

## Ohje

# Johdanto

illumina® on saanut tietoonsa Local Run Manager -ohjelmistossa olevan tietoturva-avaavuuden ja kehittänyt ohjelmakorjauksen, joka suojaaa järjestelmää tämän haavoittuvuuden hyödyntämiseltä etäyhteyden kautta.

Local Run Manager on erillinen ohjelmistosovellus ja osa oletuskokoonpanoa seuraavissa järjestelmissä:

- MiSeq
- MiSeqDx\*
- NextSeq 500
- NextSeq 550
- NextSeq 550Dx\*
- MiniSeq
- iSeq.

\*In vitro -diagnostiseen käyttöön.

Tämä ohje koskee yllä lueteltuja illumina-laitteita ja lisäksi laitteen ulkopuolisia tietokoneita, joihin on asennettu Local Run Managerin erillisversio.

Haavoittuvuus koskee todentamatonta etäkomentojen suorittamista (RCE, Remote Command Execution), ja se on merkittävyydeltään täydet 10,0 CVSS-pistettä eli kriittinen,

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H.

Yllä luetelluille laitteille on tehtävä seuraavat korjaavat toimet niiden suojaamiseksi valtuuttamattomien käyttäjien pääsystä ja etähyökkäykseltä yhteen tai useampaan laitteeseen.

Jos asennusohjelmaa ei jostain syystä voida suorittaa, katso lisäohjeita tämän asiakirjan lopussa olevasta muista korjaavista toiminnoista käsittelevästä osasta tai ota yhteyttä osoitteeseen [techsupport@illumina.com](mailto:techsupport@illumina.com).

Katso kohdasta [Local Run Manager -päivityksen hankkiminen](#), miten voit ladata korjaustiedoston tai pyytää siitä kopion.

- **Ohjelmakorjaus v1.0.0** – päivittää Local Run Manager -verkkomäärityksen ja estää Internet Information Services (IIS) -ohjelmiston etäkäytön.

# Local Run Managerin tietoturvaohjelmakorjauksen hankkiminen


Local Run Managerin tietoturvaohjelmakorjauksen hankkimiseen on neljä (4) eri vaihtoehtoa.

## Vaihtoehto 1 – lataus suoraan laitteeseen

Nopein keino Local Run Manager -tietoturvapäivityksen saamiseen on ladata se suoraan verkkosivulta laitteeseen.

1. Lataa ohjelmakorjauksen latausohjelma laitteeseesi suojatun sähköpostin kautta saamastasi linkistä.
2. Siirrä tiedosto laitteen C:\Illumina-kansioon.
3. Noudata ohjeita, jotka annetaan kohdassa [Local Run Managerin tietoturvaohjelmakorjauksen käyttö sivulla 4](#).

## Vaihtoehto 2 – ohjelmakorjauksen latausohjelman lataaminen tietokoneeseen ja siirtäminen laitteeseen USB-muistitikun / jaetun kansion kautta

 Jos et voi ladata tietoturvaohjelmakorjausta laitteeseen, suosittelemme sen lataamista erilliseen tietokoneeseen ja siirtämistä sitten laitteeseen.


Varmista USB-muistitikun eheys tietoturva-asioista vastaavien kanssa ennen sen käyttöä. (Suositus)

1. Lataa ohjelmakorjauksen latausohjelma suojatun sähköpostin kautta saamastasi linkistä tietokoneeseen tai kannettavaan tietokoneeseen.
2. Kopioi ladattu ohjelmakorjauksen latausohjelma tietokoneelta USB-muistitikkuun tai jaettuun kansioon.
3. Jos aiot käyttää USB-muistitikua, liitä se laitteeseen.
4. Kopioi ohjelmakorjauksen latausohjelma USB-muistitikulta tai jaetusta kansioista laitteen C:\Illumina-kansioon.
5. Noudata ohjeita, jotka annetaan kohdassa [Local Run Managerin tietoturvaohjelmakorjauksen käyttö sivulla 4](#).

## Vaihtoehto 3 – teknisen tuen pyytäminen

Illuminan teknisen tuen edustaja opastaa sinut korjausprosessin läpi yhdellä seuraavista tavoista:

- Teknisen tuen kirjautuminen sisään etäyhteyden kautta  
Teknisen tuen edustaja muodostaa etäyhteyden analysaattoriin ja asentaa ohjelmakorjauksen asiakkaan puolesta.

 Järjestelmään täytyy voida muodostaa etäyhteys. Pyydä tarvittaessa apua paikalliselta IT-vastaavalta.

- Opastus

Teknisen tuen edustaja antaa ohjeet puhelimitse. Ota yhteyttä paikalliseen teknisen tuen edustajaan.

#### Vaihtoehto 4 – esimääritetyn muistitikun tilaaminen Illuminalta

Asiakas voi tilata kirjoitussuojattuja USB-muistitikkuja veloituksetta. Voit tilata ohjelmakorjauksen sisältävän muistitikun osoitteesta [techsupport@illumina.com](mailto:techsupport@illumina.com).

**i** | Lähetyksissä tai varastoinneissa voi olla viivästyksiä, jotka saattavat vaikuttaa toimituksen oikea-aikaisuuteen. Järjestelmien välittömämmäksi suojaamiseksi on erittäin suositeltavaa, että ne suojataan tavalla, joka tarjoaa tehokkaimman ratkaisuvaihtoehdon.

# Local Run Managerin tietoturvaohjelmakorjauksen v.1.0 asennusohjelman käyttö

Illumina MSI (Microsoft Installer) -asennusohjelman suorittaminen päivittää Local Run Manager - verkkopalvelinmäärityksen siten, että käyttäjien lataamien sisältöjen suorittaminen ja kaikki etäyhteydet Local Run Managerin verkkoliittymään lähiverkkoyhteyksistä estetään.

**i** | Local Run Managerin verkkoliittymää laitteiden etäkäyttöön hyödyntävien käyttäjien osalta tämä työnkulku lakkaa toimimasta tämän ohjelmakorjauksen asentamisen jälkeen. Illumina aikoo palauttaa tämän toiminnon myöhemmin käyttöön pysyvällä ohjelmakorjauksella. Jos tämä aiheuttaa keskeytyksen vakiintuneisiin työnkulkuihin, ota yhteyttä osoitteeseen [techsupport@illumina.com](mailto:techsupport@illumina.com).

MSI-asennusohjelma soveltuu kaikkiin Local Run Manager -versioihin ja määrittää automaattisesti tarvittavan korjauksen laitteeseen/tietokoneeseen asennetun Local Run Manager -version perusteella.

Tämä MSI-asennusohjelma luo myös tarkistustiedoston, jossa osoitetaan tämän korjaavan toimen toteuttaminen yhdessä aikaleiman kanssa sen merkiksi, että asennus on tehty oikein.

MSI-asennusohjelman suorittaminen – kun MSI-asennusohjelma suoritetaan ensimmäisen kerran, se korjaa järjestelmän ja luo tarkistustiedoston, jossa ilmoitetaan suoritus aika.

**i** | Kun MSI-asennusohjelma suoritetaan uudelleen, näkyviin tulee **Repair (Korjaa)** -vaihtoehto ja käyttäjä voi suorittaa ohjelmakorjauksen uudelleen tai peruuttaa sen. Huomautus: mikäli ohjelmakorjaus peruutetaan, laitekokoontaminen jää suojaamattomaksi.

# Local Run Managerin tietoturvaohjelmakorjauksen käyttö

## Asenna ohjelmakorjaus seuraavasti:

1. Kirjautu järjestelmään käyttämällä järjestelmänvalvojan tiliä (esim. sbsadmin).

**i** | Illumina suosittelee, että ohjelmakorjaus asennetaan, kun laite ei ole toiminnassa. Jos laitteessa on ajo käynnissä, ohjelmakorjaus tulee asentaa välittömästi ajon päättymisen jälkeen.

2. Etsi järjestelmään ladattu korjaustiedosto.
3. Siirrä ohjelmakorjauksen asennusohjelma C:\Illumina-kansioon (vapautus ohjelmistorajoituskäytännöstä).
4. Käynnistä liittymä kaksoisnapsauttamalla asennusohjelman kuvaketta.
5. Kun sovellus lataa, aloita ohjelmakorjauksen asentaminen valitsemalla **Next** (Seuraava).
6. Valitse asennuksen valmistumisnäytössä **Finish** (Lopeta).

**i** | Mikäli asennusraportti on tarkistettava, katso kohta [Tarkistus sivulla 5](#).

**i** | Järjestelmä on käynnistettävä uudelleen asennuksen päätteeksi.

## Korjaus

Virhetilanteissa asiakas voi korjata asennuksen seuraavien ohjeiden mukaisesti:

1. Kirjautu järjestelmään käyttämällä järjestelmänvalvojan tiliä (esim. sbsadmin).
2. Etsi järjestelmään ladattu korjaustiedosto.
3. Siirrä ohjelmakorjauksen asennusohjelma C:\Illumina-kansioon (vapautus ohjelmistorajoituskäytännöstä).
4. Käynnistä liittymä kaksoisnapsauttamalla asennusohjelman kuvaketta.
5. Asennusohjelma havaitsee automaattisesti, onko määrittästyökalu suoritettu aiemmin ja esittää uusia vaihtoehtoja:
  - a. Muutos: näkyy harmaana eikä ole käytettävissä
  - b. Korjaus: korjaa virheet ja antaa vaihtoehtoja uudelleenmäärittämiselle
  - c. Poisto: poistaa ohjelmakorjauksen asennuksen ja palauttaa sen oletuskokoonpanoon (katso [Asennuksen poisto sivulla 5](#))
6. Valitse asennuksen valmistumisnäytössä **Finish** (Lopeta).


**i** | Mikäli asennusraportti on tarkistettava, katso kohta [Tarkistus sivulla 5](#).

**i** | Järjestelmä on käynnistettävä uudelleen asennuksen päätteeksi.


## Asennuksen poisto


Ohjelmakorjauksen asennuksen poisto palauttaa sovelluksen isännän kokoonpanotiedostoon tehdyt muutokset.

1. Kirjautu järjestelmään käyttämällä järjestelmänvalvojan tiliä (kuten sbsadmin).
2. Etsi järjestelmään ladattu korjaustiedosto.
3. Siirrä ohjelmakorjauksen asennusohjelma C:\Illumina-kansioon (vapautus ohjelmistorajoituskäytännöstä).
4. Käynnistä liittymä kaksoisnapsauttamalla asennusohjelman kuvaketta.
5. Poista ohjelmakorjauksen asennus ja palauta kaikki arvot oletusasetuksiin valitsemalla **Remove (Poista)**.
6. Varmista toiminto, jolla ohjelmakorjauksen asennus poistetaan ja kaikki arvot palautetaan oletusasetuksiin, valitsemalla **Remove (Poista)**.

 Tämä asetus tekee järjestelmästä suojaamattoman ja alttiiksi hyökkäyksille. Ennen asennuksen poistamisen valitsemista on erittäin suositeltavaa kiinnittää huomiota teknisiin vaikutuksiin, jotka aiheuttavat ohjelmakorjauksen poistovaihtoehdon.

7. Valitse asennuksen valmistumisnäytössä **Finish (Lopeta)**.

 Mikäli asennusraportti on tarkistettava, katso kohta [Tarkistus sivulla 5](#).

 Asennuksen lopuksi järjestelmä on suositeltavaa käynnistää uudelleen.

## Tarkistus

Jos asennus on tarkistettava, järjestelmä on luonut tarkistustiedoston, joka sisältää päivä- ja aikaleiman, asennetun Local Run Manager -version ja muita olennaisia tarkistusarvoja. Pyydä tätä tiedostoa osoitteesta [techsupport@illumina.com](mailto:techsupport@illumina.com).

# Korjaavia toimia ja tietoturvaa koskevat lisäsuositukset

Tutkimuslaitteiden (RUO) ja lääkinällisten diagnostiikkalaitteiden käytön turvallisuus riippuu suojaustasoista. Illumina suosittelee vahvasti, että laitteita käytetään pienimmässä mahdollisessa verkon aliverkko- tai suojauskontekstissa luotettujen laitteiden kanssa. Saapuvien ja lähtevien yhteyksien rajoittamiseksi on erittäin suositeltavaa käyttää palomureja ja muita verkkokäytäntöjä.

Suosittelemme myös seuraavia toimenpiteitä:

- Varmista kaikkien laitteiden ulkopuolisten yhteyksien salaus ottamalla käyttöön Transport Layer Security (TLS) -protokolla.
  - Katso Transport Layer Security (TLS) -protokollan käyttöönottoa koskevat ohjeet Local Run Manager -ohjelmiston ohjeesta.

# Muut vaihtoehdot

Jos korjaustiedoston suorittaminen ei jostain syystä ole vaihtoehto, seuraavilla manuaalisilla korjaavilla toimilla riskiä voidaan pienentää:

- Poista käytöstä etäyhteys Local Run Manageriin lisäämällä Windows-palomuurisäännöt, jotka estävät porttien 80 ja 443 saapuvat yhteydet.  
MSI-asennusohjelma estää automaattisesti saapuvat etäyhteydet Local Run Managerin verkkopalvelinmäärityksissä. Samaan tulokseen päästään manuaalisella korjaavalla toimella, joka tapahtuu ottamalla käyttöön Windows-palomuurimääritys, joka estää saapuvat yhteydet HTTP (TCP:80) - ja HTTPS (TLS, TCP:443) -yhteyksiin.  
Käyttöönoton jälkeen Local Run Manageriin voi muodostaa yhteyden vain tietokoneesta, johon se on asennettu, ja siihen ei enää pääse muista samaan verkkoon yhdistetyistä tietokoneista.

**i** Mikäli käyttäjän työkulkuun sisältyy Local Run Managerin etäkäyttö, tämä toiminto ei enää toimi.

- Pidä muiden verkkoon liitettyjen laitteiden määrä mahdollisimman pienenä.  
Haavoittuvuuden hyödyntämisen mahdollisuus on pienempi, kun verkko määritetään siten, että haavoittuvuudelle alttiina olevaan laitteeseen yhteydessä olevien verkon laitteiden määrä on mahdollisimman pieni. Mitä vähemmän yhteyksiä järjestelmään on saatavilla, sitä vähemmän mahdollisuuksia on päästä siihen käsiksi.  
Tämä voi edellyttää kääntymistä paikallisten tietoturva- tai IT-vastaavien puoleen.
- Poista laite verkosta.  
Jos muut vaihtoehdot eivät ole toteutuskelpoisia, lopullinen korjaava toimi on laitteen poistaminen verkosta kokonaan. Tämä estää Illumina Cloud/SaaS -palveluiden, kuten Proactiven ja BaseSpacen® Sequence Hubin, sekä tavallisten genomitietojen purun työkulkujen käytön.  
Tämä voi edellyttää kääntymistä paikallisten tietoturva- tai IT-vastaavien puoleen.

## Mahdollisen valtuuttamattoman käytön tutkiminen

Seuraavat toimenpiteet voivat auttaa laitteen käyttäjää saamaan selville, onko valtuuttamaton käyttäjä päässyt järjestelmään.

1. Tutki C:\inetpub\logs\LogFiles\W3SVC1-kansioon tallennetut IIS-lokit poikkeavien kutsujen varalta.
  - Local Run Manager -verkkopalvelimelle saapuvat normaalit kutsut ovat seuraavanlaisia:

```
GET http /normalresource.extension?normal-URI-decoration
```

- Local Run Manager -verkkopalvelimelle saapuvat poikkeavat kutsut voivat olla esimerkiksi seuraavanlaisia:

```
POST http /hackertool.asp
```

2. Tutki IIS-loki sisällön POST-latauksia ilmaisevien merkkien varalta, lukuun ottamatta manifestitiedostoja. Esimerkiksi seuraavat kutsut viittaavat epäilyttävään toimintaan:

```
wscript  
shell  
wscript.network  
scripting.filesystemObject
```

3. Jos asennettuna on virusten/haittaohjelmien torjuntasovellus, tarkista ohjelmistolokit poikkeavan toiminnan varalta.
4. Tutki Windows-lokit poikkeavien virheviestien varalta.  
Jos uhkatoimijat ovat päässeet murtautumaan järjestelmänvalvojan oikeuksilla, he ovat voineet muuttaa kaikkia paikallisia laitelokeja ja -tapahtumia tai poistaa ne.

Tarkista mahdolliset päätepisteet, joihin järjestelmä on saattanut yrittää muodostaa yhteyden. Luettelon odotetuista lähtevistä yhteyksistä näet kohdasta [Ohjaustietokoneen palomuri](#).

Pyydä tarvittaessa apua Illuminan teknisestä tuesta.

# Versiohistoria

Asiakirja	Päivämäärä	Muutoksen kuvaus
Asiakirjanro 200017330 v02	Huhtikuu 2022	Lisätty suositus ohjelmakorjauksen asentamisesta silloin, kun laite ei ole toiminnassa.  Lisätty ohje, että laitteen uudelleenkäynnistys vaaditaan ohjelmakorjauksen asennuksen jälkeen.  Versiohistorian kuvaus korjattu version v01 osalta.
Asiakirjanro 200017330 v01	Huhtikuu 2022	Asiakirjan nimeksi muutettu LRM-ohjelmakorjauksen 1.0 ohje  Poistettu maininnat versiosta v1.0.1.  Lisätty mahdollisen valtuuttamattoman käytön tutkimista koskeva osio.
Asiakirjanro 200017330 v00	Maaliskuu 2022	Ensimmäinen versio.

Tämä asiakirja ja sen sisältö ovat Illumina, Inc:n ja sen tytäryhtiöiden ("Illumina") omaisuutta, ja ne on tarkoitettu ainoastaan Illuminan asiakkaiden sopimuskäyttöön tässä kuvattujen tuotteiden käyttöön liittyen eikä mihinkään muuhun tarkoitukseen. Tätä asiakirjaa ja sen sisältöä ei saa käyttää tai jakaa missään muussa tarkoituksessa ja/tai välittää, paljastaa tai jäljentää millään muulla tavoin ilman Illuminalta ennakkoon saatua kirjallista lupaa. Illumina ei tällä asiakirjalla luovuta mitään käyttöoikeuksia sen patenti-, tavaramerkki-, tekijänoikeus- tai tapaoikeuksien nojalla eikä vastaavien kolmansien osapuolten oikeuksien nojalla.

Tässä kuvattuja tuotteita saa käyttää vain pätevä ja asianmukaisesti koulutettu henkilökunta noudattamalla täsmällisesti tässä asiakirjassa annettuja ohjeita, jotta tuotteiden asianmukainen ja turvallinen käyttö voidaan taata. Asiakirjan sisältö on luettava ja ymmärrettävä kokonaisuudessaan ennen näiden tuotteiden käyttöä.

MIKÄLI TÄSSÄ ANNETTUJA OHJEITA EI LUETA JA TÄSMÄLLISESTI NOUDATETA, SEURAUKSENA VOI OLLA TUOTTEIDEN VAURIOITUMINEN, HENKILÖVAHINKOJA JOKO KÄYTTÄJILLE TAI MUILLE JA MUITA OMAISUUSVAHINKOJA, MINKÄ LISÄKSI TUOTTEITA MAHDOLLISESTI KOSKEVAT TAKUUT MITÄTÖITYVÄT.

ILLUMINA EI OLE VASTUUSSA TÄSSÄ KUVATTUJEN TUOTTEIDEN VÄÄRINKÄYTÖSTÄ (MUKAAN LUKIEN TUOTTEEN OSAT JA OHJELMISTO).

© 2022 Illumina, Inc. Kaikki oikeudet pidätetään.

Kaikki tavaramerkit ovat Illumina, Inc:n tai niiden vastaavien omistajien omaisuutta. Tarkemmat tavaramerkkitiedot annetaan osoitteessa [www.illumina.com/company/legal.html](http://www.illumina.com/company/legal.html).