How do I configure my authentication endpoint for use with ESET Secure Authentication (ESA)

Ondersteuning | ESET Nederland - 2017-11-28 - Comments (0) - ESET Secure Authentication

https://support.eset.com/kb3403

Issue

Configure ESET Secure Authentication (ESA) for use with your authentication endpoint

Solution

VPN Types

ESA differentiates three VPN types based on the way they handle authentication in an Active Directory (AD) environment.

1. VPN does not validate AD user name and password

All VPNs should support this scenario.

Requirements

Configure the authentication of your VPN connection to use RADIUS authentication pointing to a RADIUS server you configured in ESA Management Console.

How does it work?

SMS authentication: Users try to log in using their AD username and password. Entering correct credentials acts as a failed login attempt, but the user receives an OTP via SMS, and upon next login attempt the user enters the received OTP alone into the password field.

Mobile OTP / Hard Token authentication: Users log in using their AD username and password, while the password and OTP are

concatenated.

Push authentication: Users attempt to log in using their AD login credentials. A push notification is generated on user's mobile device. Approving the notification results in successful login.

> NOTE:
> If a user has both SMS and Push authentication enabled, only SMS will work in this case.

User without 2FA / whitelisted user: Users log in using their AD login credentials. ESA validates the password.

2. VPN validates AD user name and password

Make sure the VPN supports this and is configured correctly. Incorrect configuration can lead to skipping AD password verification.

Requirements

Set up one Active Directory authentication pointing to your Active Directory server and one RADIUS authentication pointing to ESA RADIUS server.

How does it work?

VPN provides two password fields, first one for the user's AD password, second one for OTP.

SMS authentication: There are two login attempts required. On first one, users enter their AD password to the first password field, and into the second one they type "sms", without quotation marks. If correct AD username and password was supplied, the login screen will show up again without any error message, and the user receives an OTP via SMS. On second login attempt the user enters the received OTP into the second password field.

Mobile OTP / Hard Token authentication: Users enter the generated OTP into the second password field.

Push authentication: Users leave the second password field empty, or type "none" or "push" without quotation marks into that field. ESA generates a push notification and waits for its approval.

User without 2FA / whitelisted user: Users leave the second

password field empty, or type "none" or "push" without quotation marks into that field.

3. Use Access-Challenge feature of RADIUS

Only some VPNs support this, and it must be configured correctly on the VPN server.

Requirements

Configure the authentication of your VPN connection to use RADIUS authentication pointing to a RADIUS server you configured in ESA Management Console.

How does it work?

The login has 2 phases, generic AD login and entering OTP or approving push notification. The VPN displays a popup dialog or another page to enter the OTP or waits for approval of push notification.

SMS authentication: Users log in using their AD login credentials, in the next screen or popup dialog they enter the OTP received via SMS.

Mobile OTP / Hard Token: Users log in using their AD login credentials, in the next screen or popup dialog they enter the generated OTP.

Push authentication: Users log in using their AD login credentials and approve the generated push notification.

> NOTE:
> If the user has only Push authentication enabled, there is no subsequent dialog or page displayed requesting OTP or informing about waiting for approval of push notification, but the user has to approve the push notification, otherwise the login attempt fails.

User without 2FA / whitelisted user: Users use only AD login credentials.

Integration guides

Click the appropriate link below to view the ESET Secure Authentication integration guide for your configuration. The integration guides are

designed to be used in combination with the ESET Secure Authentication Verifying ESA RADIUS functionality document. Note that some of the guides might be outdated and serve as a sample. For up-to-date integration guide consult the vendor of your VPN applience with regard to supported VPN types described above.

VPN, Firewall and UTM endpoints:

Barracuda
Check Point Software
Cisco ASA IPsec
Cisco ASA SSL
Citrix Access Gateway
Citrix Netscaler
Cyberoam
F5 Firepass
Fortinet Fortigate
Juniper
Juniper (Access-Challenge)
Microsoft RRAS
Microsoft RRAS with NPS
Microsoft Forefront Threat Management Gateway
Netasq
OpenVPN Access Server
Palo Alto
Sonicwall

Cloud and VDI endpoints

VMWare Horizon View
Citrix XenApp server

In addition to the application-specific integration guides, we recommend that you also read the ESET Secure Authentication Product Manual or the ESET Secure Authentication Installation Guide (if installing older 1.X versions) when implementing ESET Secure Authentication. If you plan to add ESET Secure Authentication to an existing application using the ESET Secure Authentication API, the ESET Secure Authentication API User Guide and ESET Secure Authentication SSL Certificate Replacement documents are also available.

- Tags
- Endpoint
- ESA