



FORTINET®



# SIA Agentless SWG Deployment Guide

FortiSASE



DEFINE / DESIGN / **DEPLOY** / DEMO



# Table of Contents

<b>Change log</b> .....	4
<b>Deployment overview</b> .....	5
Intended audience .....	6
About this guide .....	6
Design concept and considerations .....	7
Proxy configuration .....	7
User configuration .....	7
Product prerequisites .....	8
Deployment plan .....	8
<b>Deployment procedures</b> .....	9
Provisioning your FortiSASE instance .....	9
Configuring SSO SAML users .....	9
Configuring RADIUS users .....	11
Configuring security profiles and SWG policies .....	12
Customizing the PAC file .....	13
Downloading the preconfigured PAC file .....	14
Downloading, customizing, and hosting the PAC file .....	14
Hosting the custom PAC file .....	17
Installing the FortiSASE CA certificate on endpoints .....	17
Windows .....	18
macOS .....	18
Chrome OS .....	18
Managed Chromebook .....	19
Configuring proxy settings on endpoints .....	20
Windows .....	21
macOS .....	21
Chrome OS .....	22
Managed Chromebook .....	24

---

(Optional) Installing and configuring the SWG Chrome extension .....	25
Testing SWG user connections to the Internet .....	28
<b>More information</b> .....	31
Appendix A: Documentation references .....	31
Feature documentation .....	31
4-D resources: SASE .....	31

---

# Change log

Date	Change description
2024-08-09	Initial release.

---

# Deployment overview

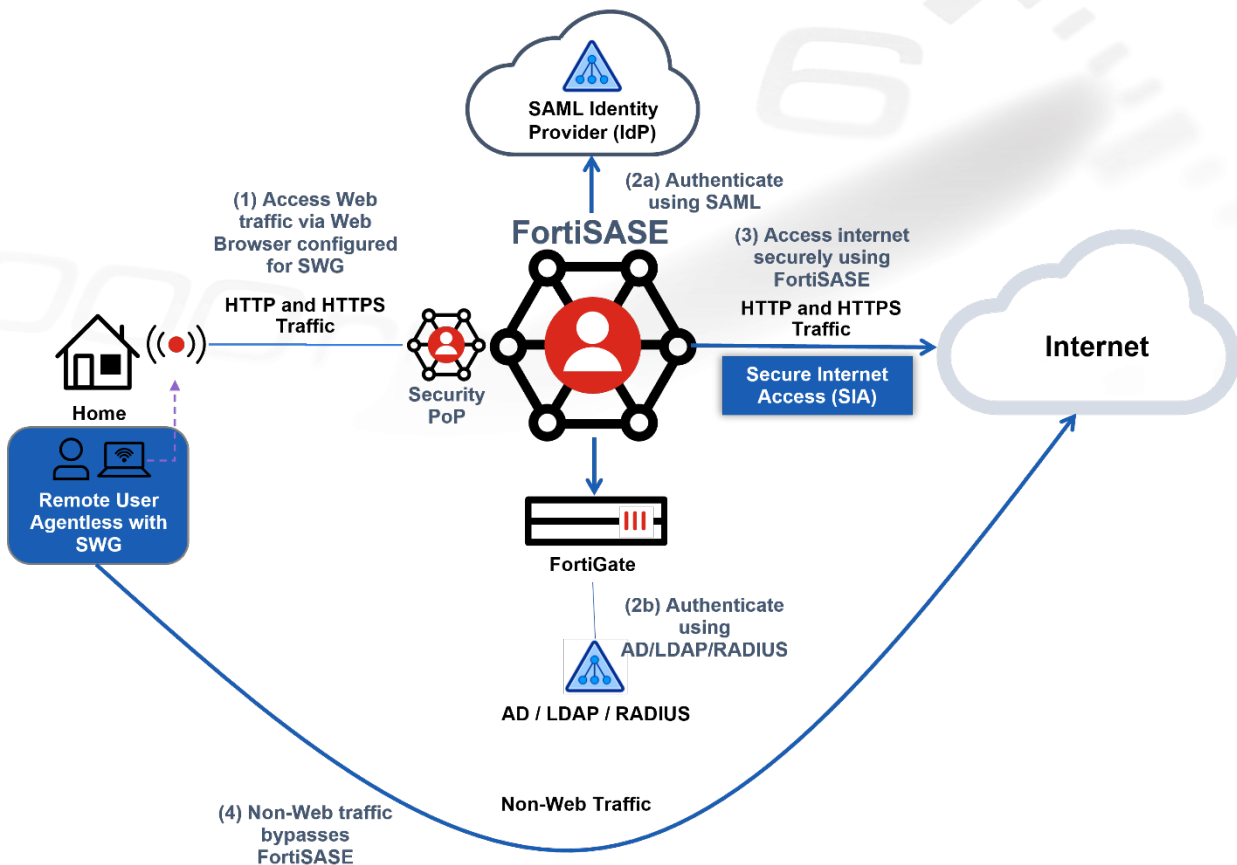
FortiSASE secure internet access (SIA) extends an organization's security perimeter that a next generation firewall typically achieves to remote users by enforcing common security policy for Intrusion Prevention Systems and Application Control, web and DNS filtering, antimalware, sandboxing, and antibotnet/command and control.

SIA for agentless remote users involves setting up a web browser, or a browser-based device using a proxy autoconfiguration (PAC) file to use the FortiSASE secure web gateway (SWG) service as an explicit web proxy. The web browser redirects HTTP and HTTPS traffic to the SWG, which secures user web traffic by implementing SWG security policies. All other non-web traffic bypasses FortiSASE and is forwarded to the internet directly.

You can achieve agentless remote user authentication by configuring the authentication source as Active Directory/LDAP or RADIUS or as a SAML identity provider.

You can automate initial configuration of the proxy settings for web browsers using Windows group policy objects or Microsoft System Center Configuration Manager.

A typical topology for deploying this example design is as follows:



This deployment guide describes how to configure FortiSASE SIA for agentless remote users to redirect, or forward traffic to the FortiSASE SWG or explicit proxy.

## Intended audience

Midlevel network and security architects, engineers, and administrators in companies of all sizes and verticals looking to deploy FortiSASE SIA for agentless remote users using FortiSASE SWG should find this guide helpful. A working knowledge of FortiOS, FortiGate, and web browser proxy configuration is helpful.

For comments and feedback about this document, visit [FortiSASE Secure Web Gateway Deployment](https://community.fortinet.com) on [community.fortinet.com](https://community.fortinet.com).

## About this guide

This deployment guide describes the steps involved in deploying a specific architecture for the FortiSASE SIA use case for agentless remote users using SWG.

Readers should first evaluate their environment to determine whether the architecture outlined in this guide suits them. Reviewing the reference architecture guide(s), such as the [FortiSASE Architecture Guide](#), is advisable if readers are in the process of selecting the right architecture. See also the [FortiSASE Concept Guide](#).

This deployment guide presents one of possibly many ways to deploy the solution. It may also omit specific steps where readers must make design decisions to further configure their devices. It is recommended that readers also review supplementary material found in product administration guides, example guides, cookbooks, release notes, and other documents where appropriate on the [Fortinet Document Library](#).

## Design concept and considerations

### Proxy configuration

This solution's design uses FortiSASE secure web gateway agentless mode, which involves configuring and hosting a proxy autoconfiguration (PAC) file for respective endpoints to connect to the FortiSASE gateway. FortiSASE provides a preconfigured PAC file hosted on the FortiSASE server for use. You can download and customize the PAC to exclude the SSL VPN gateway and internal networks from being proxied. The customer server must host the custom PAC file.

Once the PAC file is hosted, endpoint computers must be configured to enable the proxy server and point to the PAC file to retrieve the proxy settings. On a Windows machine, configuring proxy settings at the operating system (OS) level is recommended so that all traffic is proxied. On other OSes where there is no option to configure proxy settings at the OS level, you can configure the browser to point to the PAC file.

To centrally manage proxy settings on endpoints, customers should consider using group policy management for Windows or other centralized management systems like mobile device management.

### User configuration

You configure users on FortiSASE for endpoints to authenticate and connect to the FortiSASE gateway. If SAML SSO is enabled on FortiSASE, you cannot configure an LDAP or RADIUS connection. When designing the solution, consider where users are defined in your organization and use one of the following methods to integrate it with FortiSASE:

User type	Integration method
LDAP	<ol style="list-style-type: none"><li>1. Configure an LDAP connection.</li><li>2. Import users and groups from the LDAP server to FortiSASE.</li></ol>
RADIUS	<ol style="list-style-type: none"><li>1. Configure a RADIUS connection.</li><li>2. Import users and groups from the RADIUS server to FortiSASE.</li></ol>
Single sign on (SSO)	Configure an SSO connection, with FortiSASE as the service provider and another service, such as Azure Active Directory, as the identity provider.

See [Authentication Sources and Access](#) for information on authentication methods.

---



SSO authentication is strongly recommended for SWG users. See [Known issues](#) for details.

See [Configuring SSO SAML users on page 9](#) for steps on configuring SSO authentication for SWG users.

---

## Product prerequisites

Customers should obtain enough FortiSASE Secure Web Gateway seats to support the number of remote endpoints that will use this service.

## Deployment plan

This outlines the major steps to deploy this solution. Go to [Deployment procedures on page 9](#) for detailed configuration steps:

1. Provision your FortiSASE instance and select the regions where your users will be located. Input licenses as needed. See [Provisioning your FortiSASE instance on page 9](#).
2. Configure users. See [Configuring SSO SAML users on page 9](#) and [Configuring RADIUS users on page 11](#).
3. Configure Secure Web Gateway policies to apply desired scanning and filtering for your users. See [Configuring security profiles and SWG policies on page 12](#).
4. Download the proxy autoconfiguration (PAC) file from the FortiSASE portal. Customize the file to exclude SSL VPN gateway and internal corporate networks. Host the custom PAC file on an externally accessible server. See [Customizing the PAC file on page 13](#).
5. Install the FortiSASE CA certificate on endpoints using steps that are specific to each operating system. See [Installing the FortiSASE CA certificate on endpoints on page 17](#).
6. Configure proxy settings on endpoints to point to the PAC file. See [Configuring proxy settings on endpoints on page 20](#).
7. (Optional) Configure the FortiSASE SWG Chrome extension for managed Chrome browsers and Chromebook support. See [\(Optional\) Installing and configuring the SWG Chrome extension on page 25](#).
8. Test connections to the Internet on a SWG user device. See [Testing SWG user connections to the Internet on page 28](#).

---

# Deployment procedures

## Provisioning your FortiSASE instance

Ensure that you have purchased the contract to provision FortiSASE.

To provision your FortiSASE instance:

1. From the [Fortinet Support site](#), register your FortiSASE contract.
2. Once registered, go to *Services > Cloud Services > FortiSASE* to provision your FortiSASE instance.
3. When provisioning, select the geographic location for your security sites and logging.
4. Once provisioned, the FortiSASE dashboard displays your entitlement in the *Remote User Management* widget. The number of FortiSASE SWG users that the widget lists is the number of users that are entitled to use this service in SWG agentless mode.
5. Go to *System > SWG Configuration*. Toggle *Enable* to on, then click *OK*. The GUI may take a few minutes to reload to display SWG configuration options in the menu.



SSO authentication is strongly recommended for SWG users. See [Known issues](#) for details.

See [Configuring SSO SAML users on page 9](#) for steps on configuring SSO authentication for SWG users.

---

## Configuring SSO SAML users



SSO authentication is strongly recommended for SWG users. See [Known issues](#) for details.

See [Configuring SSO SAML users on page 9](#) for steps on configuring SSO authentication for SWG users.

---

Depending on the authentication source, the user configuration steps differ. This example shows configuring single sign on (SSO) users and user groups against an Azure Active Directory (AD) identity provider (IdP).

For configuring other authentication sources, see [Authentication Sources and Access](#). When SSO is configured, other user types do not work.

To configure the SSO SAML configuration:

1. Go to *Configuration > SWG User SSO*.
2. In step one, *Configure Identity Provider*, collect the URLs on FortiSASE and enter them into the respective fields in the SSO settings of the respective Azure AD enterprise application.

FortiSASE SAML field	Azure AD Basic SAML Configuration field
Entity ID	Identifier (Entity ID)
Assertion Consumer Service (ACS) URL	Reply URL (Assertion Consumer Service URL)
Portal (Sign On) URL	Sign on URL
Single Logout Service (SLS) URL	Logout Url (Optional)

Click *Next*.

3. In step two, *Configure Service Provider*, collect the URLs from the Azure AD enterprise application *Single sign-on > Set up <application name>*. Enter them into the respective fields in FortiSASE.

Azure AD > Set up <application name> fields	FortiSASE SAML field
Login URL	IdP Single Sign-On URL
Azure AD Identifier	IdP Entity ID
Logout URL	IdP Single Log-Out URL

Click *Next*.

4. With claims mapping, you can specify the identifier for the username and group name attributes in Azure. The default configuration uses username and group respectively, which matches the attribute names in Azure. If you need custom names, modify them here.
5. Enable and configure *SAML Group Matching* if you only want Azure AD users of a certain group to be allowed to authenticate. Otherwise, leave this setting disabled. You can further define more granular groups when you configure user group settings.
6. FortiSASE requires the IdP certificate is required. Configure the IdP certificate. Download the certificate from Azure AD enterprise application > *Single sign-on > SAML Signing Certificate*. Download Certificate (Base64).
  - a. On the *IdP Certificate* dropdown list, click *Create*.
  - b. In the *Import Remote Certificate* slide-in, upload the certificate from Azure.
  - c. Enter a unique name for the certificate, then click *OK*.
  - d. Select the certificate, then click *Next*.
7. In the *Service Provider Certificate* field, use *FortiSASE Default Certificate* or your own custom certificate. Click + to add your own custom certificate.
8. For *Digest Method*, select *SHA-1* or *SHA-256*. The digest method should match the digest method on Azure if *Certificate Verification* is enabled on Azure.



*FortiSASE Default Certificate* is a built-in wildcard certificate on FortiSASE signed by a well-known public CA and remains same across all of your points of presence.

*FortiSASE Default Certificate* also periodically renews. Thus, if the IdPs are using *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with new SP certificate. To avoid having to update your IdP configuration frequently, we recommend uploading your own certificate.

9. Review your settings. The click *Submit* to apply. Upon successful configuration, FortiSASE prompts for instructions to onboard users. Follow the steps under *SWG Users* to download the SWG certificate for usage on the client. The certificate package contains the built-in certificate authority certificate for the FortiSASE instance. This must be installed in the certificate store on the client to trust the certificate chain for pages that FortiSASE has signed.

To configure an SSO user group:

1. Go to *Configuration > Users*.
2. Click *Create*. Select *User Group*, and click *Next*.
3. In the *Name* field, enter the desired name.
4. Under *Remote Groups*, click *Create*.
5. From the *Remote Server* dropdown list, select the SAML server that you created.
6. In the *Groups* field, enter the names of the group(s) that you will allow access on FortiSASE. This is the group object ID of the user group defined on Azure.
7. Click *OK* to finish. Click *OK* again to create the user group. You can apply this new user group to your SWG policies.

## Configuring RADIUS users



SSO authentication is strongly recommended for SWG users. See [Known issues](#) for details.

See [Configuring SSO SAML users on page 9](#) for steps on configuring SSO authentication for SWG users.

Depending on the authentication source, the user configuration steps differ. The example shows configuring a RADIUS server and user groups. For configuring other authentication sources, see [Authentication Sources and Access](#).

If Secure Web Gateway (SWG) user single sign on (SSO) is configured, RADIUS user configuration does not take effect. If you plan to use RADIUS, first delete your SWG user SSO configuration.

To configure the RADIUS server:

1. Go to *Configuration > RADIUS*.
2. Click *Create* to add a new RADIUS server.
  - a. Configure the RADIUS server settings:
  - b. Enter the desired server name.
  - c. Do not enable *Include All Users* unless you want all users on the RADIUS server to be allowed access to FortiSASE.

- d. Click *Next*.
  - e. In the *Primary Server > IP/Name* field, enter the primary server IP address or fully qualified domain name.
  - f. In the *Primary Server > Secret* field, enter the primary server secret.
  - g. If your organization has a redundant RADIUS server, enter its information in the *Secondary Server* section.
3. Click *Test Connection*.
  4. Do one of the following:
    - a. If the connection succeeds, click *Next*.
    - b. If the connection does not succeed, try again. Confirm your RADIUS server allows traffic from the FortiSASE gateway IP address. This may require sniffing for traffic on port 1812.
  5. Review and submit the settings.

To configure a RADIUS user group:

1. Go to *Configuration > Users*.
2. Click *Create*.
3. Configure the RADIUS user group(s):
  - a. In the *Name* field, enter the desired name.
  - b. Under *Remote Groups*, click *Create*.
  - c. From the *Remote Server* dropdown list, select the RADIUS server that you created.
  - d. In the *Groups* field, enter the group names of the group(s) that will be allowed access on FortiSASE.

4. Click *OK*.
5. Click *OK* again.
6. A slide-in appears with instructions on how to onboard an end user. Follow the steps under *SWG Users* to download the SWG certificate for usage on the client. The certificate package contains the built-in certificate authority certificate for the FortiSASE instance. This must be installed in the certificate store on the client to trust the certificate chain for pages that FortiSASE has signed.
7. Click *Close*.

## Configuring security profiles and SWG policies

FortiSASE has a default security profile configured, which is applied to the Allow-All Secure Web Gateway (SWG) policy. When all users, sources, and destinations require the same scanning and protection, maintaining only one default security profile suffices. However, if different users, sources, or destinations require different protection, create different profile groups for each group of users.

The default SWG policies block any traffic destined for Botnet and C&C servers but allow the rest. Consider your user base and design your SWG policies carefully. FortiSASE matches policies from top down, so add more restrictive policies at the top and less restrictive policies at the bottom.

To configure a new security profile:

1. Go to *Configuration > Security*.
2. On the top-right, click the dropdown list beside *Profile Group*, then click *Create*.

3. In the *Create Profile Group* slide-in, enter a name for the new profile.
4. In *Initial Configuration*, select whether to use a basic initial configuration or base the profile on an existing profile.
5. Click *OK*.
6. On the top-right, click the dropdown list again, and select your newly created profile.
7. Edit the profile as desired. See [Security](#) for details.

To create an SWG policy:

1. Go to *Configuration > SWG Policies*.
2. Click *Create*.
3. Configure the SWG policy:
  - a. In the *Name* field, enter the desired policy name.
  - b. For *Action*, select *ACCEPT*.
  - c. In the *Source* field, specify source subnet(s) as desired.
  - d. In the *User* field, specify the user group used for your remote users.
  - e. In the *Destination* field, specify destination subnet(s) as desired.
  - f. In the *Profile Group* field, specify the profile that you created.
  - g. In the *Log Allow Traffic* field, select *All Sessions*.
4. Click *OK*.
5. Move the new policy above the Allow-All policy.

## Customizing the PAC file

FortiSASE secure web gateway (SWG) agentless mode involves configuring and hosting a proxy autoconfiguration (PAC) file for respective endpoints to connect to the FortiSASE gateway.

A PAC file is based on JavaScript and contains rules for the proxy client to follow to route traffic to the proxy server or directly to the Internet. For FortiSASE SWG users:

- The proxy client is a web browser or another proxy-aware application.
- The proxy server is the FortiSASE SWG.
- Routing traffic to the proxy uses the FortiSASE SWG as a web proxy.
- Routing traffic directly to the Internet bypasses the FortiSASE SWG.

Typically, some web applications require traffic to be routed directly to the Internet for specific domains which do not support redirection for security reasons or are required for authentication, such as common SAML identity providers, to load correctly. In these cases, you must customize the PAC file with specific IP addresses and hostnames, and then host the custom PAC file on a server that the endpoints can access.

The workflow for customizing and using a PAC file is as follows:

1. FortiSASE provides a preconfigured PAC file hosted on the FortiSASE server for use. Download the PAC file to a computer for editing.
2. Customize the PAC file in a text editor to exclude certain hosts from being proxied.
3. Host the custom PAC file on a server accessible by the endpoints.
4. On an endpoint, download and install the SWG certificates provided in the FortiSASE portal.
5. On an endpoint, install and configure the client browser or OS settings to point to the hosted custom PAC file.

## Downloading the preconfigured PAC file

The *System > SWG Configuration* page displays the Secure Web Gateway (SWG) servers, port, and hosted proxy autoconfiguration (PAC) file. You can download the predefined PAC file to customize.

By default, the FortiSASE hosted PAC file contains the global (recommended) URL and the SWG port specific to your instance. This global (recommended) URL automatically directs users to the closest geographical location for all browsers and proxy-aware applications. For example:

```
function FindProxyForURL(url, host) {
    return "PROXY turbo-hqwdvq17.edge.prod.fortisase.com:10925; DIRECT";
}
```

This simple PAC file specifies that the web request should be sent through the proxy server turbo-hqwdvq17.edge.prod.fortisase.com on TCP port 10925 and if the proxy does not respond to this request, the browser sends the web request directly to the Internet without using the proxy.

## Downloading, customizing, and hosting the PAC file

This example customizes the PAC file to exclude common external URLs and networks from being forwarded to the FortiSASE secure web gateway (SWG) server, which allows specific domains which do not support redirection for security reasons or are required for authentication, such as common SAML identity providers, to load correctly.

You must replace the final return statement at the end of the PAC file with the corresponding proxy URL and port listed in your preconfigured PAC file in [Downloading the preconfigured PAC file on page 14](#).

```
function FindProxyForURL(url, host) {
// Apple
if (dnsDomainIs (host, "albert.apple.com") ||
    dnsDomainIs (host, "captive.apple.com") ||
    dnsDomainIs (host, "gs.apple.com") ||
    dnsDomainIs (host, "humb.apple.com") ||
    dnsDomainIs (host, "static.ips.apple.com") ||
    dnsDomainIs (host, "sq-device.apple.com") ||
    dnsDomainIs (host, "tbsc.apple.com") ||
    shExpMatch (host, "*.push.apple.com") ||
    dnsDomainIs (host, "deviceenrollment.apple.com") ||
    dnsDomainIs (host, "deviceservices-external.apple.com") ||
    dnsDomainIs (host, "gdmf.apple.com") ||
    dnsDomainIs (host, "identity.apple.com") ||
    dnsDomainIs (host, "iprofiles.apple.com") ||
    dnsDomainIs (host, "mdmenrollment.apple.com") ||
    dnsDomainIs (host, "setup.icloud.com") ||
    dnsDomainIs (host, "vpp.itunes.apple.com") ||
    shExpMatch (host, "*.business.apple.com") ||
    shExpMatch (host, "*.school.apple.com") ||
    dnsDomainIs (host, "upload.appleschoolcontent.com") ||
    dnsDomainIs (host, "ws-ee-maidsvc.icloud.com") ||
    dnsDomainIs (host, "axm-adm-enroll.apple.com") ||
    dnsDomainIs (host, "axm-adm-mdm.apple.com") ||
    dnsDomainIs (host, "axm-adm-scep.apple.com") ||
    dnsDomainIs (host, "axm-app.apple.com") ||
    dnsDomainIs (host, "appldnld.apple.com") ||
    dnsDomainIs (host, "configuration.apple.com") ||
    dnsDomainIs (host, "gdmf.apple.com") ||
    dnsDomainIs (host, "gg.apple.com") ||
    dnsDomainIs (host, "gnf-mdn.apple.com") ||
    dnsDomainIs (host, "gnf-mr.apple.com") ||
```

```

dnsDomainIs (host, "gs.apple.com") ||
dnsDomainIs (host, "ig.apple.com") ||
dnsDomainIs (host, "mesu.apple.com") ||
dnsDomainIs (host, "ns.itunes.apple.com") ||
dnsDomainIs (host, "oscdn.apple.com") ||
dnsDomainIs (host, "osrecovery.apple.com") ||
dnsDomainIs (host, "skl.apple.com") ||
dnsDomainIs (host, "swcdn.apple.com") ||
dnsDomainIs (host, "swdist.apple.com") ||
dnsDomainIs (host, "swdownload.apple.com") ||
dnsDomainIs (host, "swscan.apple.com") ||
dnsDomainIs (host, "updates-http.cdn-apple.com") ||
dnsDomainIs (host, "updates.cdn-apple.com") ||
dnsDomainIs (host, "xp.apple.com") ||
shExpMatch (host, "*.itunes.apple.com") ||
shExpMatch (host, "*.apps.apple.com") ||
shExpMatch (host, "*.mzstatic.com") ||
dnsDomainIs (host, "itunes.apple.com") ||
dnsDomainIs (host, "ppq.apple.com") ||
dnsDomainIs (host, "appldnld.apple.com") ||
dnsDomainIs (host, "appldnld.apple.com.edgesuite.net") ||
dnsDomainIs (host, "itunes.com") ||
dnsDomainIs (host, "itunes.apple.com") ||
dnsDomainIs (host, "updates-http.cdn-apple.com") ||
dnsDomainIs (host, "updates.cdn-apple.com") ||
dnsDomainIs (host, "lcdn-registration.apple.com") ||
dnsDomainIs (host, "suconfig.apple.com") ||
dnsDomainIs (host, "xp-cdn.apple.com") ||
dnsDomainIs (host, "lcdn-locator.apple.com") ||
dnsDomainIs (host, "serverstatus.apple.com") ||
dnsDomainIs (host, "17.248.128.0/18") ||
dnsDomainIs (host, "17.250.64.0/18") ||
dnsDomainIs (host, "17.248.192.0/19") ||
shExpMatch (host, "*.appattest.apple.com") ||
dnsDomainIs (host, "bpapi.apple.com") ||
dnsDomainIs (host, "csssubmissions.apple.com") ||
dnsDomainIs (host, "fba.apple.com") ||
dnsDomainIs (host, "diagassets.apple.com") ||
dnsDomainIs (host, "doh.dns.apple.com") ||
dnsDomainIs (host, "certs.apple.com") ||
dnsDomainIs (host, "crl.apple.com") ||
dnsDomainIs (host, "crl.entrust.net") ||
dnsDomainIs (host, "crl3.digicert.com") ||
dnsDomainIs (host, "crl4.digicert.com") ||
dnsDomainIs (host, "ocsp.apple.com") ||
dnsDomainIs (host, "ocsp.digicert.cn") ||
dnsDomainIs (host, "ocsp.digicert.com") ||
dnsDomainIs (host, "ocsp.entrust.net") ||
dnsDomainIs (host, "ocsp2.apple.com") ||
dnsDomainIs (host, "valid.apple.com") ||
dnsDomainIs (host, "appleid.apple.com") ||
dnsDomainIs (host, "appleid.cdn-apple.com") ||
dnsDomainIs (host, "idmsa.apple.com") ||
dnsDomainIs (host, "gsa.apple.com") ||
shExpMatch (host, "*.apple-cloudkit.com") ||
shExpMatch (host, "*.apple-livephotoskit.com") ||
shExpMatch (host, "*.apzones.com") ||
shExpMatch (host, "*.cdn-apple.com") ||
shExpMatch (host, "*.gc.apple.com") ||
shExpMatch (host, "*.icloud.com") ||
shExpMatch (host, "*.icloud.com.cn") ||

```

```

shExpMatch (host, "*.icloud.apple.com") ||
shExpMatch (host, "*.icloud-content.com") ||
shExpMatch (host, "*.iwork.apple.com") ||
dnsDomainIs (host, "mask.icloud.com") ||
dnsDomainIs (host, "mask-h2.icloud.com") ||
dnsDomainIs (host, "mask-api.icloud.com") ||
dnsDomainIs (host, "audiocontentdownload.apple.com") ||
dnsDomainIs (host, "devimages-cdn.apple.com") ||
dnsDomainIs (host, "download.developer.apple.com") ||
dnsDomainIs (host, "playgrounds-assets-cdn.apple.com") ||
dnsDomainIs (host, "playgroups-cdn.apple.com") ||
dnsDomainIs (host, "sylvan.apple.com"))
return "DIRECT";

// VMWare
if (shExpMatch (host, "*.awmdm.com"))
    return "DIRECT";

// Okta
if (shExpMatch (host, "*.okta.com") ||
    shExpMatch (host, "*.oktacdn.com"))
    return "DIRECT";

// Microsoft
if (dnsDomainIs (host, "login.microsoftonline.com") ||
    shExpMatch (host, "*.officeconfig.msocdn.com") ||
    dnsDomainIs (host, "config.office.com") ||
    dnsDomainIs (host, "graph.windows.net") ||
    dnsDomainIs (host, "enterpriseregistration.windows.net") ||
    shExpMatch (host, "*.manage.microsoft.com") ||
    dnsDomainIs (host, "manage.microsoft.com") ||
    shExpMatch (host, "*.microsoftonline.com") ||
    shExpMatch (host, "*.msauth.net"))
    return "DIRECT";

// Google
if (dnsDomainIs (host, "client1.google.com") ||
    dnsDomainIs (host, "client2.google.com") ||
    dnsDomainIs (host, "client3.google.com") ||
    dnsDomainIs (host, "client4.google.com") ||
    dnsDomainIs (host, "client5.google.com") ||
    dnsDomainIs (host, "client6.google.com") ||
    dnsDomainIs (host, "chrome.google.com") ||
    dnsDomainIs (host, "commondatastorage.googleapis.com") ||
    dnsDomainIs (host, "dl-ssl.google.com") ||
    dnsDomainIs (host, "dl.google.com") ||
    dnsDomainIs (host, "gweb-gettingstartedguide.appspot.com") ||
    dnsDomainIs (host, "m.google.com") ||
    dnsDomainIs (host, "hangouts.google.com") ||
    dnsDomainIs (host, "pack.google.com") ||
    dnsDomainIs (host, "safebrowsing-cache.google.com") ||
    dnsDomainIs (host, "safebrowsing.google.com") ||
    dnsDomainIs (host, "ssl.gstatic.com") ||
    dnsDomainIs (host, "storage.googleapis.com") ||
    dnsDomainIs (host, "tools.google.com") ||
    dnsDomainIs (host, "www.googleapis.com") ||
    shExpMatch (host, "*.gstatic.com") ||
    dnsDomainIs (host, "play.google.com") ||
    dnsDomainIs (host, "mtalk.google.com") ||
    dnsDomainIs (host, "accounts.google.com") ||
    dnsDomainIs (host, "aadcdn.msftauthimages.net") ||

```

```
dnsDomainIs (host, "aadcdn.msftauth.net") ||
dnsDomainIs (host, "omahaproxy.appspot.com") ||
dnsDomainIs (host, "cros-omahaproxy.appspot.com"))
return "DIRECT";
```

```
// Replace this line with the corresponding line from your FortiSASE deployment's
preconfigured PAC file
return "PROXY turbo-hqwdvq17.edge.prod.fortisase.com:10925; DIRECT";
}
```

To selectively use sections of exempted URLs above, you can comment them out using the double slash // at the beginning of each JavaScript line to prevent the URLs from being exempted and force them to go through the FortiSASE SWG.

For example, to ensure VMware Workspace One traffic is sent to the proxy, since the rule consists of an if statement and a return statement, comment them out both:

```
// VMWare
// if (shExpMatch (host, "*.awmdm.com"))
//     return "DIRECT";
```

## Hosting the custom PAC file

Once you have modified the proxy autoconfiguration (PAC) file, you should host it on a web server (such as Amazon S3) that is externally accessible by your remote users. The web server must be configured to allow .PAC file extensions to be downloaded and specified using the MIME type application/x-ns-proxy-autoconfig.

The PAC file does not require user authentication to access. However, any user that is pointing to the PAC file will be subject to authentication by FortiSASE when it accesses the Internet.

## Installing the FortiSASE CA certificate on endpoints


When users connect to FortiSASE in secure web gateway (SWG) agentless mode, FortiSASE proxies traffic from the client. While being proxied, connections using secure protocols like HTTPS have their certificates replaced and signed by FortiSASE. To avoid seeing warnings and errors, the client must trust the signing Certificate Authority (CA) and have a valid certificate chain back to the root CA. Therefore, installing FortiSASE's CA certificate on the client's trusted certificate store is important.

You should provide users with the required CA certificate during onboarding. In SWG agentless mode, when you onboard users from the GUI, download the SWG Certificates package that appears at the end of the Secure Web Gateway Users instructions. You can also find this on the right side of the *System > SWG Configuration* page.


Secure Web Gateway Users

To onboard Secure Web Gateway users, perform the following manual steps:

1. Download the certificates required for SWG from below and install them on the client.
2. Configure the proxy connection on the client using PAC file.

<https://download.fortisase.com/> proxy-qki8yrr2.pac 

3. To avoid untrusted certificate errors, ensure that the latest set of certificates is installed on all clients.

 Download SWG Certificates

The following instructions demonstrate installing certificates on various operating systems:

- [Windows on page 18](#)
- [macOS on page 18](#)

- [Chrome OS on page 18](#)
- [Managed Chromebook on page 19](#)

## Windows

To install the FortiSASE CA certificate on a Windows 10 device:

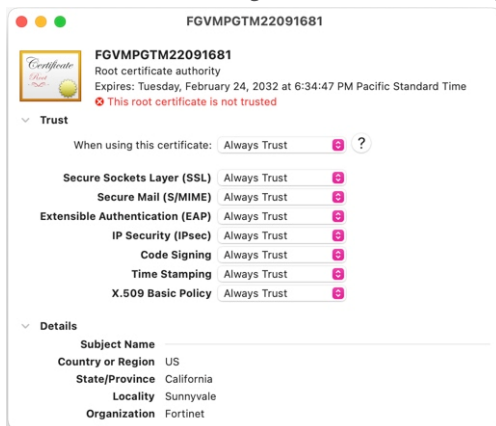
1. Double-click the FortiSASE certificate that the administrator provided during onboarding.
2. On the *General* tab, click *Install Certificate*.
3. You can install the certificate for the current user or local machine. Installing for the local machine requires administrator permissions. Select the desired option and click *Next*.
4. Choose where you want the certificate to be kept. To customize this, select *Place all certificates in the following store* and browse the store. Then select *Trusted Root Certification Authorities*. Click *Next*.
5. Review and click *Finish* to install the certificate.

## macOS

To properly browse any HTTPS websites, you must install the FortiSASE root certificate on the endpoint.

To upload the FortiSASE CA certificate on a mac:

1. Double-click the FortiSASE certificate that the administrator provided during onboarding.
2. From the *Keychain* dropdown list, select *System*, then click *Add*.
3. When you view the certificate, the root certificate appears as not trusted. Expand the *Trust* section. From the *When using this certificate* dropdown list, select *Always Trust*.



4. Save the configuration and add the certificate to the system keychain. You can connect to HTTPS websites without seeing a warning.

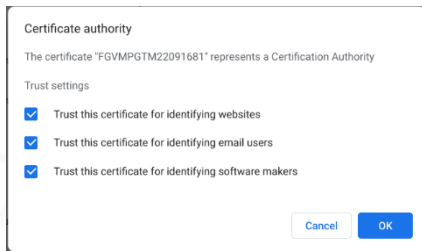
## Chrome OS

To upload the FortiSASE CA certificate on a Chromebook:

1. In Chrome, open *Settings* from the menu or go to `chrome://settings`.
2. Go to *Privacy and security*. On the configuration page, click *Security*.
3. In the *Security settings* page, scroll to the bottom to find *Advanced > Manage certificates*. Click the right arrow.
4. In the *Manage certificate* page, select *Authorities*.

## INSTALLING THE FORTISASE CA CERTIFICATE ON ENDPOINTS

5. Click *Import* to import the FortiSASE certificate authority (CA) certificate.
6. If the Fortinet\_CA\_SSL.cer file does not appear, change the file selection page to show all files. Then select the Fortinet\_CA\_SSL.cer cert and click open.
7. The next screen asks for your trust settings for this certificate. Select all options, then click *OK*.



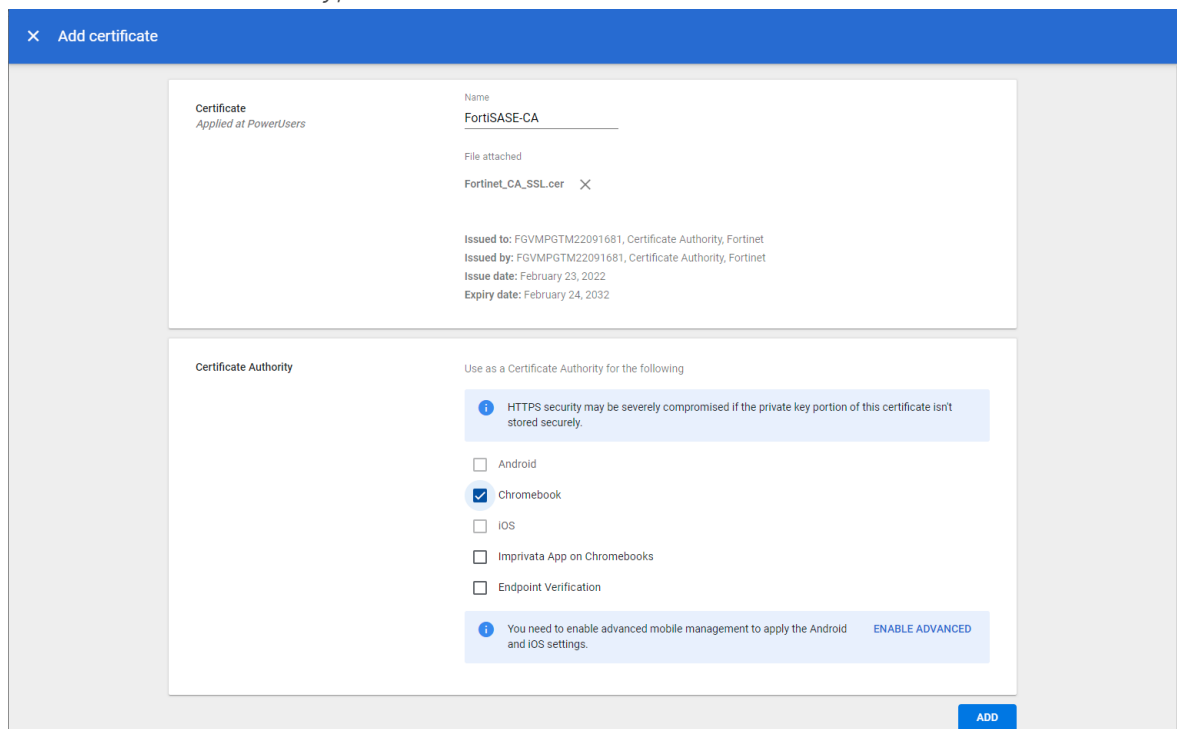
8. You have now imported the FortiSASE CA certificate. Scroll down to see the org-Fortinet entry. Expand to see the certificate and view its details.

## Managed Chromebook

If your organization manages Chromebooks using the Google Admin console, you can centrally install the FortiSASE certificate authority certificate on the Admin console and distribute it to each managed Chromebook.

To upload the FortiSASE CA certificate on Google Admin Console:

1. On the [Google Admin console](#), go to *Device > Networks*.
2. Select the organizational unit in which to apply these settings.
3. Under *Certificates*, click *Create Certificate*.
4. Enter a name for this certificate entry, then click *Upload* to upload the Fortinet\_CA\_SSL.cer certificate.
5. Under *Certificate Authority*, select *Chromebook*. Click *ADD*.



To verify the CA certificate is installed on a Chromebook:

1. In Chrome, open *Settings* from the menu or go to `chrome://settings`.
2. Go to *Privacy and security*. On the configuration page, click *Security*.
3. In the *Security settings* page, scroll to the bottom to find *Advanced > Manage certificates*. Click the right arrow.
4. In the *Manage certificate* page, select *Authorities*.
5. Scroll down to the org-Fortinet entry. Expand this entry. You will see the certificate and an icon indicating that Google Admin console is managing it.

## Configuring proxy settings on endpoints

To connect to FortiSASE in Secure Web Gateway (SWG) agentless mode, each endpoint client must configure proxy settings within its network or browser settings to point to FortiSASE’s servers. You can configure this individually on the endpoint or, if you are using an enterprise management system, push it out to managed endpoints centrally.

You should provide users one of the following during the user onboarding process:

- URL to the hosted proxy autoconfiguration (PAC) file
- Proxy server addresses and port if users are to configure proxy settings manually.

From the *System > SWG Configuration* page, make note of the following information:

Field	Description
Global (Recommended)	Global FortiSASE server address for your instance.
Secure Web Gateway Server(s)	Lists address of each individual regional FortiSASE server for your instance.
Secure Web Gateway Port	Port that client should connect to in their proxy settings.
PAC File	Static copy of the PAC file, which you can customize and rehost on your server.
Hosted PAC File	Address of the PAC file hosted on the FortiSASE server.

Refer to [SWG Configuration](#) for more information.

Users are expected to have installed the FortiSASE certificate authority certificate on their devices. See [Installing the FortiSASE CA certificate on endpoints on page 17](#).

Proxy settings on endpoint clients can differ between operating systems (OS) and browsers. While the following examples demonstrate the configuration for the selected OSes, refer to your OS or browser for complete instructions on configuring proxy settings.

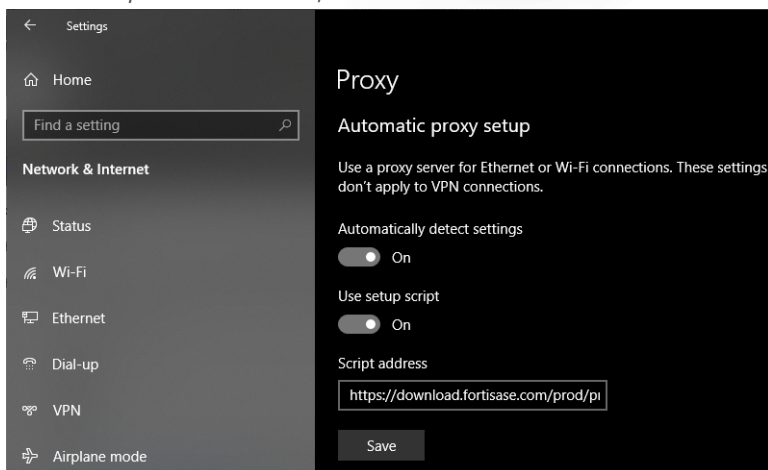
- [Windows on page 21](#)
- [macOS on page 21](#)
- [Chrome OS on page 22](#)
- [Managed Chromebook on page 24](#)

## Windows

The end user can configure proxy settings at the operating system (OS) level or in a browser. When you configure Secure Web Gateway (SWG) settings at the OS level, Windows applies them to all installed browsers. The following gives instructions for configuring SWG settings at the OS level on a Windows 10 device.

To configure Windows 10 to use the FortiSASE SWG server:

1. In Windows, go to *Windows Settings > System > Proxy Settings*.
2. Enable *Use setup script*.
3. In the *Script address* field, enter the *Hosted PAC File URL*.



4. The next time the user starts a browser session, the browser displays an authentication prompt. The end user enters their FortiSASE credentials in the prompt. After ten minutes of inactivity, the browser reprompts for authentication credentials.

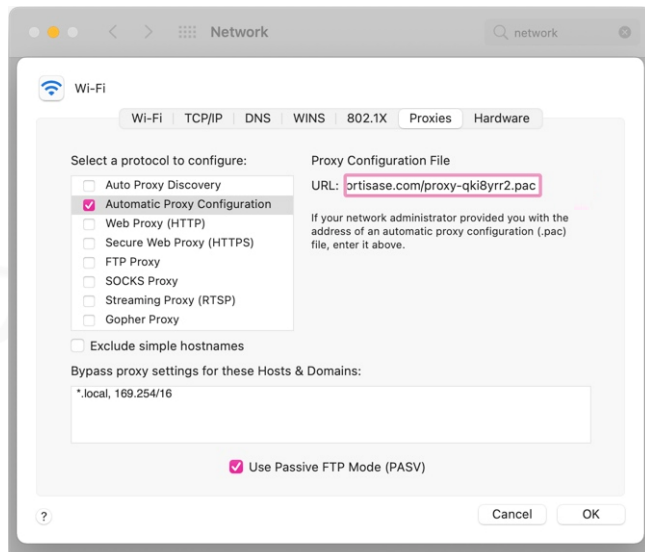
## macOS

This example demonstrates manually configuring proxy settings on macOS. See also [Change proxy settings in Network preferences on Mac](#).

To manually configure proxy settings on a macOS endpoint:

1. Go to the *Apple menu > System Preferences > Network*.
2. In the list, select the Network service. For example, you may select your connected wireless SSID.
3. Click *Advanced*.
4. On the *Proxies* tab, select the protocol to configure. Enable *Automatic Proxy Configuration*, then enter the URL to your hosted PAC file.

5. Click *OK*, then apply to apply the changes.



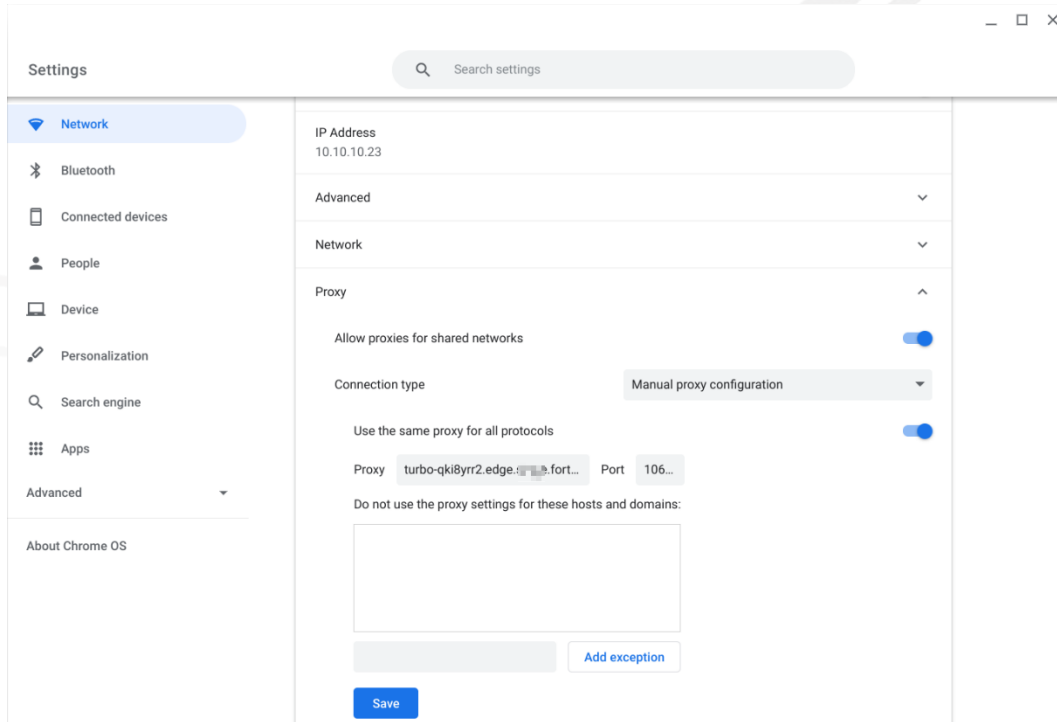
6. The next time that the user starts a browser session, the browser displays an authentication prompt. The end user enters their FortiSASE user credentials in the prompt to authenticate.

## Chrome OS

To configure proxy as a system-wide setting:

1. Open the Launcher, and search for *Settings*.
2. Click *Network* on the left menu. Then select your Wireless Network SSID and click the right arrow to expand.
3. Scroll to the bottom and expand the proxy settings.
4. For *Connection type*, select one of the following:
  - a. Select *Automatic proxy configuration*. This is the recommended method. Point the *Autoconfiguration URL* to the FortiSASE hosted PAC file.
  - b. To configure manual proxy configuration, do the following:
    - i. Select *Manual proxy configuration*.
    - ii. Enable *Use the same proxy for all protocols*.
    - iii. Enter the proxy server address, and the Secure Web Gateway port that your administrator provided. You can select the global proxy or the server closest to you.

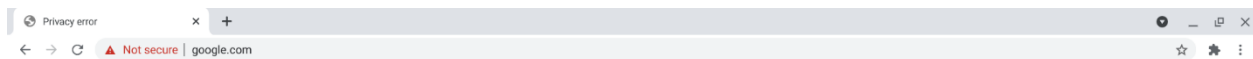
iv. Click Save.



If issues arise with some websites using SOCKS, you can work around this by disabling *Use the same proxy for all protocols*. Then only define the proxy server address for HTTP proxy and secure HTTP proxy.

5. On a successful connection, your browser prompts you to authenticate. Enter your user credentials to authenticate to FortiSASE and continue browsing the web.

If you receive a warning message from Chrome preventing you to go further, you must disable your proxy settings, and install the FortiSASE certificate authority certificate before reenabling proxy.



**An application is stopping Chrome from safely connecting to this site**

"Fortinet" wasn't installed properly on your computer or network. Ask your IT administrator to resolve this issue.

NET:ERR\_CERT\_AUTHORITY\_INVALID

To get Chrome's highest level of security, [turn on enhanced protection](#)

Hide advanced

A root certificate for "Fortinet" is required but isn't installed. Your IT administrator should look at configuration instructions for "Fortinet" to fix this problem. Applications that can cause this error include antivirus, firewall, and web-filtering or proxy software.

## Managed Chromebook

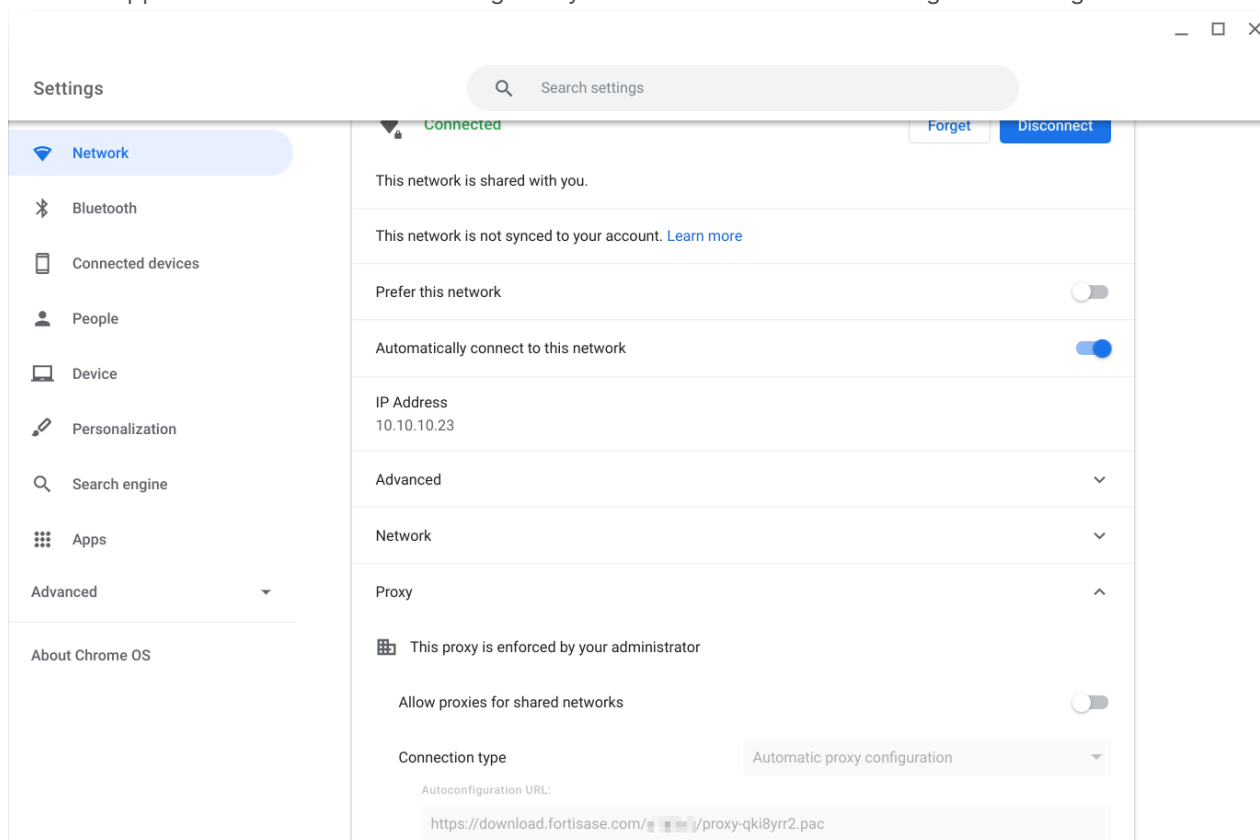
If your organization manages Chromebooks using the Google Admin console, you can centrally configure proxy settings on the Admin console and distribute them to each managed Chromebook.

To configure proxy as a system-wide setting on Google Admin Console:

1. On the [Google Admin console](#), go to *Device > Chrome > Settings > Users & Browsers..*
2. Select the organizational unit in which to apply these settings.
3. Under *User and Browser Settings*, filter for the keyword `Proxy`. The *Network* section appears.
4. For *Proxy mode*, use one of the following options:
  - a. Select *Always use the proxy auto-config specified below*. Enter FortiSASE's hosted PAC file address. Save.
  - b. Select *Always use the proxy specified below*. Enter the proxy server URL in the format `<proxy server address>:<SWG port>`. Save.

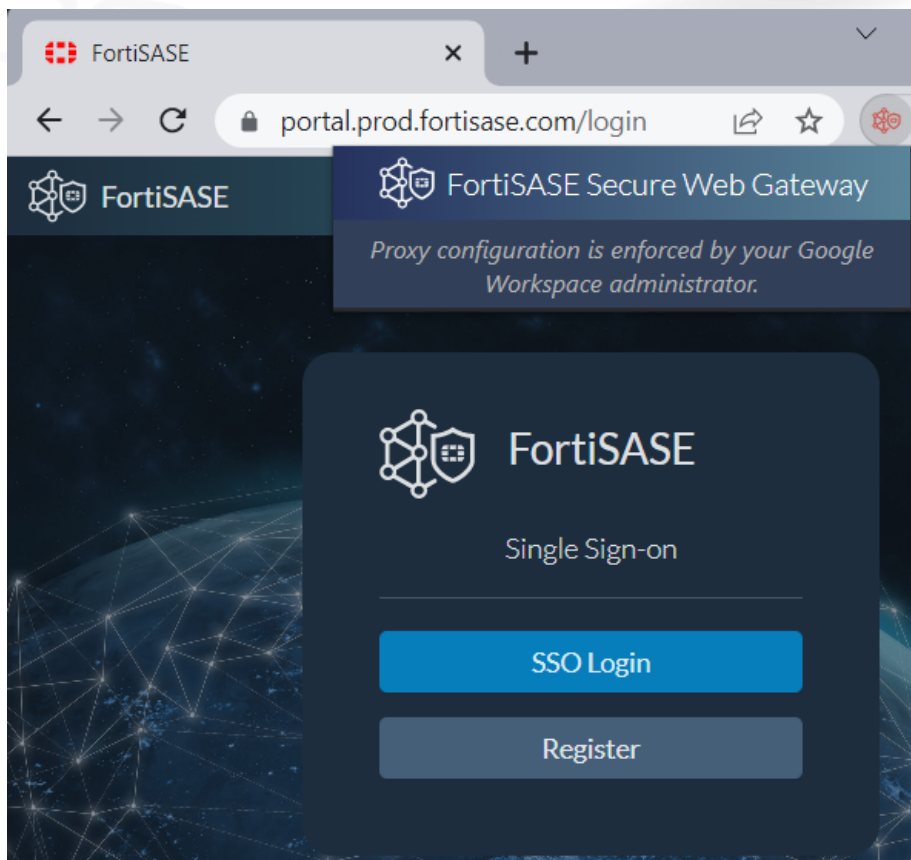
To verify proxy settings are configured on the managed Chromebook:

1. Open the Launcher and search for Settings.
2. Click *Network* on the left menu. Then select your Wireless Network SSID and click the right arrow to expand.
3. Scroll to the bottom and expand the proxy settings. The settings pushed from the Google Admin Console appear with an icon and warning that your administrator is enforcing this setting.



## (Optional) Installing and configuring the SWG Chrome extension

FortiSASE supports a Chrome extension that allows enforcing FortiSASE secure web gateway (SWG) connectivity for selected endpoints with the Chrome browser installed, including Chromebooks, based on the endpoint operating system (OS) and the corresponding extension policy that the Google Workspace administrator configured.



This extension relies on the following features being configured in FortiSASE:

- SWG single sign-on
- SWG configuration

The extension also requires that the user has already downloaded and installed the SWG certificates to the device certificate store as [Installing the FortiSASE CA certificate on endpoints on page 17](#) describes. Alternatively, you can use Google Workspace to install certificates on Chromebooks as [Managed Chromebook on page 24](#) describes.

Since this extension is not installed in Chrome incognito mode, the administrator should disable incognito mode in Google Workspace.

This extension allows you to configure the following settings on an endpoint through Google workspace:

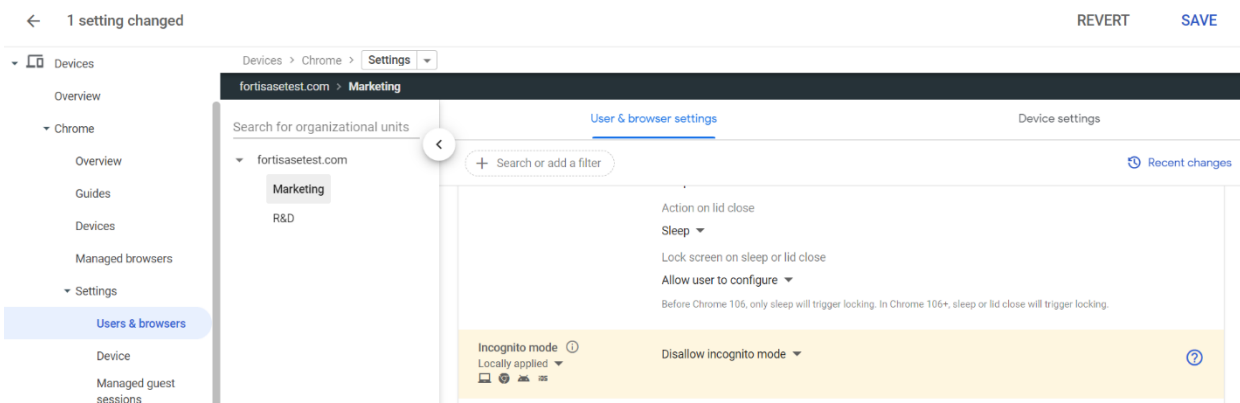
- Default or custom hosted PAC file URL
- User ability to view PAC file URL within the extension
- Configuration of supported platforms (ChromeOS, Linux, macOS, and Windows) where SWG is enforced

## (OPTIONAL) INSTALLING AND CONFIGURING THE SWG CHROME EXTENSION

To disable incognito mode in Google Workspace:

Since this extension is not installed in incognito mode, SWG policies are not enforced when using incognito mode. The Google Workspace administrator must disallow incognito mode to ensure that SWG is always enforced on the Chromebook and other devices with managed Chrome browsers.

1. Go to *Devices > Chrome > Settings > Users & browsers*.
2. Select the desired organizational unit (OU).
3. Scroll to *Security > Incognito mode*.
4. From the dropdown menu, select *Disallow incognito mode*.
5. Click *Save*.



To configure the extension policy for FortiSASE SWG Chrome extension:

You can apply the FortiSASE SWG extension to one or more user OUs within Google Workspace. All users assigned within an OU that the FortiSASE SWG extension is applied to have the extension installed and SWG enforced on their Chromebook and Chrome browser.

1. In the Google Admin console, go to *Devices > Chrome > Apps & extensions > Users & browsers*.
2. Select the desired OU to install and enforce the FortiSASE SWG extension.
3. Add the Chrome extension to the OU by clicking the + button on the bottom right, clicking *Chrome app or extension by ID*, and searching using the ID `aecejhdejcfnfihadbfdmndehobfdpcc`.
4. Select the *FortiSASE Secure Web Gateway extension* to push to Chromebooks and devices with managed Chrome browsers.

5. Configure the policy using the following parameters:

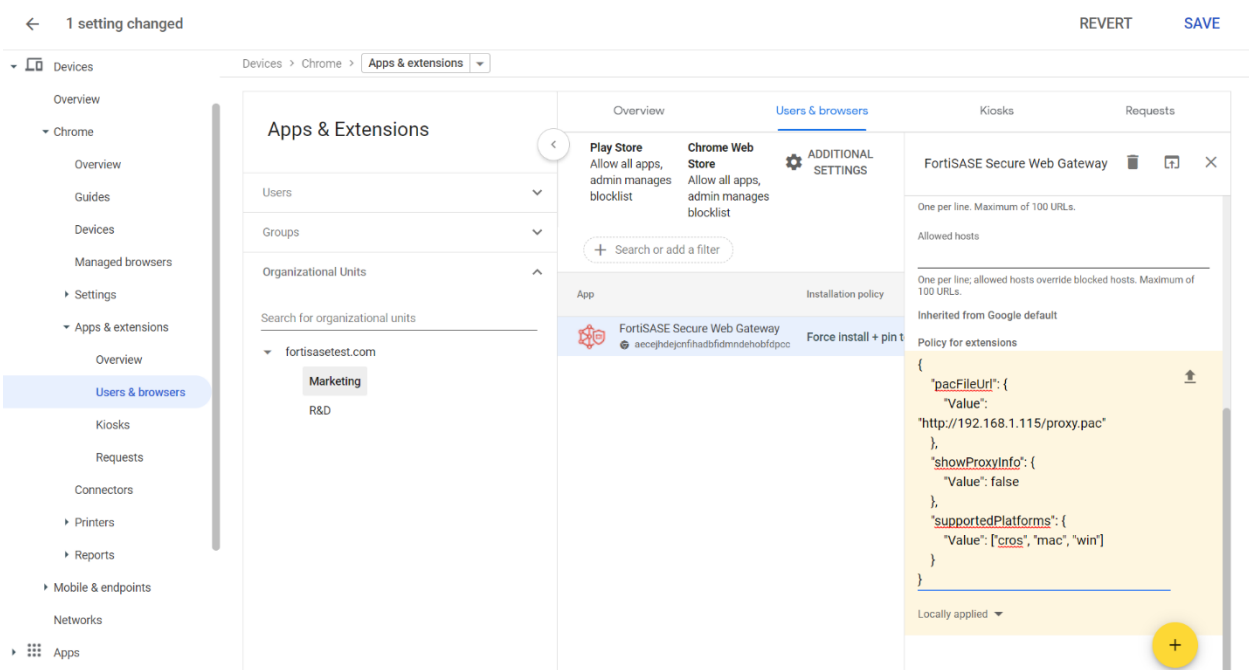
Parameter	Description
pacFileUrl	PAC file that the extension will enforce. Configure one of the following: <ul style="list-style-type: none"><li>• Default hosted PAC file link from FortiSASE in <i>System &gt; SWG Configuration</i>. See <a href="#">SWG Configuration</a>.</li><li>• Custom hosted PAC file link from a server accessible to endpoints. See <a href="#">Customizing the PAC file on page 13</a>.</li></ul>
showProxyInfo	Possible values: <code>false</code> or <code>true</code> . <ul style="list-style-type: none"><li>• Setting this to <code>false</code> hides the PAC file URL from the extension.</li><li>• Setting this value to <code>true</code> makes the PAC file URL visible to the extension.</li></ul>
supportedPlatforms	Possible values include <code>cros</code> , <code>linux</code> , <code>mac</code> , and <code>win</code> to specify ChromeOS (Chromebook), Linux, macOS, and Windows, respectively. To exempt a device from SWG enforcement, you can set one of these options: <ul style="list-style-type: none"><li>• Remove the device OS from the <code>supportedPlatforms</code> array</li><li>• Set <code>pacFileUrl</code> to an empty string</li><li>• Remove the <code>pacFileUrl</code> key-value pair from the policy configuration</li></ul>

6. Click *Save*.

Following is an example extension policy configuration using a custom PAC file hosted on a LAN server with the PAC file URL hidden from extension and the extension applied to ChromeOS, macOS, and Windows devices:

```
{
  "pacFileUrl": {
    "Value": "https://192.168.1.115/proxy.pac"
  },
  "showProxyInfo": {
    "Value": false
  },
  "supportedPlatforms": {
    "Value": ["cros", "mac", "win"]
  }
}
```

The following shows the FortiSASE SWG extension and example extension policy applied to users within the Marketing OU:



To verify the policy has been enforced on the device with the extension installed:

On the Chromebook or device with Chrome browser installed, go to `chrome://policy` from the Chrome browser to verify the aforementioned example policy has been enforced on the Chromebook or device with managed Chrome browser:

FortiSASE Secure Web Gateway

Policy name	Policy value	Source	Applies to	Level	Status
pacFileUrl	https://192.168.1.115/proxy.pac	Cloud	Machine	Mandatory	OK, Superseding <a href="#">Show more</a>
showProxyInfo	false	Cloud	Machine	Mandatory	OK, Superseding <a href="#">Show more</a>
supportedPlatforms	["cros", "mac", "win"]	Cloud	Machine	Mandatory	OK, Superseding <a href="#">Show more</a>

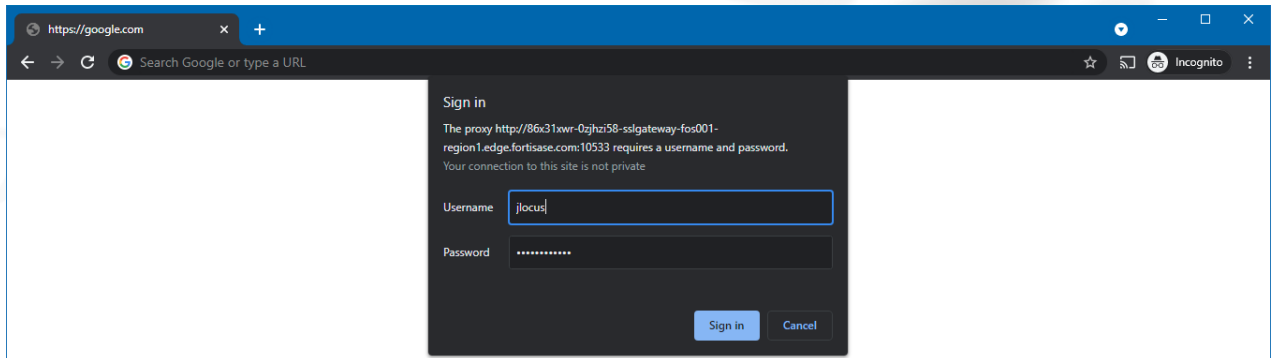
## Testing SWG user connections to the Internet

The basic configuration is complete at this point. Test the connections to the Internet and corporate networks on an endpoint.

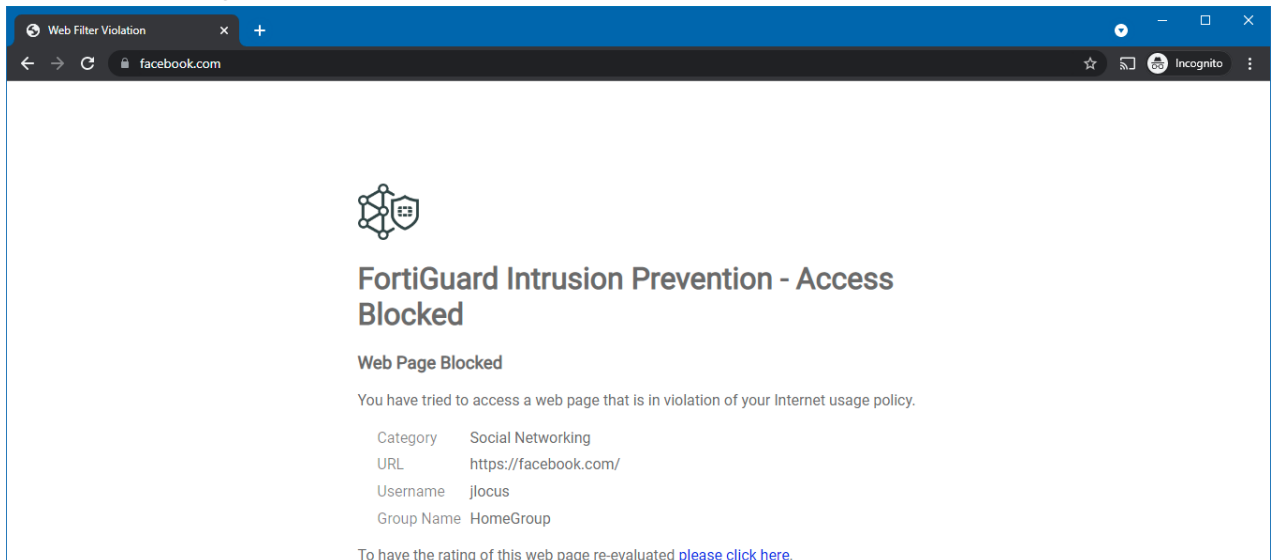
## TESTING SWG USER CONNECTIONS TO THE INTERNET

To test connection to the Internet on a Windows computer with a RADIUS user:

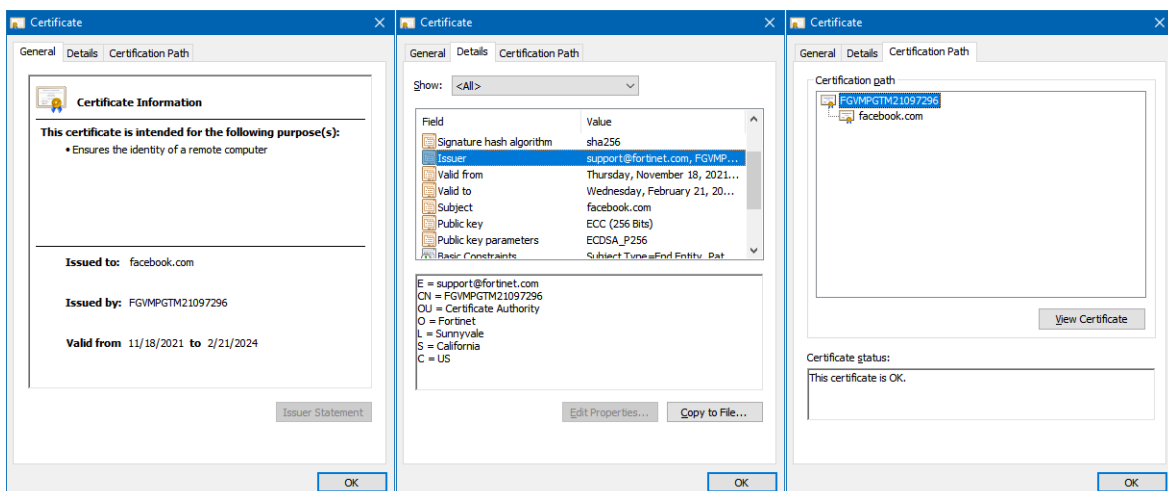
1. From the endpoint, open a browser.
2. Browse to a webpage.
3. An authentication prompt appears. Enter your username and password.



4. Once authenticated, you can browse to any webpage. FortiSASE scans this traffic.
5. Browse to a webpage that triggers a Web Filter violation. The browser shows a message that FortiSASE blocks the webpage.



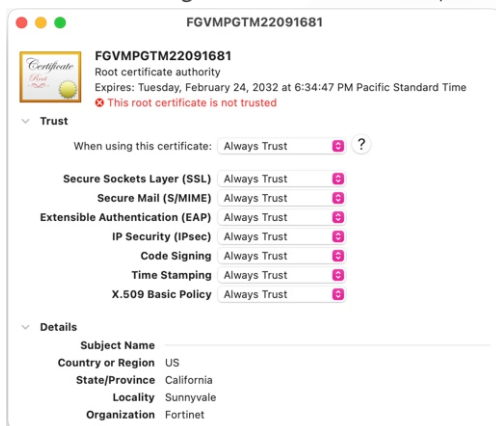
For the blocked webpage message to display without a certificate warning, you must install the FortiSASE root certificate authority certificate on the endpoint. The following shows a valid certificate chain:



6. In FortiSASE, go to *User Connection Monitor* to see the logged in user.

To test connection to the Internet on a macOS computer with an Azure Active Directory (AD) user:

1. From the endpoint, open a browser.
2. Browse to a webpage. The page redirects to a Microsoft login page to perform single sign on.
3. Log in using your Azure AD credentials.
4. Once authenticated, you can browse to any webpage. FortiSASE scans this traffic.
5. To properly browse any HTTPS websites, you must install the FortiSASE root certificate on the endpoint. Double-click the FortiSASE certificate that the administrator provided during onboarding. In the *Keychain* field, select *System*, then click *Add*.
6. When you view the certificate, the root certificate appears as not trusted. Expand the *Trust* section. In the *When using this certificate* field, select *Always Trust*.



7. Save the configuration and add the certificate to the system keychain.
8. You can connect to HTTPS websites without seeing a warning. Browse to an HTTPS website, then go to *User Connection Monitor* in FortiSASE to see the logged in user.

---

# More information

## Appendix A: Documentation references

### Feature documentation

Product document	Specific chapter if available
FortiSASE Admin Guide	<ul style="list-style-type: none"><li>• SWG Policies</li><li>• Configuring FortiSASE with a RADIUS server for remote user authentication</li><li>• Configuring FortiSASE with Azure AD SSO: SAML configuration fields</li><li>• Configuring FortiSASE with Azure Active Directory single sign on in SWG agentless mode</li><li>• SWG client onboarding</li></ul>

### 4-D resources: SASE

- <https://docs.fortinet.com/4d-resources/SASE>



[www.fortinet.com](http://www.fortinet.com)

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.