

UKK: Microsoft Exchange Online (M365) SMTP Basic Authentication -tuen poistaminen ja vaikutukset Toshibaa monitoimilaitteisiin.

Microsoft tekee merkittäviä muutoksia siihen, miten sähköpostin todennus toimii Exchange Onlinessa. Näiden päivitysten tarkoituksena on parantaa tietoturvaa poistamalla käytöstä Basic Authentication ja siirtymällä turvallisempiin, moderneihin menetelmiin.

Auttaaksemme sinua ymmärtämään, mitä on muuttumassa ja miten se voi vaikuttaa organisaatioosi, olemme koonneet vastauksia usein kysyttyihin kysymyksiin.

1. Mikä on SMTP Basic Authentication?

SMTP Basic Authentication on vanha menetelmä, jota käytetään sähköpostien lähettämiseen Simple Mail Transfer Protocolin (SMTP) kautta. Se käyttää staattista käyttäjätunnusta ja salasanaa, mikä tekee siitä haavoittuvan tietoturvaaukille.

2. Miksi Microsoft poistaa sen käytöstä?

Microsoft poistaa Basic Authenticationin parantaakseen tietoturvaa. Se on altis:

- Tunnistetietojen varkaudelle
- Brute force -hyökkäyksille
- Monivaiheisen todennuksen (MFA) puutteelle

Modernit todennusmenetelmät, kuten OAuth 2.0, tarjoavat vahvemman suojan ja paremman identiteetinhallinnan.

3. Milloin tämä tapahtuu??

Microsoft alkoi poistaa Basic Authenticationia käytöstä Exchange Onlinessa lokakuussa 2022, ja täysi käyttöönotto jatkuu vuoteen 2026 asti. SMTP-todennus (SMTP AUTH) on jo oletuksena pois päältä uusissa ympäristöissä ja poistetaan vähitellen myös olemassa olevista. Microsoft alkaa pakottaa muutoksen **1. maaliskuuta 2026**, ja täysi poistaminen valmistuu **30. huhtikuuta 2026** (aiemmin aikataulutettu syyskuulle 2025).

4. Ketkä ovat vaikutuksen piirissä?

Muutokset voivat koskea sinua, jos:

1. Käytät skriptejä, sovelluksia tai laitteita, jotka lähettävät sähköpostia SMTP:n kautta Basic Authenticationilla.
2. Riippuvaiset vanhoista järjestelmistä tai monitoimilaitteista (MFP), jotka eivät tue modernia todennusta.
3. Käytät kolmannen osapuolen palveluita tai ohjelmistoja, jotka yhdistävät Exchange Onlineen SMTP:n kautta.

5. Mikä ongelma on sovellussalasanissa?

Sovellussalasanat ovat kiertotie vanhoille sovelluksille, jotka eivät tue modernia todennusta. Niitä **ei kuitenkaan suositella**, koska:

- Ne ohittavat MFA:n.
- Niiden hallinta ja auditointi on vaikeaa.
- Ne tarjoavat heikon näkyvyyden ja hallinnan.
- Ne ovat alttiita tunnistetietojen varkaudelle.
- Microsoft voi poistaa ne käytöstä tulevaisuudessa.

6. Miten tämä vaikuttaa monitoimilaitteisiin (MFP)?

Monet MFP-laitteet käyttävät SMTP:tä skannattujen asiakirjojen lähettämiseen sähköpostitse. Jos laitteet käyttävät Basic Authenticationia:

- a. Ne **eivät enää pysty lähettämään sähköposteja**, kun Basic Authentication poistetaan.
- b. Laitteiden hälytykset ja värikasettipyyntö sähköpostitse epäonnistuvat.
- c. Vanhemmat mallit **eivät välttämättä tue** OAuth 2.0:aa tai modernia todennusta.
- d. Skannaa sähköpostiin -työnkulut **voivat rikkoutua**, ellei niitä konfiguroida uudelleen.

7. Miten voin konfiguroida MFP:n käyttämään OAuth 2.0:aa?

Yleiset ohjeet:

I. Tarkista yhteensopivuus

- i. Tutustu MFP:n dokumentaatioon tai ota yhteyttä toimittajaan vahvistaaksesi tuen OAuth 2.0:lle tai Microsoft Graph API:lle.
- ii. Tarkista, onko saatavilla laiteohjelmistopäivityksiä, jotka lisäävät modernin todennuksen tuen.

II. Konfiguroi OAuth-asetukset MFP:ssä

- a. Ota yhteyttä Toshiba-edustajaan saadaksesi ohjeet konfigurointiin.

III. Testaa konfiguraatio

- a. Lähetä testiskannaus sähköpostiin.
- b. Seuraa lokitietoja onnistuneen tai epäonnistuneen todennuksen varalta.

IV. Varavaihtoehto:

- a. Jos Monitoimilaitte ei tue OAuth 2.0:aa, ota yhteyttä Toshiba-edustajaan suositeltujen vaihtoehtojen saamiseksi.

8. Mitkä ovat vaihtoehdot muille järjestelmille?

- **OAuth 2.0:** Turvallinen, token-pohjainen todennus MFA- ja ehdollisen pääsyn tuella.
- **Microsoft Graph API:** Moderneille sovelluksille ja palveluille, jotka tarvitsevat sähköpostin lähettämistä tai Microsoft 365 -datan käyttöä.
- **Monitoimilaitteen appsit:** Joihinkin laitteisiin voidaan lisätä Scan-sovelluksia, jotka mahdollistavat sähköpostin lähetyksen ja pilvitallennuksen (esim. OneDrive).
- **SMTP-välitys modernilla todennuksella:** Laitteille, kuten MFP:ille, jotka eivät tue suoraan OAuth 2.0:aa.

9. Miten voin tarkistaa, käyttääkö organisaationi SMTP Basic Authenticationia?

Ylläpitäjät voivat:

- Käyttää Microsoft 365 Admin Centerin raportteja.
- Tarkistaa Azure AD:n kirjautumislokit.
- Tarkistaa Exchange Onlinen viestien seurantatiedot.
- Käyttää PowerShellä todennusmenetelmien kyselyyn.

10. Mitä tapahtuu, jos en siirry uuteen järjestelmään?

- Sähköpostin lähetys SMTP:n kautta epäonnistuu.
- Sovellukset ja monitoimilaitteet, jotka käyttävät Basic Authenticationia, voivat lakata toimimasta.
- Saatat kohdata palvelukatkoja ja lisääntyneitä tietoturvariskejä.

11. Voinko ottaa SMTP Basic Authenticationin väliaikaisesti uudelleen käyttöön?

Microsoft salli aiemmin väliaikaisen uudelleenkäytön tukipyyntöjen kautta, mutta tämä vaihtoehto poistuu ja **sitä ei suositella**.

12. Mistä löydän lisätietoa?

Lisätietoa löytyy Microsoftin resursseista:

- Microsoft Learn: [Basic Authenticationin poistaminen](#)
- Exchange Team Blog