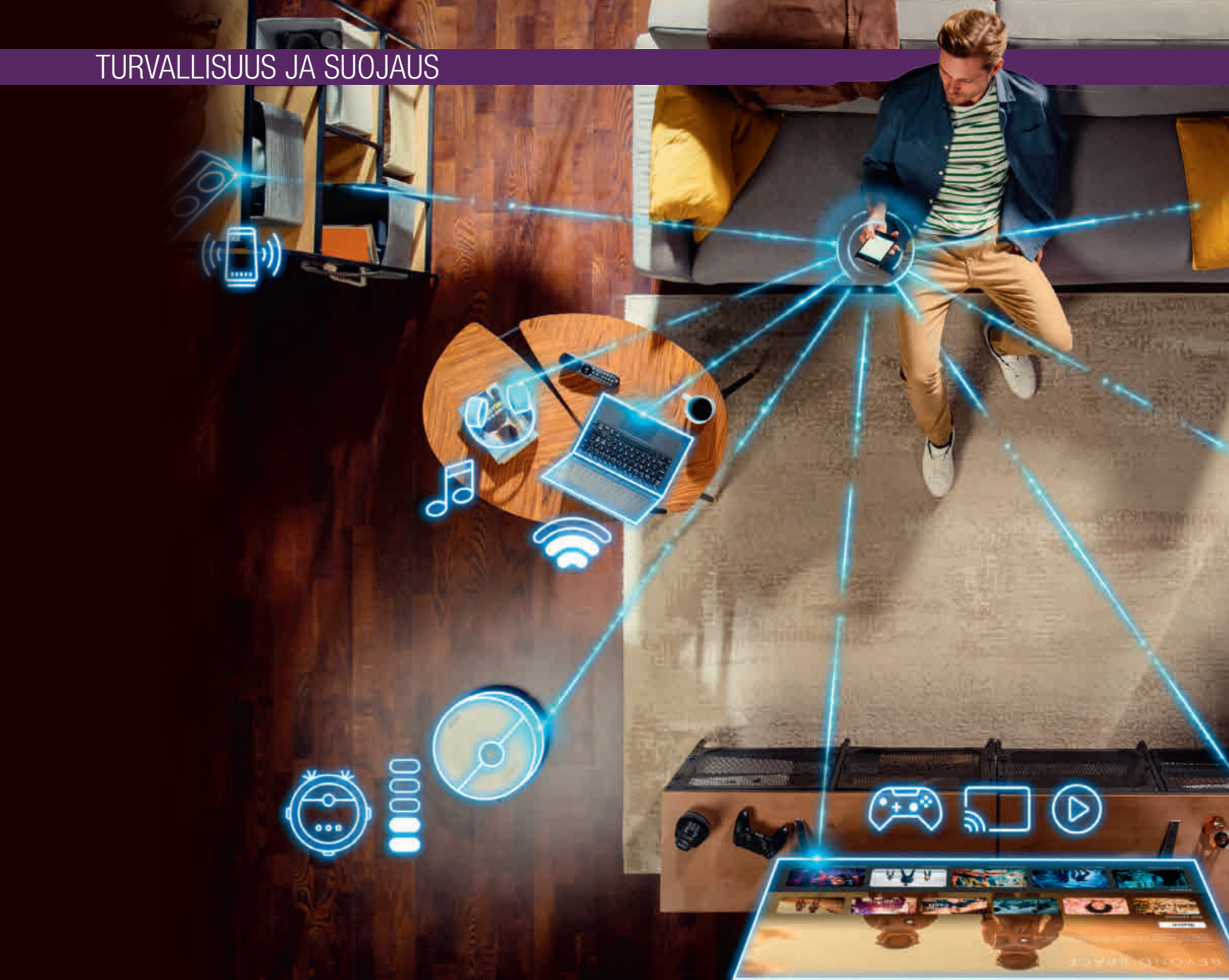




TORJU VERKKOOSI KOHDISTUVAT HYÖKKÄYKSET:

Suojaa kaikki kotisi laitteet

Tietokoneen ja puhelimen suojaaminen verkkohyökkäyksiltä ei riitä, sillä kaikki verkkoon liitetyt laitteet voivat olla vaarassa. Tarkista siis kaikkien laitteidesi suojaus jo tänään.



Tarkista kotisi tietoturva

Käytätkö laitteita, joihin voi kohdistua verkkohyökkäyksiä? Alla on luettelo laitteista, jotka tulisi suojata.

- Sonos tai muut älykaiuttimet
- Verkkokamerat
- Verkkoon liitetyt tulostimet
- TV-boksit, esimerkiksi Google TV ja Apple TV
- Älypistorasiat
- Älyvalaisimet
- Verkkolevypalvelin (NAS)
- Äly-TV-laitteet
- Langaton reititin
- Tukiasemat lämmityksen tai valaistuksen ohjaukseen
- Pelikonsolit
- Älykäs ovikello
- Robotti-imurit
- Älyovilukko
- Laitteet, joissa on sisäänrakennettu Wi-Fi
- Verkkoon liitetty sääasema



Toimittaja
Henning Rasmussen

Toimivan ja käyttökelpoisen elektroniikan hävittäminen saattaa tuntua kohtuuttomalta. Saatat kuitenkin joutua tähän tilanteeseen, jos laite on liitetty verkkoon eikä sen valmistaja tarjoa enää sille elintärkeitä tietoturvapäivityksiä.

Vaaralliset tietoturva-aukot

Tietoturva-asiantuntijat, valmistajat ja valitettavasti myös rikolliset keksivät jatkuvasti uusia tapoja päästä luvattomasti käsiksi kotiverkkoihin liitettyihin laitteisiin. Haavoittuvuudet korjataan usein siten, että valmistaja julkaisee laiteohjelmistopäivityksen esimerkiksi älykytkimille, verkkovalevyille ja verkkokameroille.

Valitettavasti vain ani harvat valmistajat jatkavat tietoturvallisten laitteiden päivittämistä sen jälkeen, kun niiden käyttöikä on ylittänyt viiden vuoden rajan.

Kallis kamera roskeen

Opin tämän tuskallisen totuuden kantapään kautta. Minulla oli monta vuotta kotonani kolme kallista D-Link-valmistajan verkkokameraa. Vaikka ne olivat yli kymmenen vuotta vanhoja, ne toimivat täydellisesti. Huomasin kuitenkin kameroiden ohjaussivuilla selaimessa, että valmistajan viimeisin päivitys oli seitsemän vuotta vanha. Toisin sanoen rikollisilla oli ollut seitsemän vuotta aikaa löytää tietoturva-aukko tuhansissa kameroissa, kuten minun kameroissani. Niinpä päätin raskain mielin luopua kameroistani, vaikka ne olisivat todennä-

köisesti olleet toimintakuntoisia vielä useiden vuosien ajan. Ehkä siunallakin on tällainen tilanne edessä.

Kotien laitteet voi suojata monilla eri tavoilla. Aloita tarkistamalla, että laitteisiin pääsy on suojattu vahvalla salasanalla, jonka sinä olet valinnut – eikä valmistaja. Varmista myös, ettei reitittimessäsi ole tarpeettomia portteja auki ja että kaikkiin laitteisiin on päivitetty niiden laiteohjelmiston uusin versio.

Ellet ole varma, mitkä kotisi laitteet ovat liitettyinä verkkoon, aloita skannaamalla verkkosi Advanced IP Scannerilla. Ohjelma paljastaa kaikki kotiverkossasi olevat laitteet ja niiden IP-osoitteet, joita tarvitset voidaksesi käyttää laitteitasi selaimen kautta. Sitten oletkin valmis suojaamaan kaikki kotisi laitteet seuraamalla yksinkertaisia ohjeitamme.





Advanced IP Scanner

Ohjelma skannaa koko verkkosi ja näyttää kaikki verkkoon liitetyt laitteet.

Kieli
Suomi

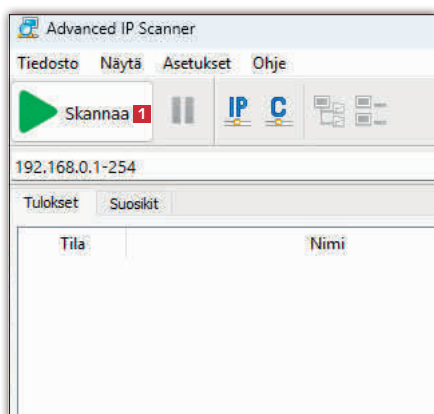
Järjestelmä
Windows 10 ja 11

Lataa ohjelma verkkosivuilta:
kotimikro.fi/2511

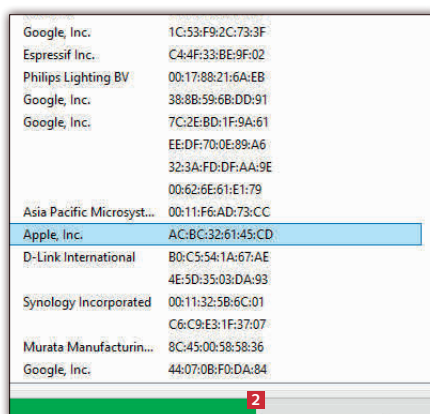


Aloita etsimällä kaikki kotiverkkosi laitteet

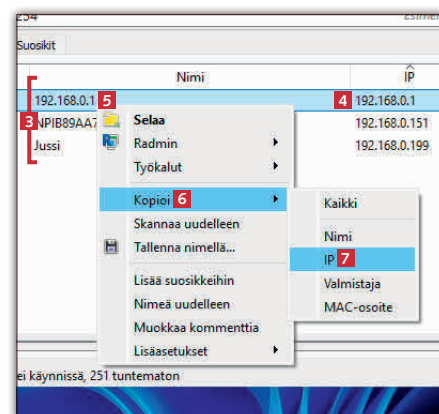
Sinun on tiedettävä laitteidesi IP-osoitteet, jotta voit kirjautua niihin sisään ja tarkistaa niiden tietoturvan. Löydät osoitteet helposti Advanced IP Scannerilla.



1 Lataa Advanced IP Scanner verkkosivuiltamme ja asenna ohjelma. Kun avaat ohjelman, valitse vasemmasta yläkulmasta **Skannaa** **1**.



2 Odota kunnes koko verkko on skannattu. Prosessi on valmis, kun vihreä viiva ulottuu koko ikkunan alareunan poikki **2**.

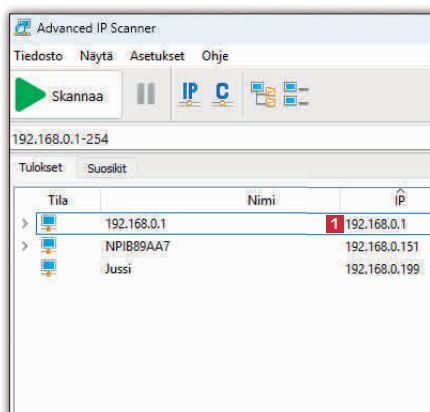


3 Laitteet **3** IP-osoitteineen **4** näytetään. Napsauta laitetta hiiren oikealla painikkeella **5** ja valitse **Kopioi** **6** sekä **IP** **7**. Liitä osoite selaimen osoiteriville.

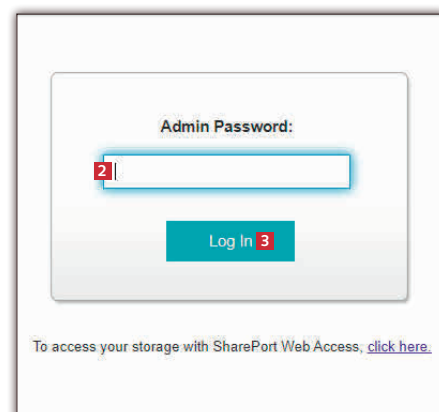


Päivitä reitittimesi

Langaton reitittimesi on suoraan yhteydessä verkkoon, joten on tärkeää pitää se ajan tasalla päivitettyinä valmistajan uusimmalla laiteohjelmistolla.



1 Avaa Advanced IP Scanner ja skannaa tietokone. Havaittujen laitteiden luettelon yläreunassa näet reitittimesi ja sen IP-osoitteen **1**. Tarvitset sen seuraavassa vaiheessa.

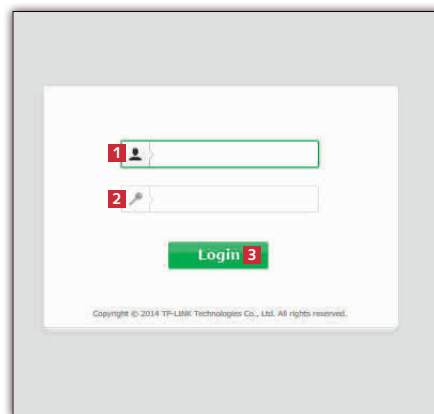


2 Avaa selain ja kirjoita reitittimen osoite osoiteriville. Paina sitten **Enter**-näppäintä. Syötä vielä reitittimen salasana **2**. Sen valitset sinä tai valmistaja. Valitse sitten **Log In** **3**.

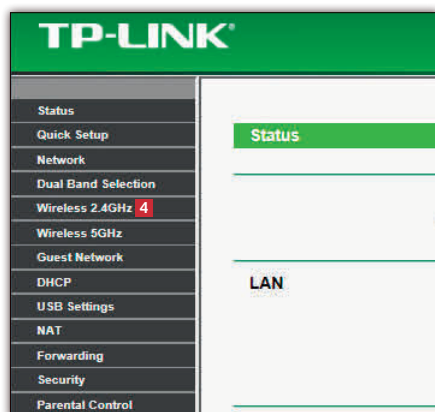


Valitse vahvin salaus

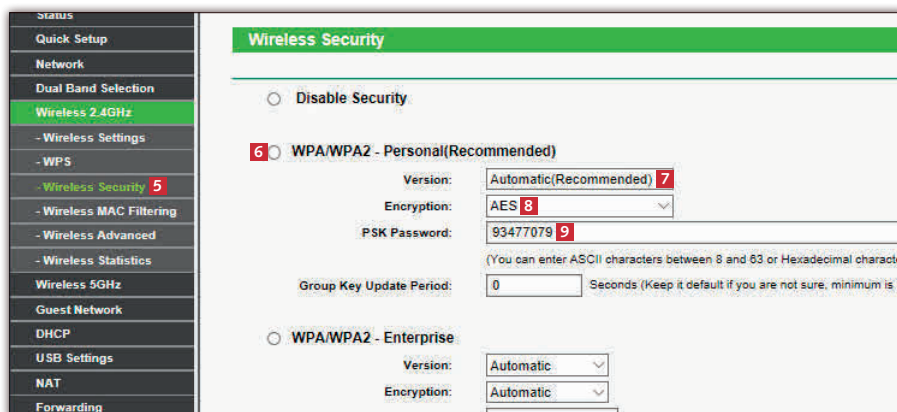
Laitteesi ja reitittimen välinen langaton yhteys on suojattu salauksella, josta on saatavana eri versioita. Varmista vain, että valitset aina uusimman ja turvallisimman standardin.



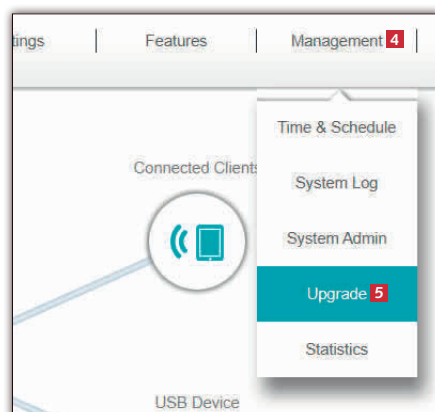
1 Avaa selain ja kirjoita reitittimen osoite osoitekenttään. Paina **Enter**. Syötä reitittimen käyttäjänimi **1** ja salasana **2** (joka on käyttäjäoppaassa). Valitse sitten **Login 3**.



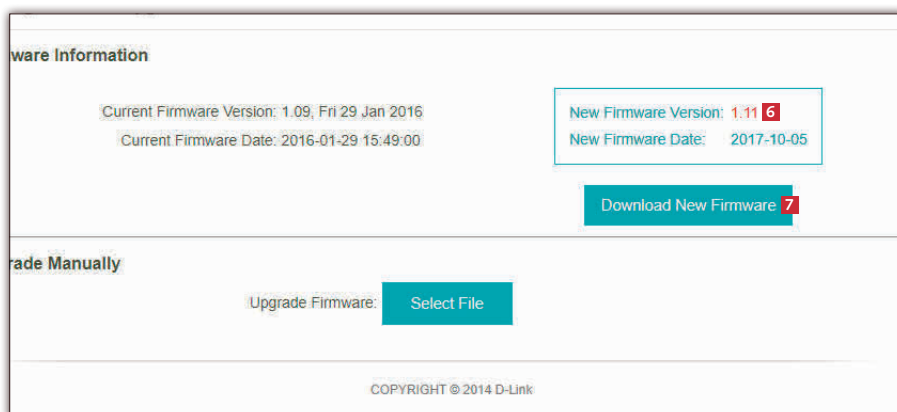
2 Muuta 2,4 GHz:n langattoman verkon asetuksia valitsemalla valikosta **Wireless 2.4GHz 4**.



3 Valitse **Wireless Security 5**. Merkitse **WPA/WPA2 Personal 6** tai WPA3, jos se on käytettävissä. Valitse **Automatic 7**, **AES 8** ja syötä koodi, jota muut eivät voi helposti arvata. **9**. Valitse **Save**. Nyt reitittimesi käynnistyy uudelleen. Kun se on käynnissä, kirjaudu takaisin verkkoon kaikilla laitteillasi. Toista prosessi myös 5GHz-verkon kanssa.



3 Valitse tässä reititinmallissa **Management 4** ja sitten kohta **Upgrade 5**. Muissa malleissa asetuksen nimi voi olla vaikkapa **Advanced** tai **Firmware Upgrade**.



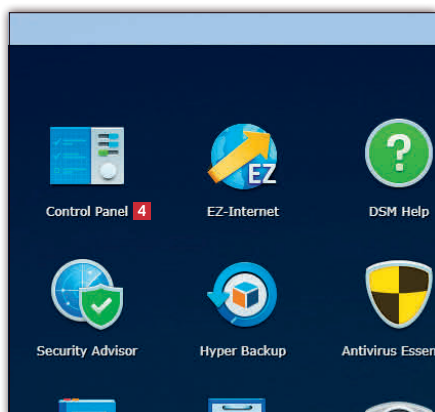
4 Täältä näet, onko reitittimellesi julkaistu uusi laiteohjelmisto **6**. Lataa ja asenna päivitys valitsemalla **Download New Firmware 7**. Tarkista asennuksen jälkeen uudelleen, onko käytössäsi uusien laiteohjelmisto.



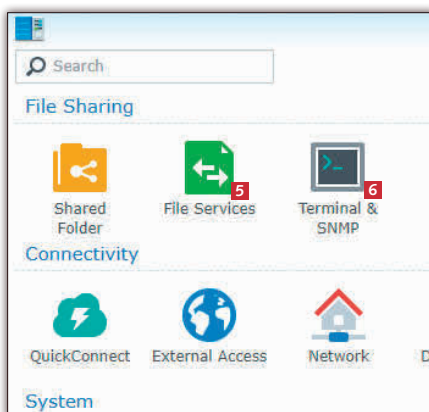


Sulje NAS-palvelimen avoimet portit

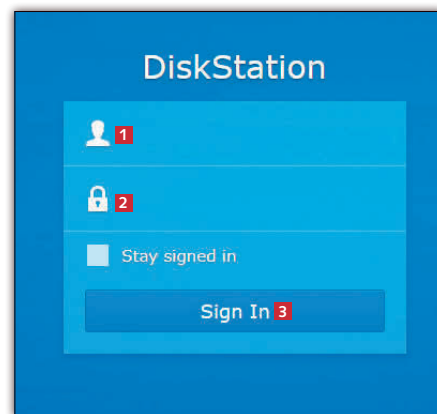
Moderneilla verkkolevypalvelimilla (NAS) on paljon muitakin ominaisuuksia kuin tiedostojen tallentaminen. Siksi kannattaakin tarkistaa, ovatko NAS:n palvelintoimintojen portit suljettu.



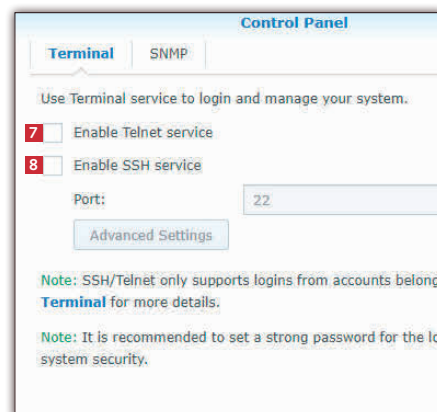
2 Etsi NAS:n ohjauspaneeli eli **Control Panel** **4**. Se näyttää erilaiselta ja voi olla eri niminen mallista ja merkistä riippuen. Tässä esimerkissä malli on Synology.



3 NAS:n avoimet portit löytyvät yleensä joko kohdasta **File Services** **5** tai **Terminal & SNMP** **6**.



1 Etsi NAS:n osoite Advanced IP Scannerilla. Avaa selain ja syötä osoite. Paina **Enter**. Anna sitten käyttäjätunnus **1** ja salasana **2**. Valitse seuraavaksi **Sign in** **3**.

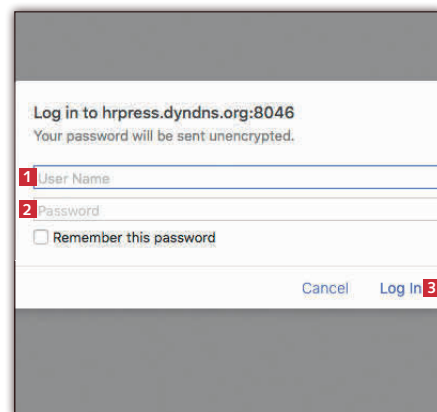


4 Poista valinta ruuduista **Enable Telnet services** **7** ja **Enable SSH service** **8**, jos et käytä niitä aktiivisesti. Valitse sitten **Käytä**. Riski on nyt eliminoitu.



Laadi vahvempia salasanoja

Kun ostat uuden laitteen, se on yleensä suojattu valmistajan luomalla salasanalla. Sinun kannattaakin vaihtaa se itse valitsemaasi hyvään ja vahvaan salasanaa. Näin vaihdat verkkokamerasi salasanan itse.

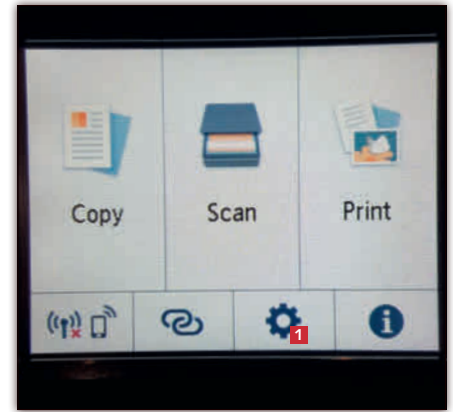


1 Etsi verkkokamerasi osoite Advanced IP Scannerilla ja syötä se selaimesi osoiteriville. Paina sitten **Enter**. Kirjoita käyttäjätunnus **1** ja salasana **2**. Valitse **OK** **3**.



Muista päivittää kaikki laitteesi

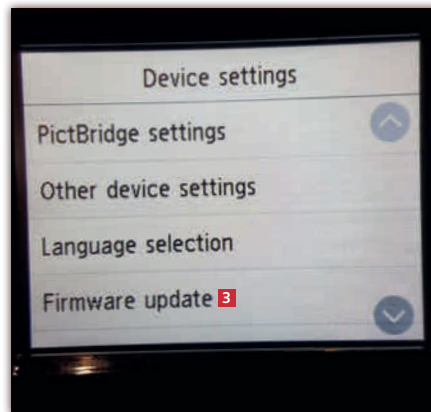
Valmistajat eivät päivitä kaikkia laitteitaan automaattisesti ja jatkuvasti. Siksi sinun on tarkistettava säännöllisesti itse, onko uusia päivityksiä saatavilla. Näin on toimittava myös silloin, kun tulostimesi on liitetty verkkoon.



1 Uudemmassa Canon-tulostimessa, jossa on langaton verkkoyhteys, tulostimen pienen näytön päävalikko näyttää tältä. Paina hammasratasta **1**.



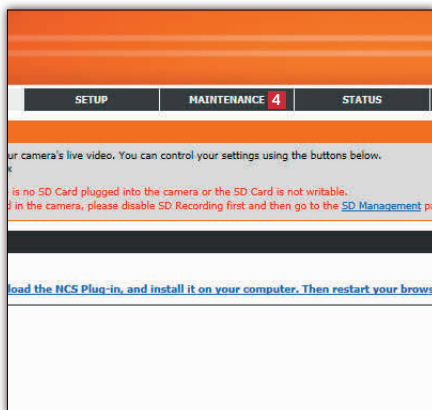
2 Valitse seuraavaksi kohta **Device settings** **2**.



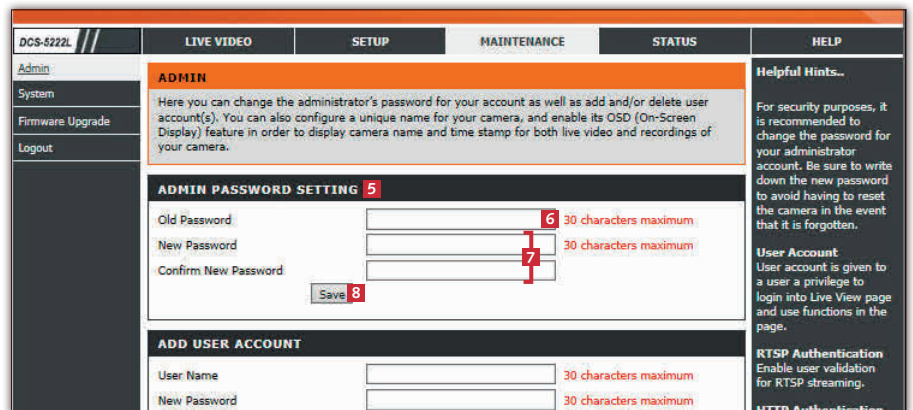
3 Selaa valikon alareunaan ja valitse **Firmware update** **3**.



4 Valitse **Install update** **4** ja päivitä tulostimen laiteohjelmisto ohjatulla toiminnolla. Tämä minimoi tulostimeesi kohdistuvien verkkohyökkäysten riskin.



2 Tässä tarkastelemme D-Linkin IP-kameraa. Eri valmistajien laitteiden sivut näyttävät erilaisilta. D-Linkin laitteen ollessa kyseessä valitse **Maintenance** **4**.



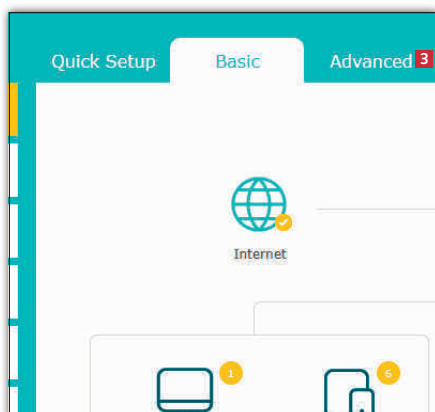
3 Kirjoita kohtaan **Admin password setting** **5** laitteen vanha salasana **6**. Syötä sitten uusi salasana alla oleviin kenttiin kahteen kertaan **7**. Tallenna uusi salasanasasi valitsemalla **Save** **8**. Olet nyt vaikeuttanut laitteeseesi murtautumista.



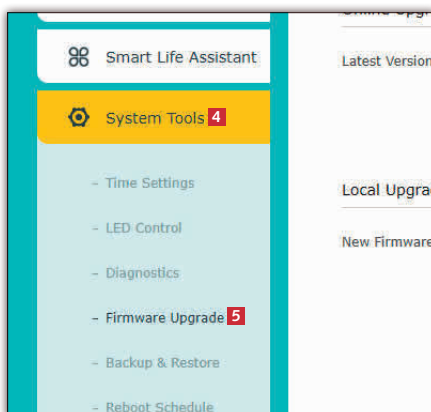


Eivätkö laitteesi enää päivity?

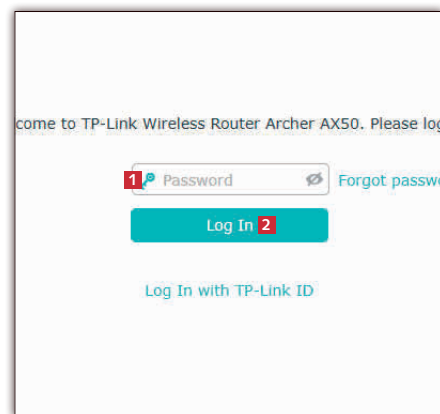
Laitteiden ohjaussivuilta näet yleensä, milloin uusiin laiteohjelmistoon on asennettu. Jos siitä on kulunut yli viisi vuotta, on syytä harkita vahvasti laitteen vaihtamista hyökkäysriskin poistamiseksi. Tässä käytämme esimerkkinä TP-Linkin reititintä.



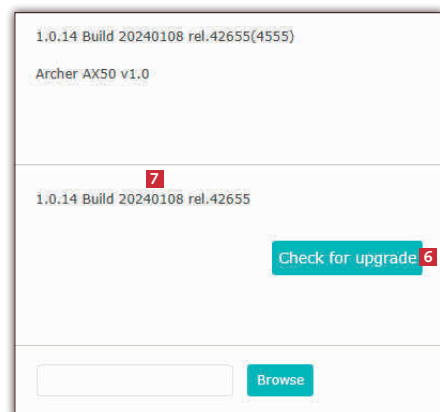
2 Joissakin laitteissa sinun on ensin valittava **Advanced** **3** ennen kuin viimeisimmän asennetun laiteohjelmiston tiedot näytetään.



3 Valitse seuraavaksi **System Tools** **4** tai vastaava, ja valitse sitten **Firmware Upgrade** **5**.



1 Etsi reitittimesi osoite Advanced IP Scannerilla. Kirjoita osoite selaimesi osoiteriville ja paina sitten **Enter**-näppäintä Syötä salasanasi **1** ja valitse **Log in** **2**.



4 Valitse **Check for upgrade** **6**. Näet laiteohjelmiston version **7**. Jos sen päivitys on ajalta ennen vuotta 2020, laitteeseen ei todennäköisesti enää tule lisää päivityksiä.

Harkitse vanhojen laitteidesi hävittämistä

Monien kodin valaistuksen ja lämmityksen valvontaan ja ohjaukseen tarkoitettujen älylaitteiden käyttöön-otosta on kulunut 10–15 vuotta, jolloin monet laitteet ovat tulleet ikään, jossa valmistaja ei enää päivitä niitä. Näin saattaa olla myös kotonasi olevien laitteiden kohdalla varsinkin, jos olet omistanut ne

jo useita vuosia. Valitettavasti monet haavoittuvuudet ovat niin syvälle juurtuneita, että vain valmistajan upouusi laiteohjelmisto voi korjata ne. Siksi erityisesti uudemmat merkkilaitteet päivitetään usein aina, kun uusia haavoittuvuuksia löydetään. Tilanne on erilainen vanhempien laitteiden tai kiinalaisten tuontituotteiden kohdalla. Siksi sinulla on oikeastaan vain kaksi vaihtoehtoa, jos jotkin laitteistasi eivät

enää saa päivityksiä: voit heittää laitteen pois ja ostaa uuden tai irrottaa laitteen verkosta sekä internetistä ja käyttää sitä paikallisesti kotona, jos se on vain mahdollista.



Jos sinulla on älykaiutin, saatat huomata, että uusien tietoturvakorjausten lataaminen on loppunut jo kauan sitten.

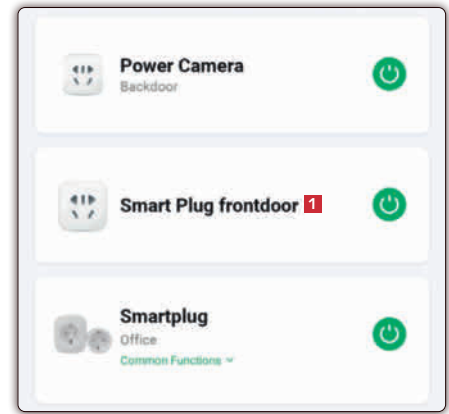
Monet verkkokamerat eivät enää saa laiteohjelmistopäivityksiä. Tämä tarkoittaa sitä, ettei mahdollisia tietoturva-aukkoja enää korjata.



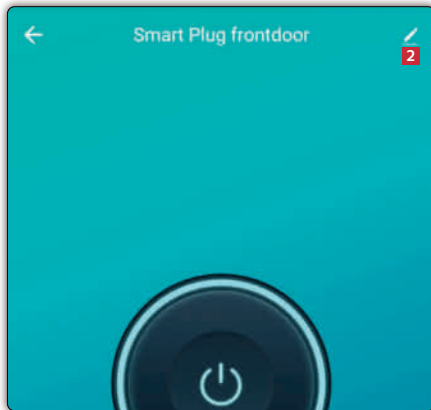


Päivitä laitteesi sovelluksella

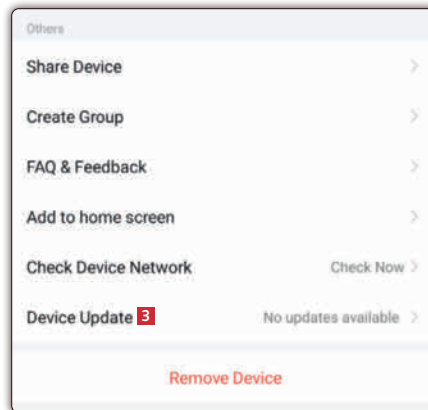
Suurta osaa nykyisin myytävistä kodin älylaitteista voi ohjata vain puhelimen sovelluksella. Siksi sinun on ehkä myös etsittävä ja asennettava päivitykset laitteisiin juuri tästä sovelluksesta.



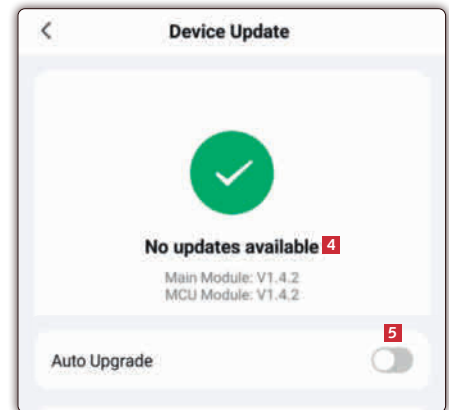
1 Mikäli laitetta voidaan ohjata vain yhdellä sovelluksella, avaa kyseinen sovellus. Jos sovellus ohjaa useampaa kuin yhtä laitetta, napauta päivitettävää laitetta **1**.



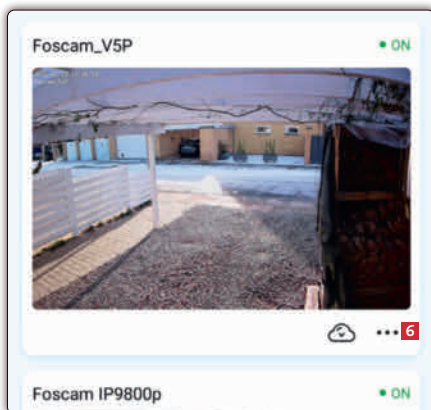
2 Siirry laitteen asetuksiin napauttamalla kynäkuvaketta **2**.



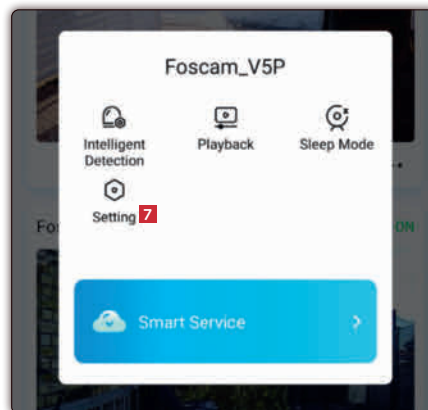
3 Valitse **Device Update** **3** tai vastaava.



4 Täältä voit tarkistaa, onko laitteellesi tullut uusia päivityksiä **4**. Voit tässä näkymässä määrittää laitteesi lataamaan uudet päivitykset automaattisesti tulevaisuudessa **5**.



5 Jos laitteesi on sovelluksella ohjattava verkkokamera, napsauta yleensä kameran kuvan alla olevia kolmea pistettä **6**. Tässä tapauksessa laitteesi tuotemerkki on Foscam.



6 Valitse kohta **Setting** **7**.



7 Valitse seuraavaksi **Firmware Upgrade** **8**. Täältä voit sekä päivittää kameran että tarkistaa, milloin uusin päivitys on asennettu.