

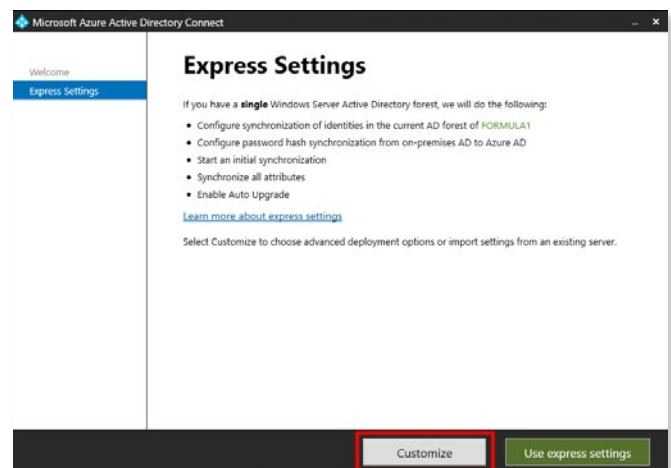
How to: Microsoft 365 mit ESET Secure Authentication absichern

Microsoft Entra Connect einrichten

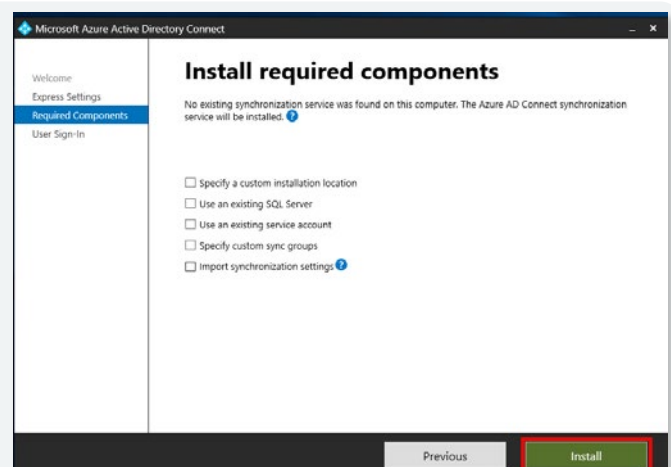
Um Microsoft Entra Connect zu konfigurieren, müssen Sie intern und bei Microsoft 365 dieselbe Dömane nutzen.

Bitte beachten Sie, dass diese Anleitung keine technische Beratung ersetzt. Führen Sie die folgenden Schritte nicht ohne einen Microsoft Spezialisten durch.

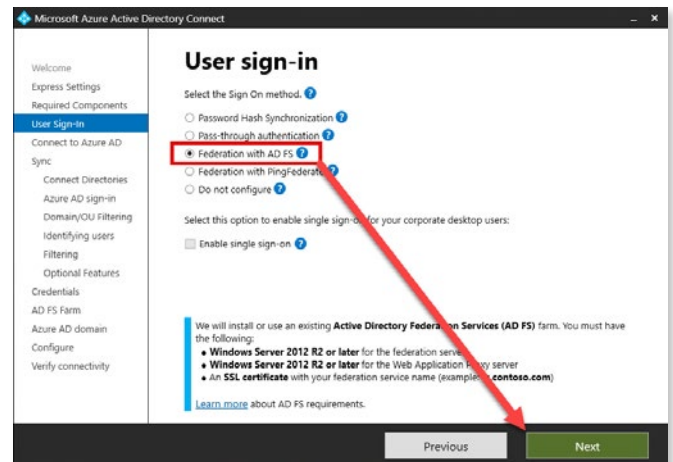
Laden Sie Microsoft Entra Connect [hier](#) herunter und fahren Sie mit der Installation fort. Wählen Sie hier die "Customize" Variante.



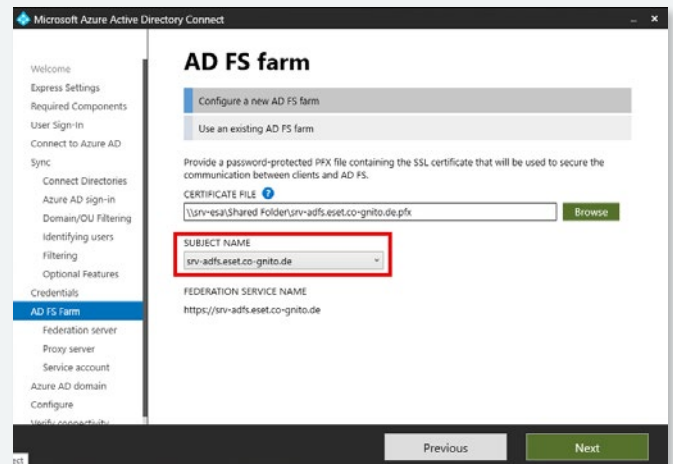
Im folgenden Menü können Sie selbst wählen, ob Sie eine der Optionen nutzen möchten oder die Installation fortsetzen.



Nach der Installation erscheint folgendes Menü, bei welchem Sie „Federation with AD FS“ auswählen.

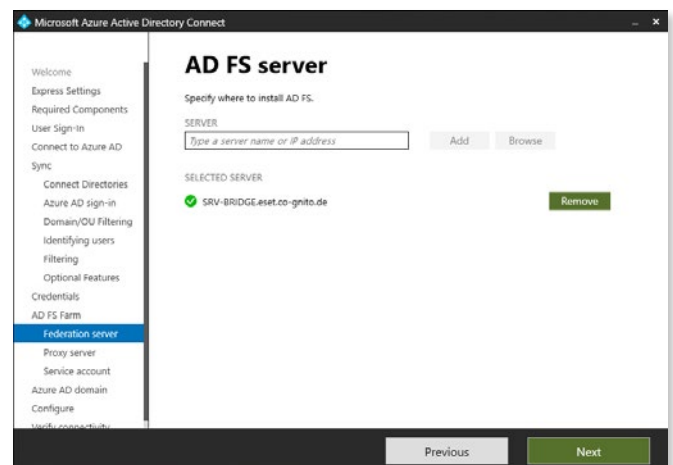


Klicken Sie weiter bis zum Punkt: AD FS Farm. Verwenden Sie hierfür unbedingt ein öffentlich validiertes Zertifikat mit einem extern auflösbaren FQDN, da der Server auch von extern erreichbar sein muss.



Wählen Sie im Anschluss den AD FS Server aus. In diesem Beispiel ist der AD FS Server auch der Server, auf welchem der Entra Connect Installer ausgeführt wird.

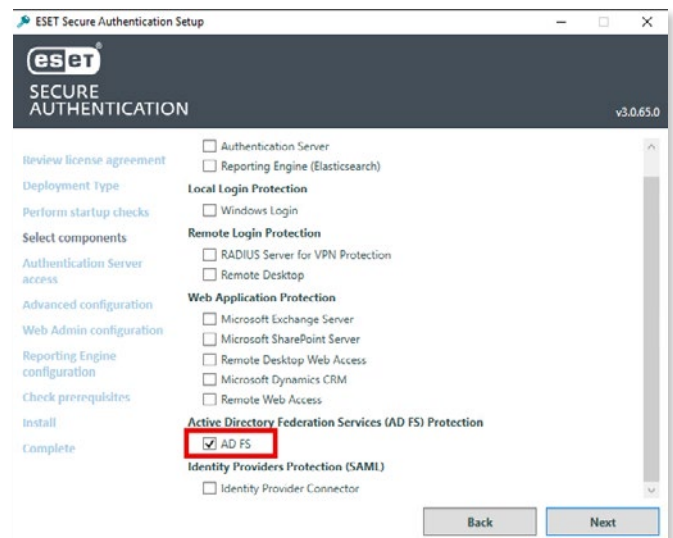
Alle weiteren Einstellungen können problemlos individuell eingerichtet werden.



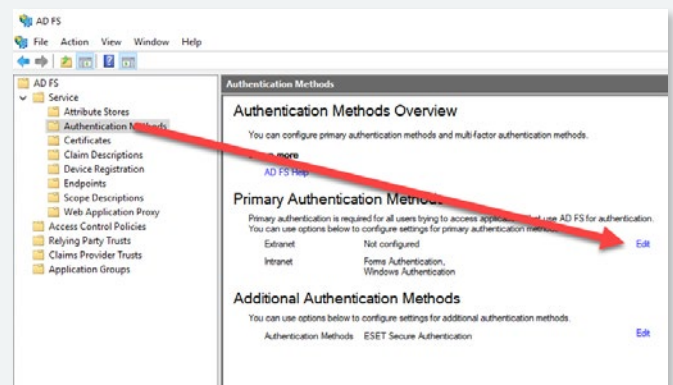
ESET AD FS Komponente installieren

Zunächst muss der ESET Secure Authentication Installer [heruntergeladen](#) und ausgeführt werden.

Wählen Sie im Installer unter "Select Components" AD FS aus.

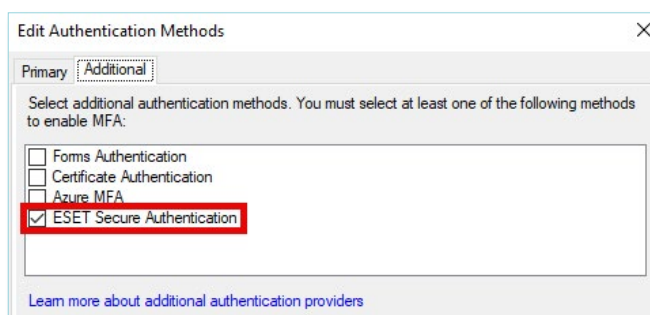
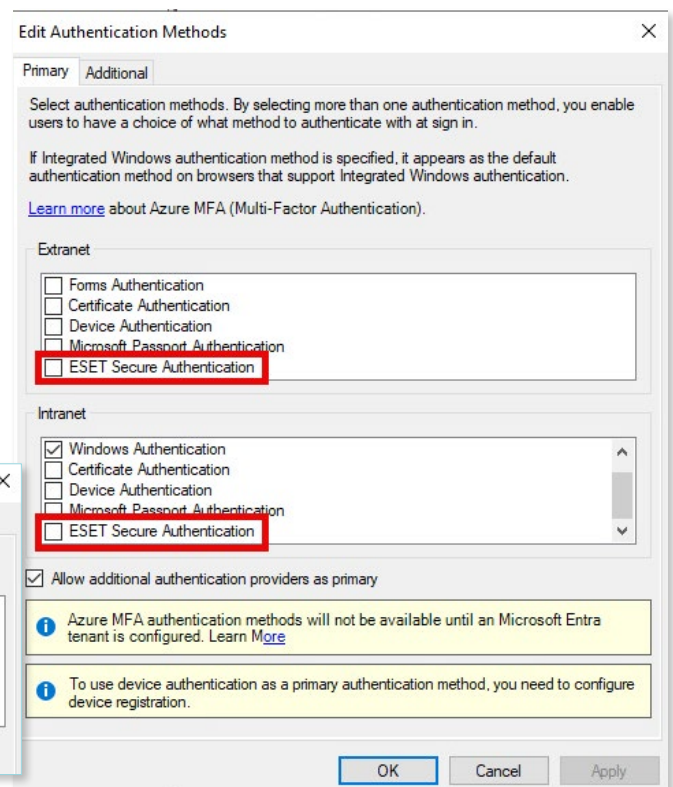


Nach Abschluss der Installation stellen Sie im AD FS Management noch Folgendes ein:



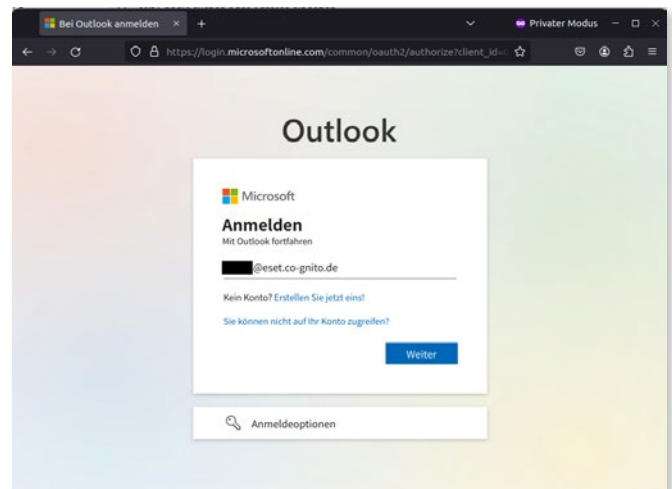
Setzen Sie unter "Primary" bei ESET Secure Authentication KEINEN Haken.

Sie müssen unter "Additional" bei ESET Secure Authentication das Häkchen setzen.

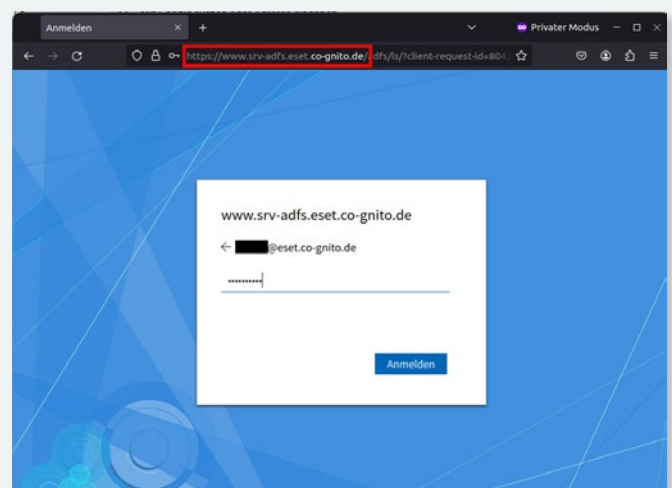


Nutzer Login bei Microsoft 365-Diensten

Nach Abschluss der Einrichtung von AD FS kann sich der User bei einem Microsoft 365 Dienst einloggen.

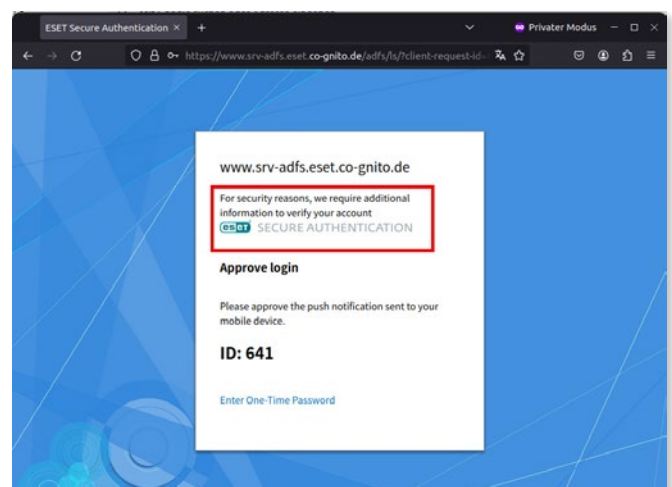


Anschließend wird der Nutzer zum AD FS Server weitergeleitet, wo die Authentifizierung einschließlich zweiten Faktor von ESET durchgeführt wird. Dafür muss der AD FS Server allerdings per Browser erreichbar sein. Sowohl von extern als auch von intern.



Da das Häkchen im AD FS als "Additional Authentication Method" ESET Secure Authentication gesetzt wurde, wird nun auch der zweite Faktor des Users abgefragt.

Ihr Microsoft 365 ist nun durch ESET Secure Authentication abgesichert.



Über ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Unternehmensgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihr Netzwerk mithilfe von Cloud Sandboxing frei von Zero Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungsprodukte unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen.

Unsere XDR-Basis mit Endpoint Detection and Response-Lösung, Frühwarnsysteme (bspw. Threat Intelligence) und dedizierte Services ergänzen das Angebot im Hinblick auf Forensik sowie den gezielten Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

3 VON ÜBER 400.000 ZUFRIEDENEN KUNDEN



Seit 2019 ein starkes Team
auf dem Platz und digital



Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer



ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT



ESET wurde das Vertrauensiegel
„IT Security made in EU“ verliehen



Unsere Lösungen sind nach den Qualitäts- und
Informationssicherheitsstandards ISO 9001:2015
und ISO/IEC 27001:2013 zertifiziert

KONTAKT

Bei Rückfragen können sich ESET Partner
an die Partnerbetreuung wenden.

Tel: +49 (0) 3641 / 31 14 - 220 (Mo - Fr 8 - 17 Uhr)
E-Mail: partner@eset.de

