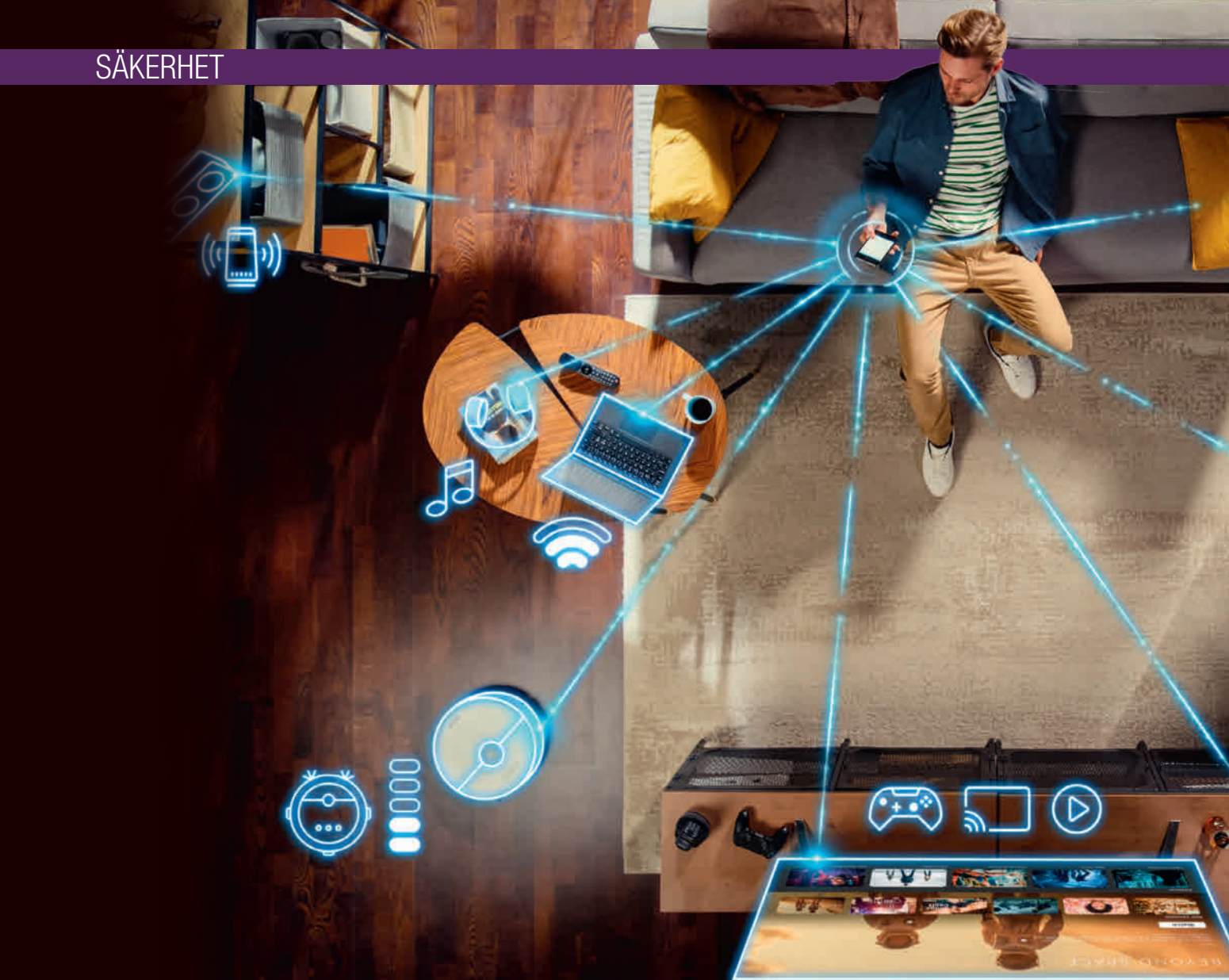




FÖREBYGG ATTACKER MOT DITT NÄTVERK

Testa att all din utrustning är säker

Det räcker inte att bara skydda datorn och mobilen mot attacker på nätet. Alla enheter som är anslutna till internet kan vara i riskzonen, så ge all din utrustning en säkerhetskontroll redan idag.



Säkerhetskolla ditt hem

Har du enheter som kan vara i riskzonen för attacker? I listan kan du se exempel på enheter som bör skyddas.

- Sonos och andra smarta högtalare
- Nätverkskameror
- Skrivare som är anslutna till nätverket
- TV-boxar som Google TV och Apple TV
- App-styrda stickkontakter
- Smart belysning
- Nätverkshårddiskar (NAS)
- Smarta TV-apparater
- Trådlösa routrar
- Hubbar för gardiner, termostater och belysning
- Spelkonsoler
- Smarta dörrklockor
- Robotdammsugare
- App-styrda dörrlås
- Vitvaror som har inbyggd Wi-Fi
- Väderstationer med nätverksåtkomst



Journalist
Henning Rasmussen

Det kan tyckas orimligt att kassera elektronik som fortfarande fungerar och som du kanske använder. Det kan dock bli nödvändigt om utrustningen är ansluten till internet men inte får nödvändiga säkerhetsuppdateringar från tillverkaren.

Farliga säkerhetshål

Säkerhetsexperten och producenter upptäcker ständigt nya möjligheter att få obehörig åtkomst till enheter som är anslutna till hemnätverket, men det gör tyvärr också kriminella. Sårbarheter åtgärdas ofta genom att tillverkaren släpper uppdateringar av inbyggda programvaran för enheter som uppkopplade kontakter, nätverks-

hårddiskar och -kameror. Tyvärr är det få tillverkare som fortsätter att uppdatera osäkra enheter även efter att de har passerat femårsgränsen många tillverkare har för utveckling av uppdateringar.

Fick kassera dyra kameror

Jag var själv tvungen att inse detta på ett smärtsamt sätt. Under många år hade jag tre dyra nätverkskameror från tillverkaren D-Link installerade i mitt hem, och trots att de var över tio år gamla fungerade de fortfarande perfekt. Jag upptäckte dock på deras administrationssidor i webbläsaren att den senaste uppdateringen från tillverkaren var sju år gammal. Med andra ord hade brottslingar haft sju år på sig att hitta ett säkerhetshål i tusentals kameror som mina. Det var med tungt hjärta jag bestämde mig

för att kassera kamerorna, trots att de kanske hade kunnat fungera i flera år till. Du kanske också har gammal utrustning i ditt hem?

Det finns flera saker du kan göra för att skydda dina enheter. Börja med att kontrollera att de har bra lösenord som du och inte tillverkaren har valt. Du kan också se till att det inte finns onödiga portar öppna i din router och att all utrustning är uppdaterad med sin senaste firmware.

Om du är osäker på vilka enheter som är anslutna till nätverket kan du börja med att använda programmet Advanced IP Scanner. Det kommer att avslöja alla enheter i nätverket och visa varje ansluten enhets IP-adress, som du behöver för att komma åt den med webbläsaren. Sedan är du redo att följa våra enkla instruktioner för att skydda alla enheter i ditt nätverk.



BONNIE PC Advanced IP Scanner

Programmet genomsöker hela nätverket och visar sedan alla enheter som är anslutna till det.

Språk
Svenska

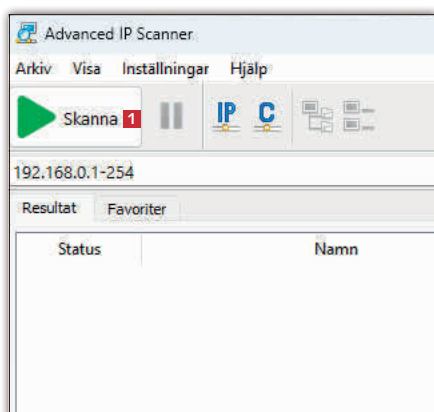
Fungerar med
Windows 10 och 11

Hämta programmet på vår hemsida:
pctidningen.se/2511

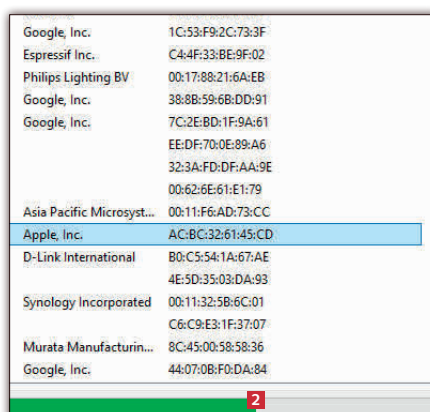


Börja med att hitta alla enheter i nätverket

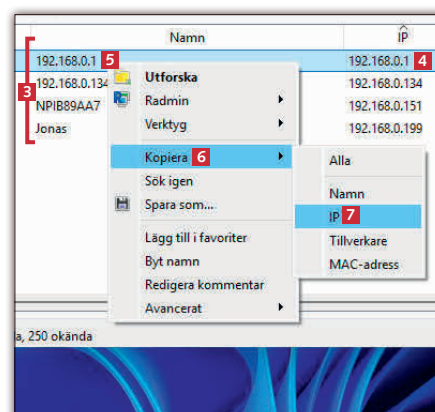
Du behöver känna till IP-adresserna för dina enheter så att du kan logga in och kontrollera deras säkerhet. Du kan enkelt hitta adresserna med Advanced IP Scanner.



1 Hämta Advanced IP Scanner från vår hemsida och installera programmet. När du startar det klickar du på **Skanna** 1 uppe till vänster.



2 Vänta medan hela nätverket genomsöks. Skanningen är klar när den gröna linjen når hela vägen till fönstrets kant 2.

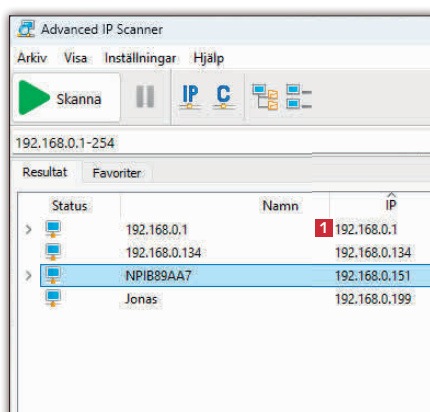


3 Alla enheter visas 3 med sina IP-adresser 4. Högerklicka på en enhet 5, välj **Kopiera** 6 och **IP** 7. Klistra in den i din webbläsare.

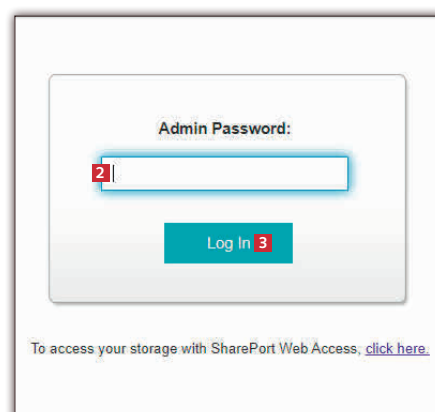


Uppdatera din router

Din trådlösa router är direktansluten till internet, så det är väldigt viktigt att du håller den uppdaterad med tillverkarens senaste firmware.



1 Öppna Advanced IP Scanner och undersök nätverket. Längst upp i listan över upptäckta enheter visas din router och dess IP-adress 1, som du behöver i nästa steg.

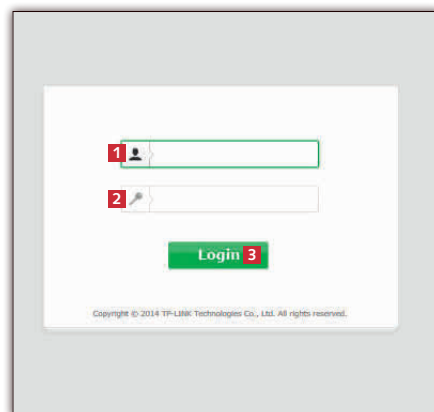


2 Öppna din webbläsare och skriv in routerns adress i adressfältet. Tryck på **Retur**. Ange lösenordet för routerns administrationssidor 2 och klicka på **Log In** 3.

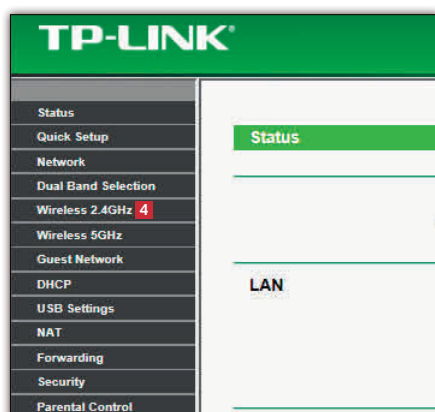


Välj den starkaste krypteringen

Den trådlösa anslutningen mellan din enhet och din router skyddas med kryptering, som finns i olika versioner. Se till att du väljer den nyaste och säkraste standarden.



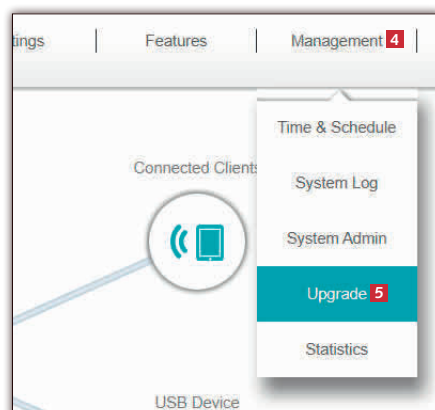
1 Öppna en webbläsare och skriv routerns IP-adress i adressfältet. Tryck på **Retur**. Fyll i namn **1** och lösenord **2** till routern administrations-sidor. Klicka på **Login** **3**.



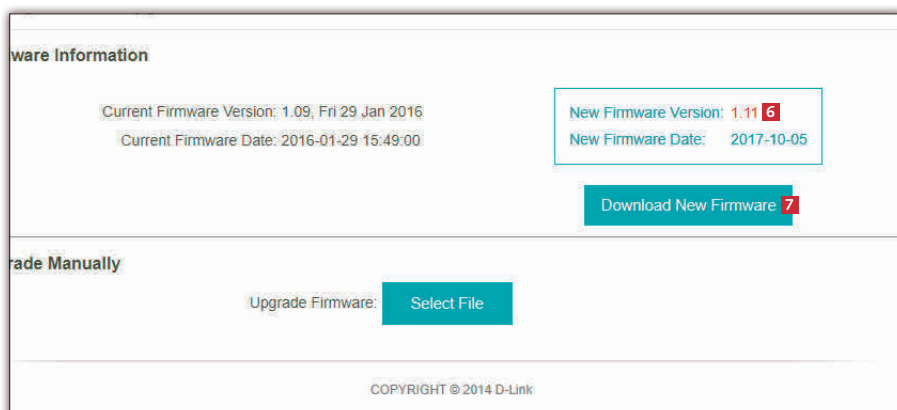
2 Klicka på **Wireless 2.4GHz** **4** för att ändra inställningarna för det trådlösa 2,4 GHz-nätverket.



3 Klicka på **Wireless Security** **5**. Markera **WPA/WPA2 Personal** **6** eller WPA3 om det finns tillgängligt. Välj **Automatic** **7**, **AES** **8**, och ett lösenord som inte kan gissas av andra **9**. Klicka på **Save**. Nu kommer din router att starta om, och när den är igång igen måste du logga in på nätverket igen med alla dina enheter. Upprepa processen för ditt 5GHz-nätverk.



3 I den här routern ska man klicka på **Management** **4** och välja **Upgrade** **5**. Det kan också heta **Advanced** eller **Firmwareuppgade** på andra modeller.



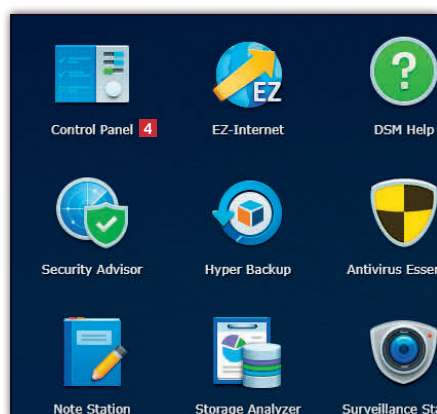
4 Här kan du se om det finns en ny firmwareversion för din router **6**. Klicka på **Download New Firmware** **7** för att hämta och installera den. Efter installationen, kontrollera igen om du har den senaste versionen av firmware.



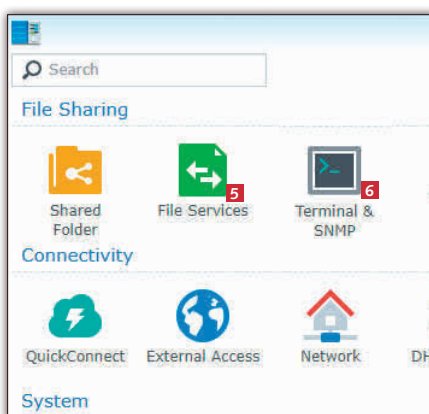


Stäng de öppna portarna i din NAS

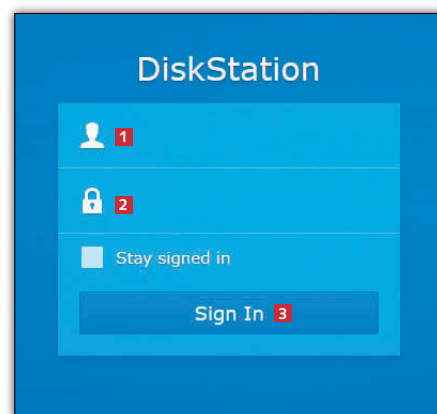
En modern nätverkshårddisk (NAS) har många andra funktioner än att bara lagra dina filer. Därför bör du kontrollera att portarna är stängda för funktioner som du inte använder.



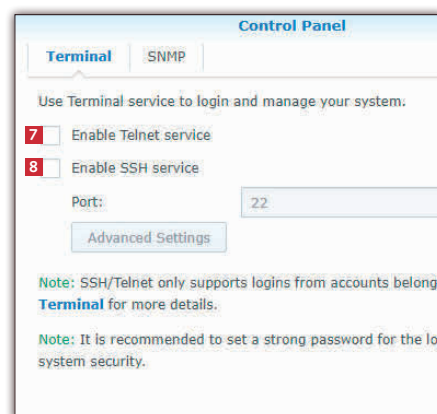
2 Klicka på **Control Panel** **4**. Den ser olika ut och har olika namn beroende på NAS-enhetens modell och märke, här är det en enhet som kommer från Synology.



3 Enhetens öppna portar kan vanligtvis hittas antingen under **File Services** **5** eller **Terminal & SNMP** **6**.



1 Hitta adressen till din NAS med Advanced IP Scanner. Öppna en webbläsare och gå till adressen. Mata in användarnamn **1** och lösenord **2**. Klicka på **Sign In** **3**.

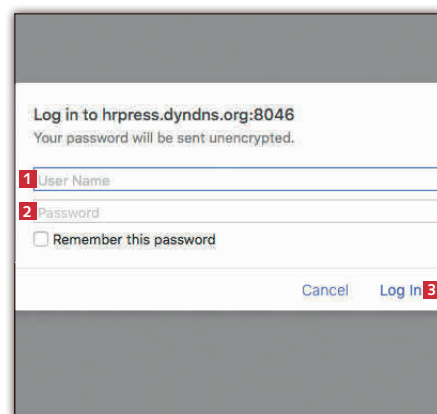


4 Ta bort markeringarna vid **Enable Telnet service** **7** och **Enable SSH service** **8** om du inte använder de funktionerna. Klicka sedan på **OK**.



Uppdatera med starkare lösenord

När du köper ny utrustning är den vanligtvis skyddad med ett standardlösenord från tillverkaren. Du bör ändra den till ett bra och starkt lösenord som du själv väljer. Här visar vi hela processen med en IP-kamera.

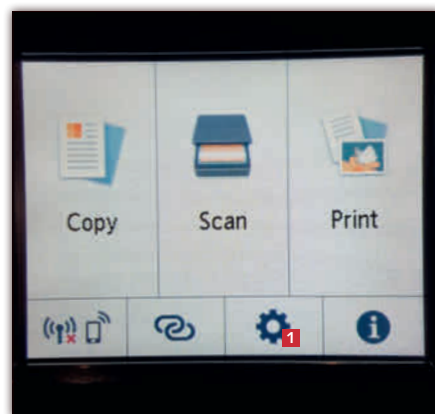


1 Leta reda på kamerans adress med Advanced IP Scanner och ange den i webbläsarens adressfält. Mata in användarnamn **1** och lösenord **2**. Klicka på **Log in** **3**.

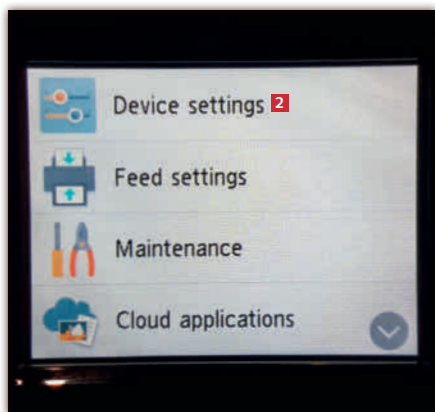


Uppdatera manuellt

Det är inte alla utrustningar som regelbundet och automatiskt uppdateras av tillverkaren. Därför bör du själv med jämna mellanrum kontrollera om det finns nya uppdateringar. Det gäller även din skrivare om den är ansluten till nätverket.



1 På en nyare Canon-skrivare med trådlös internetuppkoppling ser huvudmenyn på skrivarens lilla skärm ut så här. Här måste du trycka på kugghjulet **1**.



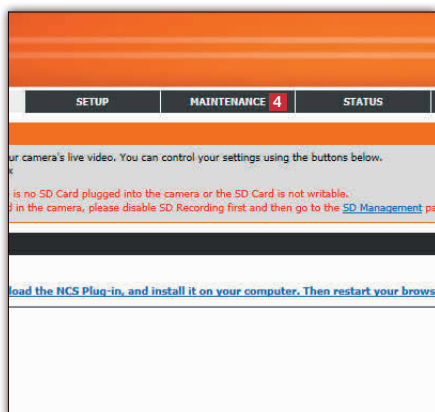
2 Välj alternativet **Device settings** **2**.



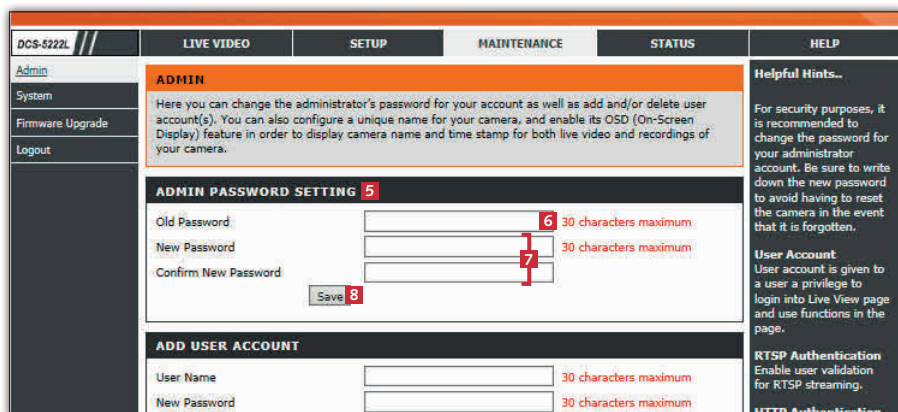
3 Bläddra ner till botten av menyn och tryck på alternativet **Firmware update** **3**.



4 Tryck på **Install update** **4** och följ guiden för att uppdatera skrivaren med den senaste inbyggda programvaran och minimera risken för attacker mot skrivaren från internet.



2 Här tittar vi på en IP-kamera från D-Link. Sidorna ser olika ut från tillverkare till tillverkare. För D-Link-utrustning behöver du först klicka på knappen **Maintenance** **4**.



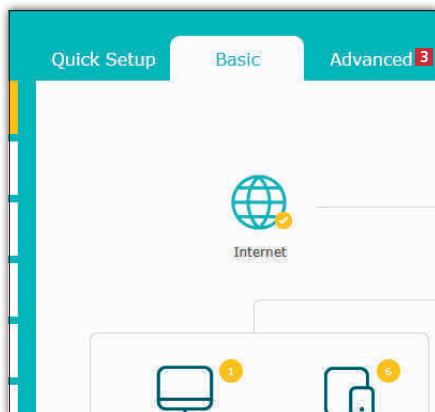
3 Under **Admin password setting** **5** behöver du först mata in det gamla lösenordet **6**. Skriv sedan in det nya lösenordet två gånger **7**. Klicka sedan på **Save** **8** för att spara de nya inställningarna.



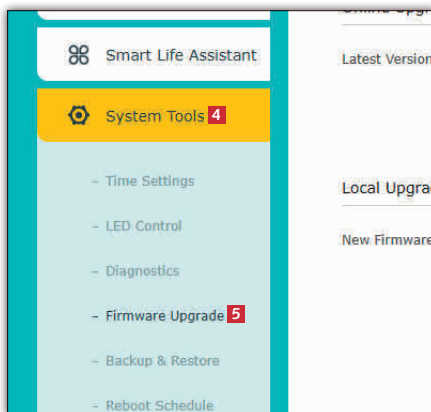
TEST 6

Uppdateras inte dina enheter längre?

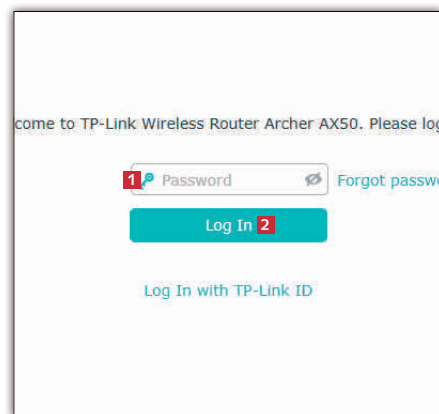
På enheternas administrationssidor kan du vanligtvis se när den senaste versionen av firmware installerades. Om det har gått mer än fem år bör du starkt överväga att kassera utrustningen för att eliminera attackrisken. Här är det en router från TP-Link.



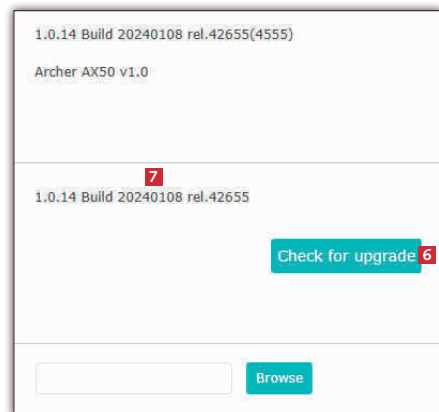
2 På en del enheter måste du först klicka på **Advanced** **3** för att se detaljer om den installerade versionen av firmware.



3 Klicka på **System Tools** **4** eller liknande, och välj sedan **Firmware Upgrade** **5**.



1 Leta reda på enhetens adress i Advanced IP Scanner. Skriv adressen i webbläsarens adressfält och tryck på **Retur**. Mata sedan in lösenordet **1** och klicka på **Log in** **2**.



4 Klicka på knappen **Check for upgrade** **6**. Här datumet **7** för programvaran. Om datumet är före 2020 är det osannolikt att din enhet kommer att få fler uppdateringar.

Överväg att kassera gammal utrustning

Det har gått 10-15 år sedan smarta enheter för övervakning och styrning av sådant som belysning och värme började användas. Som ett resultat av detta har många enheter nått en ålder där tillverkaren inte längre uppdaterar dem. Det gäller kanske även enheter som du har i ditt hem om du har ägt dem i ett antal

år. Tyvärr är många sårbarheter så djupt rotade att det bara är en helt ny firmware från tillverkaren som kan åtgärda dem. Det är därför som i synnerhet nyare märkesprodukter ofta uppdateras när nya sårbarheter upptäcks. Det är annorlunda med äldre utrustning eller importerade kinesiska produkter. Därför har du egentligen som bäst två alternativ om enheter inte längre får några nya

uppdateringar: kassera utrustningen och köp modernare alternativ, eller möjligtvis koppla bort enheten från ditt nätverk/internet och använda den lokalt hemma, om det är möjligt.



Om du har en smart högtalare kanske du upptäcker att tiden då du kunde hämta nya uppdateringar är förbi sedan länge.

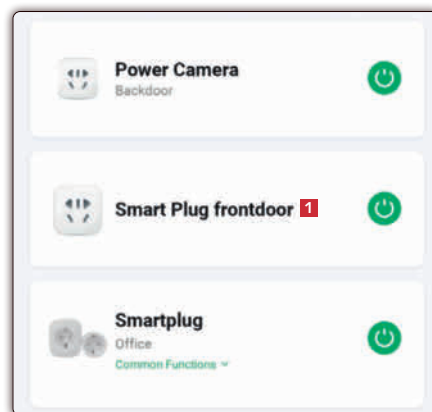
Många nätverkskameror, som den här från D-Link, får inte längre uppdaterad firmware. Det innebär att eventuella säkerhetshål inte längre täpps till.



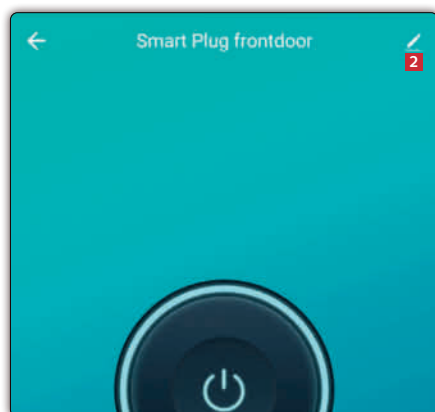


Uppdatera med hjälp av en app

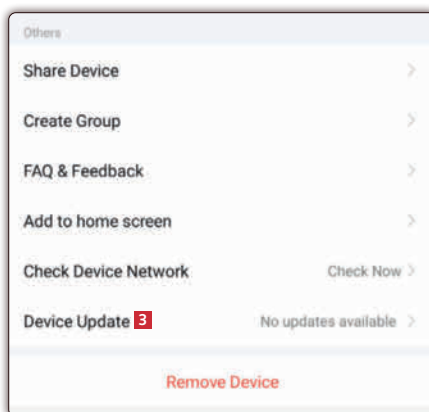
Mycket av dagens utrustning för smarta hem kan bara styras från en app i mobilen. Därför kan det också vara från den appen som du måste söka efter och installera uppdateringar till utrustningen.



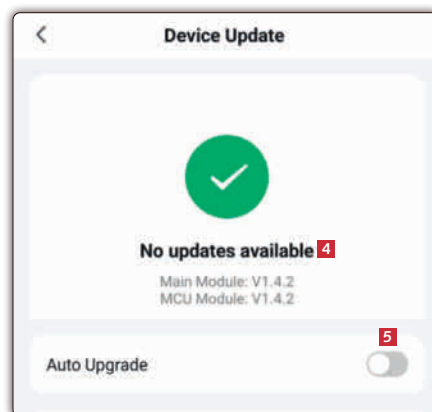
1 Om din enhet bara kan styras av en app öppnar du motsvarande app. Om den hanterar mer än en enhet trycker du på den relevanta enheten i appens översikt **1**.



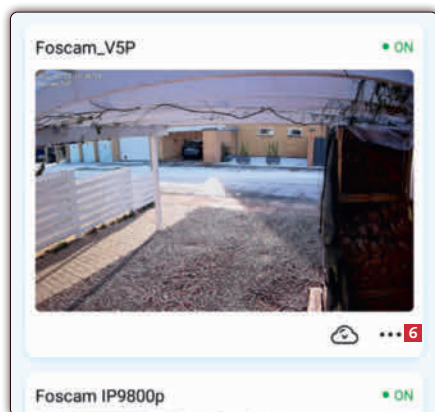
2 Gå vidare till enhetens inställningar **2**.



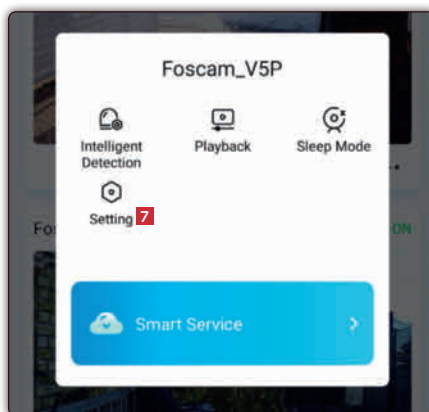
3 Tryck på **Device Update** **3** eller motsvarande.



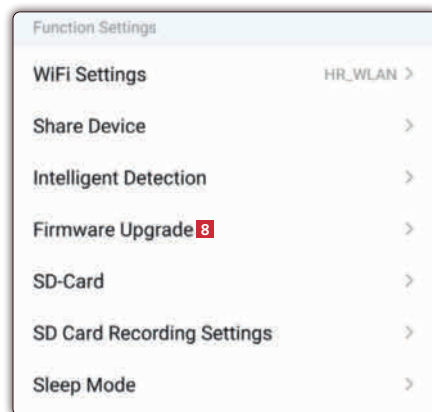
4 Här kan du se om det finns nya uppdateringar för din enhet **4**. Du kan också ofta konfigurera din enhet att automatiskt hämta och installera nya uppdateringar **5**.



5 Om din enhet är en appstyrd nätverkskamera klickar du vanligtvis på de tre punkterna under kamerabilden **6**. Här handlar det om en kamera från Foscam.



6 Klicka sedan på **Setting** **7**.



7 Välj **Firmware Upgrade** **8** i menyn. Härifrån kan du både uppdatera kameran och se när den senaste uppdateringen installerades.