



Enabling Multifactor Authentication on Sophos Firewall

Sophos Firewall
Version: 19.0v1

Multi-factor Authentication

Multi-factor authentication means that two pieces of information are required to login:

- Something you **know**
- Something you **have**



Sophos Firewall supports multi-factor authentication using one-time passwords



One-time passwords can be software tokens or hardware tokens that conform to RFC 6238

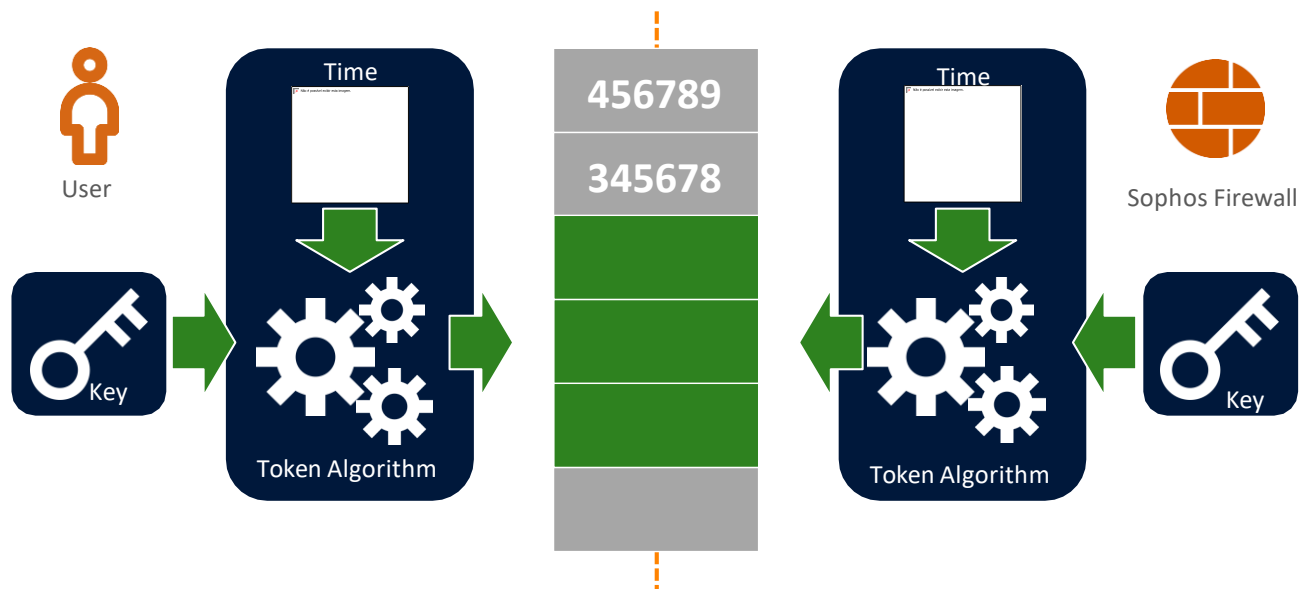
SOPHOS

A autenticação multifator significa que duas informações são necessárias para fazer login: algo que você conhece, sua senha e algo que você tem, seu token
O Sophos Firewall suporta autenticação multifator usando senhas únicas.

Existem diferentes tipos de senha de uso único. Você pode usar tokens de software, como o Sophos Authenticator App ou o Sophos Intercept X App que estão disponíveis para Android e iOS, ou tokens de hardware, se estiverem em conformidade com a RFC 6238.

Observe que os tokens RSA não são suportados.

One-Time Passwords



SOPHOS

Vejamos como as senhas de uma vez funcionam. Neste diagrama, temos o usuário com seu token ativado à esquerda e ao Sophos Firewall à direita.

O usuário tem um token que contém uma chave e obtém a hora de um relógio sincronizado. Estes são processados usando o algoritmo descrito na RFC 6238 para produzir o código do token.

O Sophos Firewall precisa ter a mesma chave e ser sincronizado com o mesmo relógio para que, quando ele calcula o código do token, ele saia com o mesmo número.

Para permitir variações no tempo entre o token e o Sophos Firewall, ele aceitará o código de token anterior e seguinte como válido por padrão. Esta é a etapa de deslocamento de token e pode ser alterada nas configurações.

Configuration

The screenshot displays the 'Authentication' configuration page in the Sophos Firewall interface. The 'Multi-factor authentication' tab is active, showing settings for 'Multi-factor authentication (MFA) settings'. Key elements include:

- One-time password (OTP):** Radio buttons for 'No OTP', 'All users' (selected), and 'Specific users and groups'. A green callout box points to 'All users'.
- Generate OTP token with next sign-in:** A toggle switch is turned 'ON'. A green callout box points to this toggle.
- Require MFA for:** A section with checkboxes for 'User portal' (checked), 'Web admin console' (checked), 'SSL VPN remote access' (unchecked), and 'IPsec remote access' (unchecked). A green callout box points to this section.
- OTP timestep settings:** Fields for 'Default token timestep' (30), 'Maximum verification code offset' (2), and 'Maximum initial verification code offset' (10). A green callout box points to the 'Default token timestep' field.

A autenticação multifator não está habilitada por padrão e deve estar ativada. Isso pode ser feito para todos os usuários ou um conjunto selecionado de usuários e grupos.

Você pode optar por fazer com que o Sophos Firewall gere automaticamente um segredo de token (chave) quando os usuários tentarem autenticar e não tiverem um. Os segredos gerados pelo Sophos Firewall podem ser usados com tokens de software. Os tokens de hardware precisam ser adicionados manualmente.

O Sophos Firewall pode usar a autenticação multifator para melhorar a segurança do WebAdmin, do Portal do Usuário (incluindo o Portal VPN Sem Cliente) e das VPNs de acesso remoto SSL e IPsec.

Você pode definir as configurações de token global. Por exemplo, se você estiver usando um token de hardware com uma etapa de tempo de 60 segundos, poderá configurá-lo aqui. Você também pode configurar as etapas de deslocamento de senha que discutimos no slide anterior.

Adding Tokens Manually

The screenshot shows the Sophos Firewall web interface. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The 'Authentication' page is active, with tabs for 'Servers', 'Services', 'Groups', 'Users', 'Multi-factor authentication', 'Web authentication', 'Guest users', 'Clientless users', and 'STAS'. The 'Add OTP token' form is displayed with the following fields: 'Secret *' (containing a 32-character hexadecimal string), 'User' (a dropdown menu with 'training-user' selected), 'Description' (empty), 'Use custom token timestep' (a toggle switch set to 'ON'), and 'Timestep' (a text box with '60' and a unit of 'Seconds (10-300 seconds)'). A green callout bubble points to the 'Use custom token timestep' toggle with the text 'Optionally override the global token timestep'. A 'Requirements' box on the right lists: 'Only hexadecimal characters' (green check), 'Even character count' (red X), 'Minimum characters: 32' (red X), and 'Maximum characters: 120' (green check). At the bottom are 'Save' and 'Cancel' buttons.

Para adicionar um token, basta especificar o segredo, que é uma cadeia de caracteres HEX de 32 a 120 caracteres. e selecione a qual usuário atribuir o token.

Opcionalmente, a etapa de tempo global pode ser substituída, o que pode ser necessário se você estiver usando uma mistura de tokens.

Adding Tokens Automatically

SOPHOS


Proceed to login

OTP tokens for training-user

Description

To enter the user portal you have to authenticate with a one-time password. Scan the QR code below with Sophos Authenticator on your phone. The app will then generate a new passcode every timestep seconds. From then on, your password, directly followed by the passcode displayed, is the one-time password you have to enter to log in.

Unused auto-generated OTP tokens



Account: training-user@C01001CP99YB30E

Secret (HEX): 6a0be3a1378260edf28d1e0dfc244262

Secret (BASE32): NIF6HLJXQJQ034UNDYG7YJCCMI

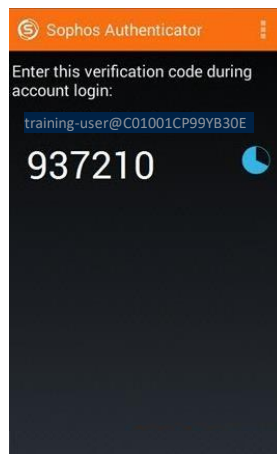
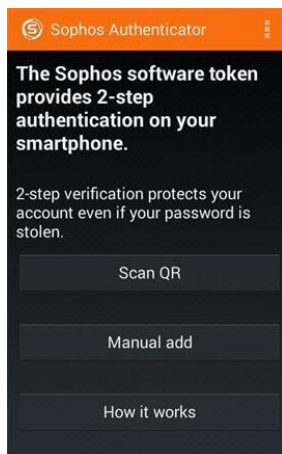
Timestep: 30s

The password becomes <User_Password><Generated_Password>

Agora vamos ver como os tokens podem ser gerados automaticamente para os usuários. Quando um usuário faz login no Portal do Usuário pela primeira vez após a habilitação de senhas únicas, o Sophos Firewall gera e exibe as informações necessárias para configurar um token de software. Na maioria dos casos, isso pode ser feito automaticamente digitalizando o código QR com um aplicativo, como o aplicativo Sophos Authenticator.

Depois que o token estiver configurado, o usuário clicará em Continuar para fazer login. O usuário será então apresentado com o login do Portal do Usuário novamente. Desta vez, eles fazem login com seus senha e anexar seu código de token atual.

Sophos Authenticator App



SOPHOS

Isso mostra um exemplo da senha gerada no aplicativo Sophos Authenticator.

Additional Token Settings

Issued tokens

Add token (for hardware tokens) Delete

<input type="checkbox"/>	Username ▾	Status	Name ▾	Description	Manage
<input type="checkbox"/>	training-user	ON	Training User	Auto-generated token for user training-user	

OTP time-offset synchronization

Enter the passcode displayed on the token (secret "98940a690b719f8bc4ca66fc230ad707") to synchronize its time-offset with the server. The offset currently set for this token is -30 seconds.

Token passcode (8 digits)

Check Cancel

SOPHOS

Aqui podemos ver um token para o usuário de treinamento que usaremos para considerar dois cenários.

No primeiro cenário, o usuário tem seu token, mas o logon está falhando.

Isso pode ser causado se a hora do token e do Sophos Firewall estiverem fora de sincronia. Para resolver isso, você pode inserir a senha atual no firewall e ele pode compensar a diferença de horário.

Additional Token Settings

SOPHOS Firewall

Authentication

Feedback | How-to guides | Log viewer | Help | admin | Sophos Training

Servers | Services | Groups | Users | **Multi-factor authentication** | Web authentication | Guest users | Clientless users | STAS

Edit OTP token

Secret: [Redacted]

User: training-user

Description: Auto-generated token for user training-user

Use custom token timestep: ☒

Timestep: 60 Seconds (10-300 seconds)

Additional codes: [Search / Add] +

Save Cancel

Generate 10 one-time codes that can be used

SOPHOS

No segundo cenário, o usuário está na estrada, mas caiu e quebrou o celular que tem o aplicativo Sophos Authenticator nele. Eles precisam acessar a VPN SSL, mas ela é protegida usando OTP.

Se isso acontecer, você poderá adicionar códigos adicionais ao token. Estes são um conjunto de códigos de uso único que serão automaticamente removidos depois de serem usados. Eles teriam que ser enviados ao usuário de alguma forma, de preferência através de um canal seguro, depois de terem sido criados. Esses códigos persistirão até que sejam usados ou um administrador os remova.

Simulation: Enable Multifactor Authentication



In this simulation you will enable multi-factor authentication on Sophos Firewall. You will then test your configuration.

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/fw/simulation/MFA/1/start.html>

SOPHOS

Nesta simulação, você habilitará a autenticação multifator no Sophos Firewall. Em seguida, você testará sua configuração.

[Informações adicionais]

<https://training.sophos.com/fw/simulation/MFA/1/start.html>