ in **Svartlista för IP-filtreringsläge**.
3. Klicka på **Redigera** i posten för den regel som ska ändras.
4. Ställ in **Programnamn**.
5. Ställ in **Protokoll**.
6. Ange IP-adressen eller IP-adressegmentet som ska filtreras i rutan **Källadressintervall**.
7. Ange portnumret eller portnummersegmentet som ska filtreras i **Intervall för källportnummer**.
8. Ange IP-adressen eller IP-adressegmentet som ska filtreras i rutan **Intervall för måladdress**.
9. Ange portnumret eller portnummersegmentet som ska filtreras i **Intervall för målportnummer**.
10. Klicka på **Spara**.

----Slut

Gör så här för att ta bort en regel för IP-svartlista:

1. Välj **Säkerhetsinställningar > IP-filter**.

Sidan **IP-filter** visas.

2. Ställ in **Svartlista för IP-filtreringsläge**.
3. Klicka på **Ta bort** i posten för den regel som ska tas bort. Ett meddelande visas.

4. Klicka på **OK**.

----Slut

Gör så här för att ta bort alla regler för IP-svartlista:

1. Välj **Säkerhetsinställningar > IP-filter**.

Sidan **IP-filter** visas.

2. Ställ in **Svartlista för IP-filtreringsläge**.
3. Klicka på **Ta bort alla**. Ett meddelande visas.
4. Klicka på **OK**.

----Slut

4.4 URL-filter

Data filtreras efter URL (Uniform Resource Locator). På den här sidan konfigurerar du enbart regler för URL-filtrering.

4.4.1 URL-vitlista

Gör så här för att lägga till en regel för URL-vitlista:

1. Välj **Säkerhetsinställningar > URL-filter**.

Sidan **URL-filter** visas.

2. Ställ in **Vitlista för URL-filtreringsläge**.
3. Klicka på **Lägg till objekt**.
4. Ställ in **URL**.
5. Klicka på **Spara**.

----Slut

Gör så här för att ändra en regel för URL-vitlista:

1. Välj **Säkerhetsinställningar > URL-filter**.

Sidan **URL-filter** visas.

2. Ställ in **Vitlista för URL-filtreringsläge**.
3. Klicka på **Redigera** i posten för den regel som ska ändras.
4. Ställ in **URL** på sidan som visas.
5. Klicka på **Spara**.

----Slut

Gör så här för att ta bort en regel för URL-vitlista:

1. V äj **Sakerhetsinställningar > URL-filter**.
Sidan **URL-filter** visas.
2. St äll in **Vitlista för URL-filtreringsläge**.
3. Klicka på **Ta bort** i posten för den regel som ska tas bort. Ett meddelande visas.
4. Klicka på **OK**.
----Slut

Gör så här för att ta bort alla regler för URL-vitlista:

1. V äj **Sakerhetsinställningar > URL-filter**.
Sidan **URL-filter** visas.
2. St äll in **Vitlista för URL-filtreringsläge**.
3. Klicka på **Ta bort alla**. Ett meddelande visas.
4. Klicka på **OK**.
----Slut

4.4.2 URL-svartlista

Om **URL-filtrering** har inställningen **Svartlista** på sidan **Brandvägg allmänt** är de URL som finns i URL-svartlistan de enda som det inte går att få åkomst till.

Gör så här för att lägga till en regel för URL-svartlista:

1. V äj **Sakerhetsinställningar > URL-filter**.
Sidan **URL-filter** visas.
2. St äll in **Svartlista för URL-filtreringsläge**.
3. Klicka på **Lägg till objekt**.
4. St äll in **URL**.
5. Klicka på **Spara**.
----Slut

Gör så här för att ändra en regel för URL-svartlista:

1. V äj **Sakerhetsinställningar > URL-filter**.
Sidan **URL-filter** visas.
2. St äll in **Svartlista för URL-filtreringsläge**.
3. Klicka på **Redigera** i posten för den regel som ska ändras.
4. St äll in **URL** på sidan som visas.
5. Klicka på **Spara**.
----Slut

Gör så här för att ta bort en regel för URL-svartlista:

1. Välj **Säkerhetsinställningar > URL-filter**.

Sidan **URL-filter** visas.

2. Ställ in **Svartlista för URL-filtreringsläge**.
3. Klicka på **Ta bort** i posten för den regel som ska tas bort. Ett meddelande visas.
4. Klicka på **OK**.

----Slut

Gör så här för att ta bort alla regler för URL-svartlista:

1. Välj **Säkerhetsinställningar > URL-filter**. Sidan **URL-filter** visas.
2. Ställ in **Svartlista för URL-filtreringsläge**.
3. Klicka på **Ta bort alla**. Ett meddelande visas.
4. Klicka på **OK**.

----Slut

4.5 Åtkomstkontroll för tjänst

Med den här funktionen kan du kontrollera antalet användare som ansluter till routern.

4.5.1 Åtkomstkontrollista

I åtkomstkontrollistan visas de typer av tjänster som kontrolleras av routern. Som standard är åtkomstkontroll för alla typer av tjänster förbjuden. Ställ **IP-adressintervall** och **Status** efter behov.

Gör så här för att ställa in åtkomstkontrollistan:

1. Välj **Säkerhetsinställningar > Åtkomstkontroll för tjänst**.

Sidan **Åtkomstkontroll för tjänst** visas.

2. Välj det objekt som ska konfigureras och klicka på **Redigera**.
3. Ställ in **IP-adressintervall**.



Om **Åtkomstriktning** är **LAN** måste IP-adressen finnas i samma nätverkssegment som IP-adressen som har angetts på sidan **Inställningar för LAN-värd**.

Om **Åtkomstriktning** är **WAN** måste IP-adressen finnas i ett annat nätverk än den IP-adress som har angetts på sidan **Inställningar för LAN-värd**.

4. Ställ **Status**.
5. Klicka på **Spara**.

----Slut

5 NAT-inställningar


5.1 DMZ-inställningar

5.1.1 DMZ

Om DMZ (DeMilitarized Zone) har aktiverats skickas de paket som kommer från WAN och som inte överensstämmer med några regler till datorn på LAN-sidan för analys eller annan ändring innan de ignoreras av brandväggen.

Gör så här för att aktivera DMZ:

1. Välj **NAT-inställningar > DMZ-inställningar**. Sidan **DMZ-inställningar** visas.
2. Markera kryssrutan **Aktivera** efter **DMZ**.
3. Ställ in **Värdadress**.

 IP-adressen måste vara en annan än den IP-adress som har angetts på sidan **Inställningar för LAN-värd**, men den måste finnas i samma nätverkssegment.

4. Klicka på **Spara**.

----Slut

5.2 Portmappning

När NAT (Network Address Translation) har aktiverats i routern syns endast IP-adressen på WAN-sidan externt. När vissa tjänster, till exempel FTP-tjänsten, ska aktiveras på den dator på LAN-sidan måste porten på routerns WAN-sida dirigeras om till FTP-porten på datorn på LAN-sidan. Därför kan värdet på WAN-sidan få åtkomst till värdet på LAN-sidan via den här porten på WAN-sidan.

Varje regel på den här sidan kan ändras oberoende av andra regler.

5.2.1 Portmappning

Gör så här för att lägga till en regel för portmappning:

1. Välj **NAT-inställningar > Portmappning**.

Sidan Portmappning visas.

2. Klicka på **Lägg till objekt**.
3. Ställ in **Typ**. Om du vill konfigurera regler ställer du in värdet **Anpassning** för den här parametern.
4. Ställ in **Protokoll**.
5. (Valfritt) Ställ in **Fjärrvärd**.
6. Ställ in **Intervall för fjärrportnummer**.

Portnumret ska ligga inom intervallet 1 till 65 535.

7. Ställ in **Lokal värd**.

IP-adressen måste vara en annan än den IP-adress som har angetts på sidan **Inställningar för LAN-värd**, men den måste finnas i samma nätverkssegment.

8. Ställ in **Lokalt portnummer**.

Portnumret ska ligga inom intervallet 1 till 65 535.

9. Ställ in **Aktivera** eller **Inaktivera** för **Status**.

10. Klicka på **Spara**.

----Slut

Gör så här för att ändra en regel för portmappning:

1. Välj **NAT-inställningar > Portmappning**.

Sidan Portmappning visas.

2. Klicka på **Redigera** i posten för det objekt som ska ändras.
3. Ställ in **Typ**. Om du vill konfigurera regler ställer du in värdet **Anpassning** för den här parametern.
4. Ställ in **Protokoll**.
5. (Valfritt) Ställ in **Fjärrvärd**.
6. Ställ in **Intervall för fjärrportnummer**.

Portnumret ska ligga inom intervallet 1 till 65 535.

7. Ställ in **Lokal värd**.

IP-adressen måste vara en annan än den IP-adress som har angetts på sidan

Inställningar för LAN-värd, men den måste finnas i samma nätverkssegment.

8. Ställ in **Lokalt portnummer**.

☰ Portnumret ska ligga inom intervallet 1 till 65 535.

9. Ställ in **Aktivera** eller **Inaktivera** för **Status**.

10. Klicka på **Spara**.

----Slut

Gör så här för att ta bort en regel för portmappning:

1. Välj **NAT-inställningar > Portmappning**.

Sidan **Portmappning** visas.

2. Klicka på **Ta bort** i posten för det objekt som ska tas bort. Ett meddelande visas.

3. Klicka på **OK**.

----Slut

Gör så här för att ta bort alla regler för portmappning:

1. Välj **NAT-inställningar > Portmappning**.

Sidan **Portmappning** visas.

2. Klicka på **Ta bort alla**. Ett meddelande visas.

3. Klicka på **OK**.

----Slut

5.3 UPnP

På denna sida anger du om UPnP-funktionen ska aktiveras eller inte.

Gör så här för att aktivera UPnP:

1. Välj **NAT-inställningar > UPnP**.

Sidan **UPnP** visas.

2. Markera kryssrutan **Aktivera** efter **UPnP**.

----Slut

5.3.1 UPnP-portmappning

På denna sida visas de regler för portmappning som konfigureras av intranätet enligt UPnP.

5.4 SIP ALG

På den här sidan aktiverar eller inaktiverar du SIP ALG.

Gör så här för att aktivera SIP ALG:

1. Välj **NAT-inställningar > SIP ALG**.

Sidan **SIP ALG** visas.

2. Markera kryssrutan **Aktivera** efter **SIP ALG**.

3. Ställ in **SIP-port**.



Standardporten med nummer 5060 rekommenderas. Standardporten måste användas för att VoIP-program ska kunna användas.

4. Klicka på **Spara**.

----Slut

6 USB-hantering

6.1 Serverinställningar

På sidan **Serverinställningar** visas grundläggande USB-information, till exempel lagringsutrymme, använt utrymme, ledigt utrymme och om FTP-servern ska aktiveras.

6.1.1 Nätverksservrar

På sidan **Nätverksservrar** visar och anger du FTP-serverns status.

Gör så här för att aktivera FTP-servern:

1. Välj **USB-hantering > Serverinställningar**.

Sidan **Nätverksservrar** visas.

2. Markera kryssrutan **Aktivera** efter **FTP-server**.
3. Klicka på **Spara**.

----Slut

6.1.2 USB-lagring

På sidan **USB-lagring** visas information om USB-lagringsutrymmet, till exempel total mängd lagringsutrymme, använt utrymme och ledigt utrymme. Gör så här för att visa USB-lagringsutrymmet:

1. Välj **USB-hantering > Serverinställningar**.

Sidan **USB-lagring** visas.

2. Klicka på **Uppdatera** för att uppdatera USB-lagringsutrymmet manuellt.

----Slut

6.2 Användarinställningar

Du kan lägga till användare i listan för att dela filerna och katalogerna på USB-disken. Genom att använda det konfigurerade kontot kan användare få åtkomst till FTP-servern via FTP-klienten.

6.2.1 Användarlista

I användarlistan visas de användare som har lagts till och information om dem, till exempel användarnamn, delade kataloger och behörigheter. Du kan lägga till, redigera och ta bort användare.

Gör så här om du vill lägga till en användare i användarlistan:

1. Välj **USB-hantering > Användarinställningar**.

Sidan **Användarlista** visas.

2. Klicka på **Lägg till objekt**.
3. På sidan som visas anger du parametrar för användaren, till exempel användarnamn, lösenord, bekräftelselösenord, delad enhet, delad katalog och behörighet.
4. Klicka på **Spara**.

----Slut

Gör så här om du vill ändra en användare i användarlistan:

1. Välj **USB-hantering > Användarinställningar**.

Sidan **Användarlista** visas.

2. Klicka på **Redigera** i posten för den användare som ska ändras.
3. Ändra parameterinställningarna för användaren på sidan som visas.
4. Klicka på **Spara**.

----Slut

Gör så här om du vill ta bort en användare från användarlistan:

1. Välj **USB-hantering > Användarinställningar**.

Sidan **Användarlista** visas.

2. Klicka på **Ta bort** i posten för den användare som ska tas bort. Ett meddelande visas.
3. Klicka på **OK**.

----Slut

Gör så här om du vill ta bort alla användare från användarlistan:

1. Välj **USB-hantering > Användarinställningar**.

Sidan **Användarlista** visas.

2. Klicka på **Ta bort alla**. Ett meddelande visas.
3. Klicka på **OK**.

----Slut

6.3 FTP-hämtning

På den här sidan kan du hämta filer till en angiven katalog på USB-disken via FTP och visa hämtningshistoriken och statusen för den aktuella hämtningen.

6.3.1 Hämtningshistorik

På sidan **Hämtningshistorik** visas den föregående hämtningshistoriken och statusen på den aktuella hämtningen.

Gör så här för att lägga till en hämtningsuppgift:

1. Välj **USB-hantering > FTP-hämtning**.

Sidan **Hämtningshistorik** visas.

2. Klicka på **Hämtning** högst upp till höger på sidan.
3. Ställ in relaterade parametrar.
4. Klicka på **Spara**.

----Slut

7 System

7.1 Enhetsinformation

På den här sidan visas information om routern, till exempel namn, serienummer (SN), IMEI (International Mobile Equipment Identity), programversion och maskinvaruversion.

Gör så här för att visa systeminformation:

1. Välj **System > Enhetsinformation**.

Sidan **Enhetsinformation** visas.

2. Visa informationen på varje rad.

----Slut

7.2 Återställa

7.2.1 Starta om

Med den här funktionen startar du om routern när den inte är avslagen. Parameterinställningarna aktiveras först när routern har startats om.

Gör så här för att starta om routern:

1. Välj **System > Återställning**.

Sidan **Återställning** visas.

2. Klicka på **Starta om**. En dialogruta visas med en fråga om du vill starta om routern.
3. Klicka på **OK**. Routern startas om automatiskt.

----Slut

7.2.2 Återställ

Med den här funktionen återställer du parametrarnas standardvärden. När routern återställs ersätts de konfigurerade parametrarnas värden med standardvärden.

Gör så här för att återställa routern:

1. V äj **System > Återställning**.
Sidan **Återställning** visas.
 2. Klicka på **Återställ**. En dialogruta visas med en fråga om du vill återställa routern till fabriksinställningarna.
 3. Klicka på **OK**. Routern återställs till fabriksinställningarna.
- Slut

7.3 Säkerhetskopiering och uppdatering

Med den här funktionen säkerhetskopierar du konfigurationsfilen på datorn så att den säkerhetskopierade konfigurationsfilen kan användas till att återställa routern när routern inte fungerar som den ska.

7.3.1 Säkerhetskopiera

Gör så här för att säkerhetskopiera den befintliga konfigurationsfilen:

1. V äj **System > Säkerhetskopiering och uppdatering**.
Sidan **Säkerhetskopiering och uppdatering** visas.
 2. Klicka på **Säkerhetskopiera** på sidan **Säkerhetskopiera**. V äj namnet på konfigurationsfilen som ska säkerhetskopieras och sök vägen till platsen där den ska sparas i dialogrutan som visas. Klicka på **Spara**. Proceduren för filhänkning kan variera beroende på vilken webbläsare som används.
- Slut

7.3.2 Uppdatera

Gör så här för att uppdatera med den säkerhetskopierade konfigurationsfilen:

1. V äj **System > Säkerhetskopiering och uppdatering**.
Sidan **Säkerhetskopiering och uppdatering** visas.
 2. Klicka på **Bläddra** på sidan **Uppdatera**. V äj den säkerhetskopierade konfigurationsfilen i dialogrutan som visas.
 3. Klicka på **Öppna**. Dialogrutan stängs. Sök vägen och namnet på den säkerhetskopierade konfigurationsfilen visas i rutan till höger om **Konfigurationsfil**.
 4. Klicka på **Uppdatera**. En dialogruta visas med en fråga om du vill uppgradera programversionen.
 5. Klicka på **OK**. Routerna uppdateras med den säkerhetskopierade konfigurationsfilen. Efter uppdateringen startas routern om automatiskt.
- Slut

7.4 Uppgradera

7.4.1 Lokal uppgradering


Med den här funktionen uppgraderar du programvaran till den senaste versionen för att rätta till fel och få en mer stabil version. Uppgraderingen rekommenderas. Innan du uppgraderar måste du spara mÅprogramversionen på datorn.

Gör så här för att utföra en lokal uppgradering:

1. Välj **System > Uppgradera**.

Sidan **Uppgradera** visas.

2. Klicka på **Bläddra** på sidan **Loka uppgradering**. Välj filen med mÅprogramversionen i dialogrutan som visas.
3. Klicka på **Öppna**. Dialogrutan stängs. Sökvägen och namnet på filen med mÅprogramversionen visas i rutan till höger om **Uppgradera fil**.
4. Klicka på **Uppgradera**. En dialogruta visas med en fråga om du vill uppgradera programversionen.

 Under uppgraderingen ska du inte stänga av routern, koppla bort LAN:et eller koppla bort det trådlösa nätverket.

5. Klicka på **OK**. Programuppdateringen startar. När uppgraderingen är klar startas routern om automatiskt och den nya programversionen används.

----Slut

7.4.2 HTTP-uppgradering

Med den här funktionen uppgraderar du programvaran till den senaste versionen för att rätta till fel och få en mer stabil version. Uppgraderingen rekommenderas. Innan du uppgraderar måste du spara mÅprogramversionen på datorn.

Gör så här för att utföra en HTTP-uppgradering:


1. Välj **System > Uppgradera**.

Sidan **Uppgradera** visas.

2. Klicka på **Kontrollera** för att identifiera den senaste versionen.

Om...	Gör så här...
Den nya versionen identifieras.	Gå till 3.
Den nya versionen inte identifieras.	Uppgraderingen avslutas.

3. Klicka på **Uppdatera** för att hämta den nya versionen.
4. När hämtningen är klar utförs uppgraderingen automatiskt.
5. När uppgraderingen är klar startas routern om automatiskt. Ett meddelande om att uppgraderingen är klar visas. Därefter visas dialogrutan för inloggning.

 Använd inte routern under uppgraderingen.

- Om uppgraderingen misslyckas startas routern om automatiskt. Sedan visas ett meddelande med en uppmaning om att återställa routern till ursprungsversionen.

---Slut

7.5 Lösenordsändring

Med den här funktionen ändrar du admin-användarens inloggningslösenord. När lösenordet har ändrats måste det nya lösenordet användas vid nästa inloggning.

Gör så här för att byta lösenord:

- Välj **System > Lösenordsändring**.

Sidan **Lösenordsändring** visas.

- Ställ in **Nuvarande lösenord**, **Nytt lösenord** och **Bekräfta lösenord**. Det nya lösenordet och bekräftelselösenordet måste bestå av 6 till 15 ASCII-tecken.

- Klicka på **Spara**.

----Slut

7.6 Datum och tid

7.6.1 Inställningar

Du kan konfigurera systemtiden manuellt eller synkronisera systemtiden med nätverket. Om du väljer **Automatisk inställning med nätverkstiden** hämtar routern regelbundet tiden från servern för synkronisering. Om sommartid (DST) har aktiverats justerar routern systemtiden till sommartid.

Gör så här om du vill ange datum och tid manuellt:

- Välj **System > Datum och tid**.

Sidan **Inställningar** visas.

- Klicka på alternativknappen **Manuell inställning med lokal tid**.
- Ställ in **Lokal tid** eller klicka på **Tid från dator**.
- Klicka på **Spara**.

----Slut

Gör så här för att synkronisera tiden med nätverket:

- Välj **System > Datum och tid**.

Sidan **Inställningar** visas.

- Klicka på alternativknappen **Automatiskt inställning med nätverkstiden**.

3. Ställ in **Tidserver 1**. Det här är den primära servern för tidssynkronisering.
4. Ställ in **Tidserver 2**. Det här är den sekundära servern för tidssynkronisering.
5. Ställ in **Tidszon**. Olika länder och regioner har olika tidszoner. Välj en tidszon i listrutan.
6. Markera kryssrutan **Aktivera sommartid**.

Om sommartid (DST) har aktiverats måste sommartidens start- och sluttid konfigureras. Routern tillhandahåller automatiskt standardsommartiden för tidszonen. Du kan ställa in **Sommartid börjar**, **Sommartid slutar** och **Sommartidsförskjutning**.

7. Klicka på **Spara**.

----Slut

7.7 Diagnos

Om routern inte fungerar som den ska kan du använda diagnosverktygen på sidan **Diagnos** för att identifiera problemet så att åtgärder kan vidtas.

7.7.1 Ping

Om routern inte kan få åtkomst till Internet kör du kommandot ping för att identifiera problemet.

Gör så här för att köra kommandot ping och identifiera problemet:

1. Välj **System > Diagnos > På sidan Verktyg**, ange **Ping** som **Diagnos**-metod.
Sidans **Ping** visas.
2. Ange domännamnet i rutan **Mål-IP-adress eller domän**, till exempel www.google.com.
3. Ställ in **Paketstorlek** och **Timeout** och markera kryssrutan **Aktivera efter Fragmentera inte**.
4. Klicka på **Ping**.
5. Vänta tills ping-åtgärden har vidtagits. Kommandots resultat visas i rutan **Resultat**.

----Slut

7.7.2 Traceroute

Om routern inte kan få åtkomst till Internet kör du kommandot Traceroute för att identifiera problemet.

Gör så här för att köra kommandot Traceroute och identifiera problemet:

1. Välj **System > Diagnos > På sidan Verktyg**, ange **Traceroute** som **Diagnos**-metod.
Sidans **Traceroute** visas.
2. Ange domännamnet i rutan **Mål-IP-adress eller domän**, till exempel www.google.com.
3. Ställ in **Max. hopp** och **Timeout**.
4. Klicka på **Traceroute**.

5. Vänta tills Traceroute-åtgärden har vidtagits. Kommandots resultat visas i rutan **Resultat**.
----Slut

7.7.3 Systemkontroll

Om routern inte fungerar som den ska kan du använda verktyget för systemkontroll för att identifiera problemet.

Gör så här om du vill använda verktyget för systemkontroll för att identifiera problemet:

1. Välj **System > Diagnos > På sidan Verktyg**, ange **Systemkontroll** som **Diagnos**-metod
Sidan **Systemkontroll** visas.
2. Klicka på **Kontrollera**.
3. Vänta tills systemkontrollen har utförts. Möjliga orsaker visas på sidan.
4. Klicka på **Exportera** för att exportera detaljerad information till datorn. Om det behövs skickar du den detaljerade informationen till underhållspersonalen.

----Slut

7.8 Loggning

I loggarna registreras ändringar och viktiga händelser. Gör så här om du vill visa loggarna:

1. Välj **System > Logg**.
Sidan **Logg** visas.
2. Välj en loggnivå i listrutan **Loggnivå**. Antalet loggar på den här nivån visas till höger om listrutan och alla loggar visas i resultatrutan.
3. Välj åtgärd.
 - **Töm**: Tömmer alla loggar i routern.
 - **Exportera**: Exporterar alla loggar i routern till en fil i datorn.

----Slut

8

Frågor och svar

POWER-indikatorn är inte släckt.
<ul style="list-style-type: none"> • Kontrollera att strömkabeln är rätt ansluten och att routern har slagits på • Kontrollera att nätadaptern följer specifikationerna.
Samtal kan inte upprättas.
<ul style="list-style-type: none"> • Kontrollera att terminalerna fungerar och att kabelanslutningarna är korrekta. • Kontrollera att routern körs i LTE-läge. • Kontrollera att VoIP-tjänsterna har konfigurerats korrekt på webbhanteringssidan. <p>Kontakta behöriga lokala tjänstleverantörer om problemet kvarstår.</p>
Det går inte att logga in på webbhanteringssidan.
<ul style="list-style-type: none"> • Kontrollera att routern har startats. • Kontrollera att nätverkskabeln mellan routern och datorn är korrekt ansluten. • Kontrollera att rätt IP-adress har angetts för datorn. <p>Kontakta behöriga lokala tjänstleverantörer om problemet kvarstår.</p>
Routern kan inte identifiera det trådlösa nätverket.
<ul style="list-style-type: none"> • Kontrollera att nätadaptern är rätt ansluten. • Kontrollera att routern är placerad på en öppen plats på ordentligt avstånd från hinder som betong- eller träväggar. • Kontrollera att routern är placerad på ordentligt avstånd från elektriska hushållsapparater som genererar starka magnetfält, till exempel mikrovågsugnar, kylskåp och parabolantennor. <p>Kontakta behöriga lokala tjänstleverantörer om problemet kvarstår.</p>
Routerns nätadapter är överhettad.
<ul style="list-style-type: none"> • Routern överhettas om den används under lång tid. Stäng den för av routern när du inte använder den. • Kontrollera att ventilationen är god runt routern och att den inte är placerad i direkt solljus.
Parametrarna återställs till standardvärden.
<ul style="list-style-type: none"> • Om routern stängs av oavsett under konfigurationen kan parametrarna återställas till standardinställningarna. • Huawei rekommenderar att du exporterar parameterinställningarna när du har ställt in parametrarna, så att du snabbt kan återställa routern till den föregående statusen med hjälp av de exporterade inställningarna.

9 Akronymer och förkortningar

ACL	Access Control List, åkomstkontrollista
AES	Advanced Encryption Standard
ALG	Application Layer Gateway
AP	Access Point, åkomstpunkt
CPE	Customer-Premises Equipment, kundutrustning
CWMP	CPE WAN Management Protocol
DDNS	Dynamic Domain Name Server
DDoS	Distributed Denial of Service, samordnad överbelastningsattack
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Server/Domain Name System
DoS	Denial-of-Service, överbelastningsattack
DST	Daylight Saving Time, sommartid
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IMEI	International Mobile Station Equipment Identity
IP	Internet Protocol
IPSec	Internet Protocol Security
ISP	Internet Service Provider
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control

MTU	Maximum Transmission Unit
NAT	Network Address Translation
NTP	Network Time Protocol
PBC	Push Button Configuration, tryckknappskonfiguration
PIN	Personal Identification Number
PKM	Privacy Key Management
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
RIP	Routing Information Protocol
RTSP	Real Time Streaming Protocol
QoS	Quality of Service
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SN	Serial Number
SNTP	Simple Network Time Protocol
SSID	Service Set Identifier
SSH	Secure Shell
SYN	Synchronous Idle
TKIP	Temporal Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA	WiFi Protected Access
WPA-PSK	WiFi Protected Access-Pre-Shared Key
WPS	WiFi Protected Setup