User Reauthentication on sensitive apps and high-risk actions with Conditional Access

Conditional Access Reauthentication ilkesinde kullanılan senaryoları için artık mevcut olan yeteneklere bir yenisi daha eklendi. Reauthentication ilkesi, genellikle kritik uygulamalara erişmeden ve hassas eylemler gerçekleştirmeden önce kullanıcıların kimlik bilgilerini etkileşimli olarak tekrar sağlamalarını zorunlu kılmanıza olanak tanımaktadır. Oturum açma sıklığının Conditional Access oturum denetimi ile birlikte, riskli kullanıcılar ve oturum açma işlemleri veya Intune kaydı için yeniden kimlik doğrulama gerektirebilmekteyiz. Ancak yeni gelen güncelleme ile artık herhangi bir uygulama ve erişim için yeniden kimlik doğrulama işlemlerine kullanıcıları zorlayabilirsiniz.

Conditional Access Nedir ?

Conditional access kullanıcıların erişimlerini yalnızca sizlerin belirlediği koşulları sağlanması durumunda oturum açabileceği bir Microsoft Entra hizmetidir. Conditional Acces ile oluşturduğunuz koşula bağlı olarak kullanıcı erişiminin konumuna, cihazına, kimlik risk düzeyine göre istenilen uygulamalara erişimlerine izin verebilir veya blocklayabilir veya yeniden authentication işlemine zorlayabilirsiniz. Intune üzerinden yapılacak Enrollment çalışmalarında da yine conditional access politikalarını kullanabilirsiniz.

Modern kimlik doğrulama methodu olarak yoğunlukla kullanılan Single Sign On (SSO), üretkenlik ve güvenlik için gizli bir yardım paketi gibidir. Verimliliği artırır çünkü kullanıcılar kimlik bilgileriyle her birinde oturum açmadan uygulamalara sorunsuzca erişebilir. SSO aynı zamanda güvenliği de artırır çünkü kimlik bilgilerinin yeniden kullanım risklerini azaltır ve Zero-Trust dağıtımlarınız için kontrol ve günlük kaydı için ortak bir nokta sağlar.

Ancak, bir kaynağa erişmeden önce etkileşimli kimlik doğrulama gibi kullanıcının girişini isteyebileceğiniz durumlar vardır. Bu durumlardan biri token hırsızlığıdır. Token Theft saldırısı, kullanıcı çok faktörlü kimlik doğrulamayı (MFA) yerine getirmiş olsa bile saldırganlar bir kullanıcıya verilen tokenları ele geçirip yeniden oynattığında erişimi sağlamasıyla meydana gelir. Kimlik doğrulama gereksinimleri karşılandığından, saldırganlar çalınan tokenları kullanarak kurumsal kaynaklara erişim izni verilmiş olur. Risk tabanlı yeniden kimlik doğrulama ilkeleri, saldırganların sistem erişimini yeniden kazanmak için yeni bir token kullanmasını gerektirerek token hırsızlığından kaynaklanan riski azaltmaya yardımcı olabilir.

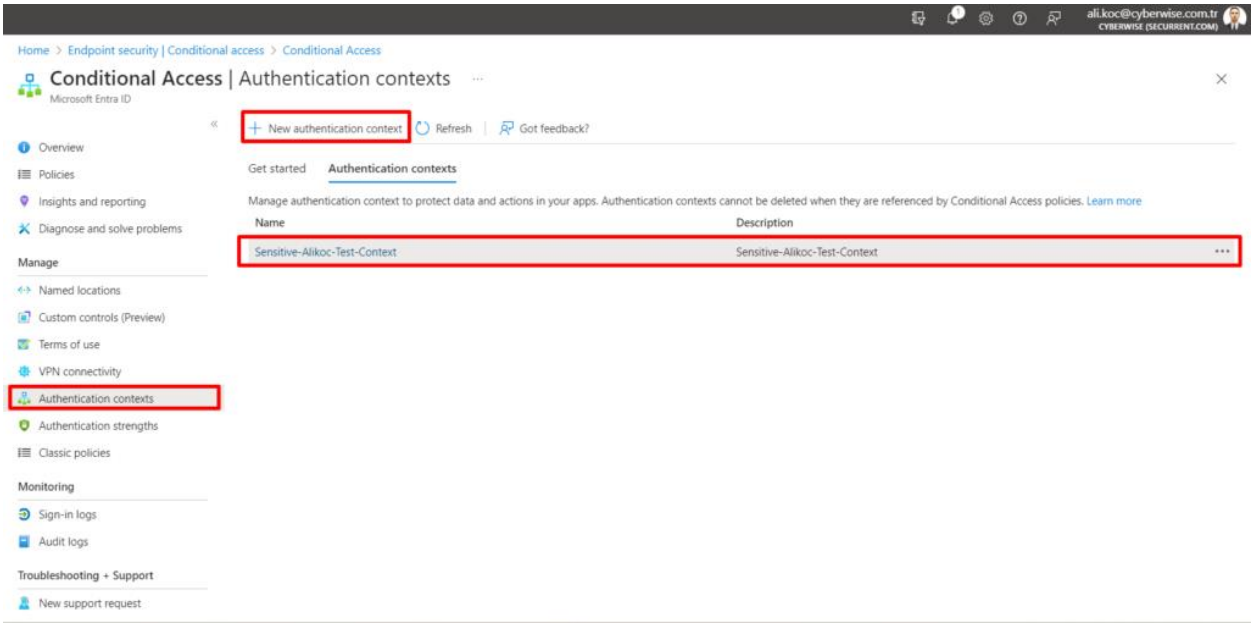
Kullanıcıdan yeniden kimlik doğrulaması yapmasını beklediğimiz durumları incelersek ;

- VPN’e bağlanmak gibi yüksek riskli kaynaklara erişim.
- Privileged Identity Management’ta (PIM) ayrıcalıklı bir rolün etkinleştirilmesi.
- Örneğin bir İK uygulamasında kişisel bilgileri değiştirmek gibi bir uygulama içinde bir eylem gerçekleştirme.
- Intune kaydı veya kimlik bilgilerinin güncellenmesi gibi kritik eylemler.
- Yukarıda belirtildiği gibi riskli oturum açma işlemleri, token hırsızlığı riskini azaltmaya ve hafifletmeye yardımcı olmaktadır.

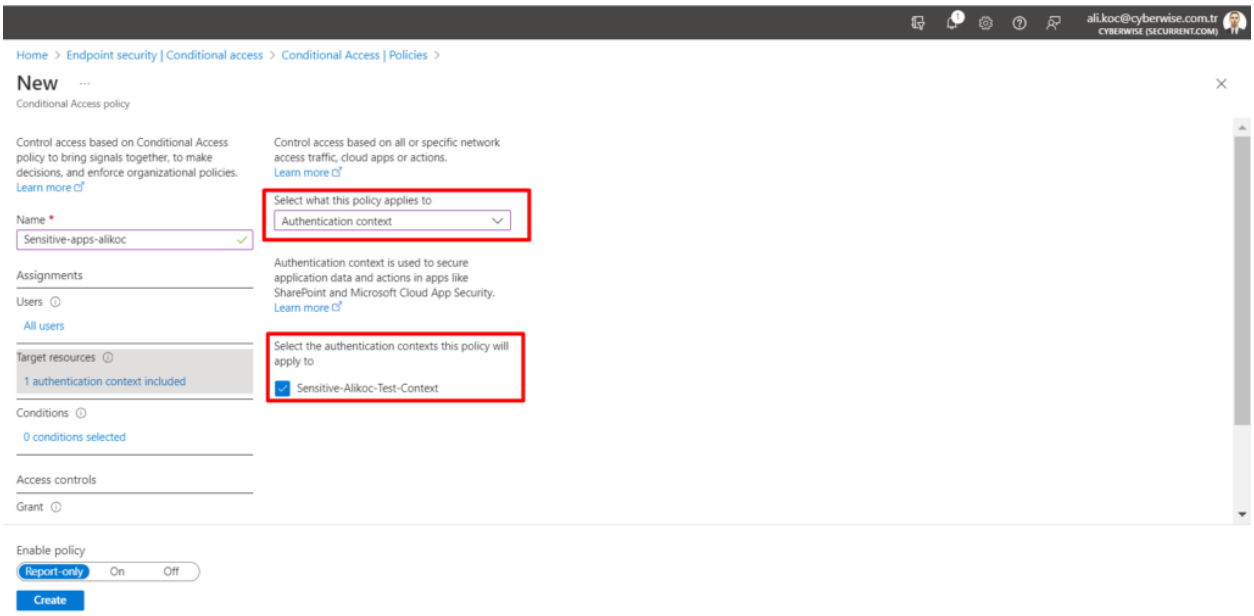
Son güncellemeyle birlikte, artık Koşullu Erişim tarafından korunan herhangi bir uygulama veya kimlik doğrulama bağlamı yeniden kimlik doğrulama gerektiren ilkeleri kolaylıkla oluşturabilirsiniz.

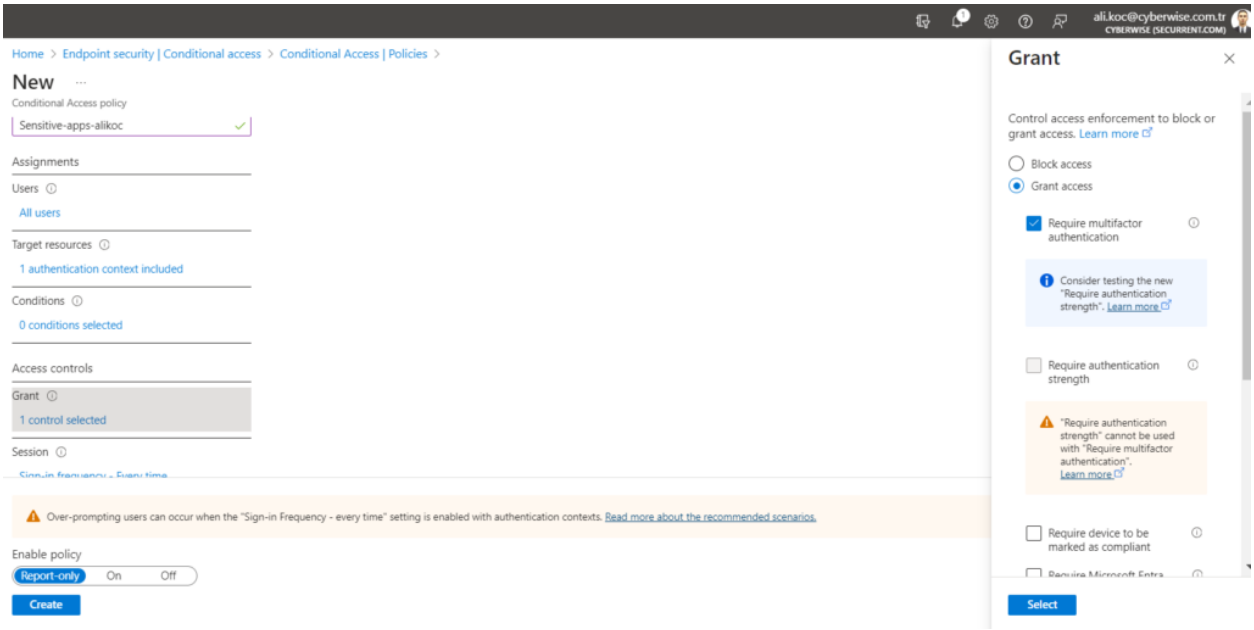
İlk olarak politikada oluşturacağımız Authentication Context’i oluşturmamız gerekmektedir.

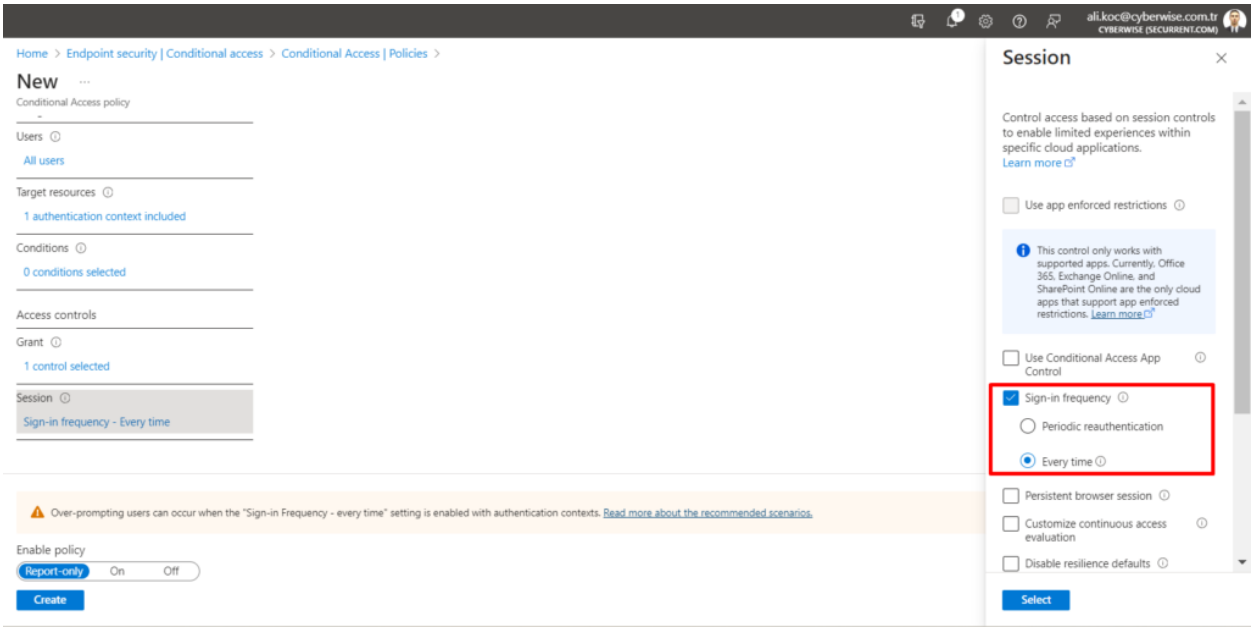
Authentication Context , uygulamalardaki verileri ve eylemleri daha da güvenli hale getirmek için kullanılmaktadır. Bu uygulamalar, kendi özel uygulamalarınız, özel iş kolu (LOB) uygulamalarınız, SharePoint gibi uygulamalarınız veya Bulut Uygulamaları için Microsoft Defender tarafından korunan uygulamalarınız olabilir.



Authentication Context oluşturma işlemi tamamlandıktan sonra “policies” ekranından Yeni bir Conditional Access Policy Create edebiliriz.


ali.koc@cyberwise.com.tr
CYBERWISE (SECURRENT.COM)
Home > Endpoint security | Conditional access > Conditional Access | Policies >
New
Conditional Access policy
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more
Name *
Sensitive-apps-alikoc
Assignments
Users
All users
Target resources
1 authentication context included
Conditions
0 conditions selected
Access controls
Grant
Control access based on all or specific network access traffic, cloud apps or actions.
Learn more
Select what this policy applies to
Authentication context
Authentication context is used to secure application data and actions in apps like SharePoint and Microsoft Cloud App Security.
Learn more
Select the authentication contexts this policy will apply to
Sensitive-Alikoc-Test-Context
Enable policy
Report-only
On
Off
Create


ali.koc@cyberwise.com.tr
CYBERWISE (SECURRENT.COM)
Home > Endpoint security | Conditional access > Conditional Access | Policies >
New
Conditional Access policy
Sensitive-apps-alikoc
Assignments
Users
All users
Target resources
1 authentication context included
Conditions
0 conditions selected
Access controls
Grant
1 control selected
Session
Over-prompting users can occur when the "Sign-in Frequency - every time" setting is enabled with authentication contexts. Read more about the recommended scenarios.
Enable policy
Report-only
On
Off
Create
Grant
Control access enforcement to block or grant access. Learn more
Block access
Grant access
Require multifactor authentication
Consider testing the new "Require authentication strength". Learn more
Require authentication strength
"Require authentication strength" cannot be used with "Require multifactor authentication". Learn more
Require device to be marked as compliant
Select



Sign-in Frequency – Every Time ayarı ile,

- Hassas uygulamalara erişim.
- VPN veya Hizmet Olarak Ağ (NaaS) sağlayıcılarının arkasındaki kaynakların güvenliğini sağlama.
- PIM'de ayrıcalıklı rol yükseltmeyi güvence altına alma.
- Azure Sanal Masaüstü makinelerinde kullanıcı oturum açma işlemlerini koruma.
- Microsoft Entra ID Protection tarafından belirlenen riskli kullanıcıları ve riskli oturum açma işlemlerini koruma.
- Microsoft Intune kaydı gibi hassas kullanıcı işlemlerinin güvenliğini sağlama.

Politikayı oluştururken yöneticiler, kullanıcıların her seferinde yeniden kimlik doğrulaması yapmasını gerektiren bir politikayı zorunlu kıldıkları uygulama sayısını sınırlamalıdır. Yeniden kimlik doğrulamanın çok sık tetiklenmesi, güvenlik sorunlarını o kadar artırabilir ki, kullanıcıların MFA yorgunluğu yaşamasına ve kimlik avı girişimlerine kapı açmasına neden olabilir. Web uygulamaları, her etkinleştirildiğinde yeniden kimlik doğrulama gerektirdiğinde genellikle masaüstü benzerlerine göre daha az rahatsız edici bir deneyim sağlar.

Bir sonraki makalede görüşmek üzere.

techcommunity.microsoft.com