



SIA Agent-based Deployment Guide

FortiSASE



DEFINE / DESIGN / **DEPLOY** / DEMO



Table of Contents

Change log	4
Deployment overview	5
Intended audience	6
About this guide	6
Design concept and considerations	7
Authentication Sources and Access	7
Deploying FortiClient on endpoints	8
Product prerequisites	8
Deployment plan	8
Deployment procedures	9
Provisioning your FortiSASE instance	9
Configuring remote authentication and onboarding users	9
Configuring FortiSASE with Entra ID SSO	9
Defining a user group of Entra ID SAML SSO users	10
Finding the group ID for SAML group matching	11
Configuring security settings and VPN policies in FortiSASE	11
Configuring security settings	11
Configuring SSL deep inspection	12
Configuring Application Control	12
Adding VPN policies to perform granular firewall actions and inspection	14
Configuring a security profile group and applying it to a policy	16
Configuring DNS Settings	17
Split DNS Rules	18
Downloading and installing FortiClient on Windows endpoints	22
Connecting FortiClient to FortiSASE and provisioning the FortiSASE VPN tunnel	23
Connecting a user's endpoint to the FortiSASE tunnel using FortiClient and verifying Entra ID SAML SSO configuration	23
Testing SIA using a managed FortiClient endpoint	23
Testing from a managed FortiClient endpoint for granular VPN policies configured on default profile	23
Testing from a managed FortiClient endpoint for Application Control enabled	24

Verifying endpoint connectivity on FortiSASE	24
More information	25
Appendix A: Products used in this guide	25
Appendix B: Documentation references	25
Feature documentation	25
4-D resources: SASE	25

Change log

Date	Change description
2024-02-12	Initial release.
2024-03-07	Updated: <ul style="list-style-type: none">• Configuring DNS Settings on page 17• Split DNS Rules on page 18

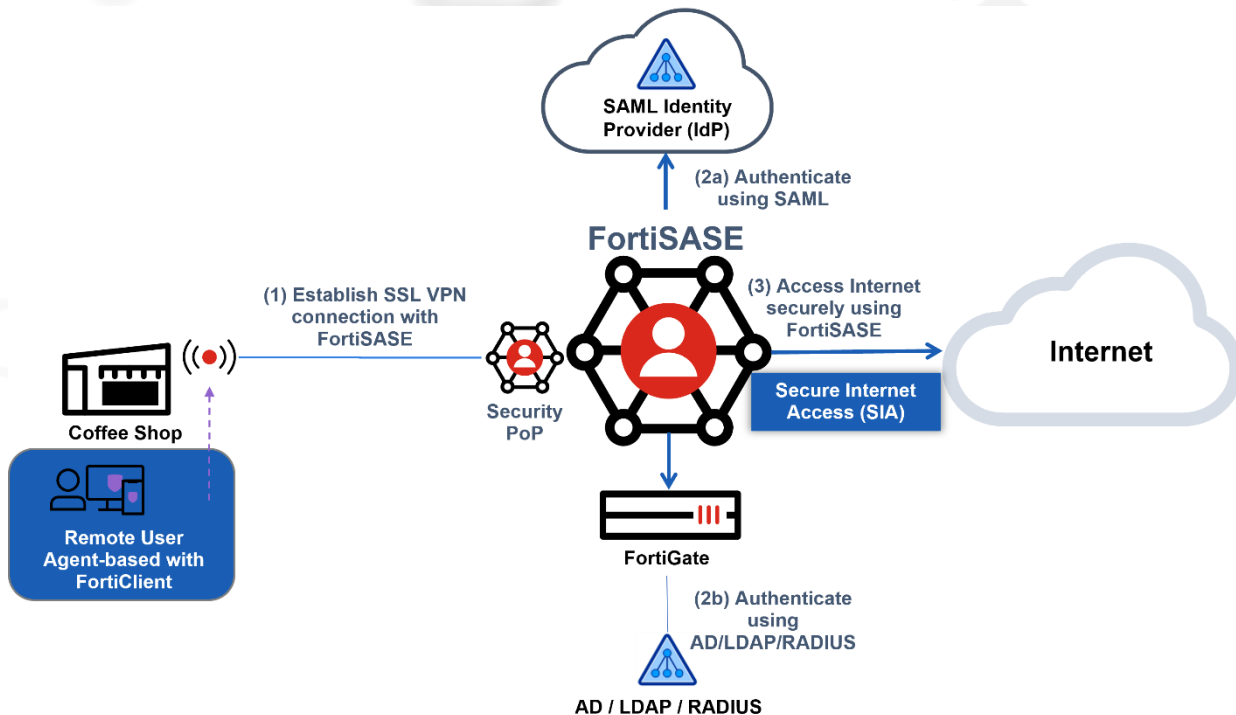
Deployment overview

FortiSASE secure Internet access (SIA) extends an organization's security by enforcing common security policy for Intrusion Prevention Systems and application control, web and DNS filtering, antimalware, sandboxing, antibotnet/Command and Control to remote users.

SIA for agent-based remote users is the most typical use case, which involves installing and configuring FortiClient on supported endpoints including Windows, macOS, and Linux endpoints. The [FortiSASE Administration Guide](#) calls this use case endpoint mode. In this use case, the FortiSASE firewall as a service (FWaaS) comes between the endpoint and the Internet. Because FortiClient essentially sets up a full-tunnel SSL VPN with the FWaaS, agent-based SIA secures all Internet traffic and protocols using VPN policies. Each endpoint connects to a security PoP. You can achieve agent-based remote user authentication by configuring the authentication source as Active Directory (AD)/LDAP, RADIUS or as a SAML identity provider (SAML IdP).

You can automate initial endpoint configuration using a mobile device management (MDM) tool. End user deployment involves entering an invitation code in FortiClient and using a username and password to log in to the SIA SSL VPN tunnel to FortiSASE.

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



This deployment guide describes how to configure FortiSASE for agent-based SIA using FortiClient for remote workers with Windows endpoints and using single-sign on (SSO) using Microsoft Entra ID (formerly known as Azure AD) via SAML as the authentication method.

Intended audience

Midlevel network and security architects, engineers, and administrators in companies of all sizes and verticals looking to deploy FortiSASE SIA for agent-based remote users should find this guide helpful. A working knowledge of FortiOS, FortiGate, and FortiClient configuration is helpful.

For comments and feedback about this document, visit the [FortiSASE Basic Endpoint Deployment](https://community.fortinet.com) on community.fortinet.com.

About this guide

This deployment guide describes the steps involved in deploying a specific architecture for the FortiSASE SIA use case using agent-based FortiClient for remote users with Windows endpoints and Entra ID via SAML for remote user authentication.

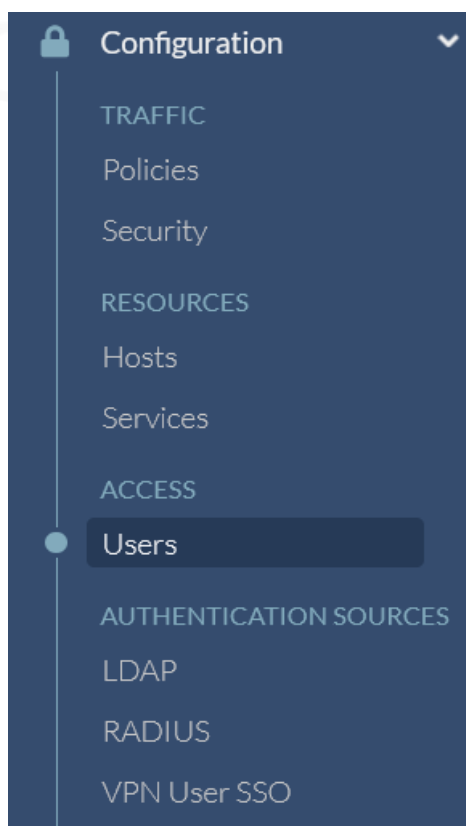
Readers should first evaluate their environment to determine whether the architecture outlined in this guide suits them. Reviewing the reference architecture guide(s), such as the [FortiSASE Architecture Guide](#), is advisable if readers are still in the process of selecting the right architecture. 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. Reviewing supplementary material found on the [Fortinet Document Library](#) in product administration guides, example guides, cookbooks, release notes, and other documents is recommended, where appropriate.

Design concept and considerations

Authentication Sources and Access

In *Configuration > Authentication Sources* and *> Access headings*, you can control network access for different users and devices in your network.



FortiSASE authentication controls system access by user group. By assigning individual users to the appropriate user groups, you can control each user's access to network resources. You can define local users and remote users in FortiSASE. You can also integrate user accounts on remote authentication servers and connect them to FortiSASE.

You can configure FortiSASE authentication as follows:

- Use *Configuration > Users* to define remote users, create/edit new user groups, and define local users
- Use *Configuration > LDAP*, *Configuration > RADIUS*, and *Configuration > VPN User SSO* to define LDAP, RADIUS, and SSO via SAML IdP authentication sources, respectively

The authentication method that you decide to configure with your FortiSASE SIA agent-based deployment depends on a variety of factors including having an existing authentication source from an existing deployment to migrate from, designing a new architecture with a new authentication source, and selecting an authentication source and method keeping in mind any onboarding or usability advantages for your remote users.

This deployment guide outlines how to configure single sign-on (SSO) using Microsoft Entra ID via SAML. For configuring other authentication sources, see [Authentication Sources and Access](#).

Deploying FortiClient on endpoints

The *Onboard Users* button, which is available from the *Remote User Management* widget on the *Status* dashboard, allows you to send an email to users to invite them to FortiSASE.

Remote users can download and install FortiClient on their own and register their FortiClient to FortiSASE Endpoint Management Service by using the instructions in the invitation email. You must still provision users via one of the aforementioned authentication sources and methods to give them access to VPN and other FortiSASE resources. The deployment guide describes how to deploy FortiClient on endpoints using this approach.

Alternatively, you can onboard users by automating the configuration of initial FortiClient settings by either using a mobile device management (MDM) tool or using FortiSASE Endpoint Management Service.

Product prerequisites

For a list of product prerequisites, see [SIA for agent-based remote users](#).

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.
2. Configure remote authentication and onboard users.
3. Configure policies to apply desired scanning and filtering for your users.
4. Configure the DNS settings to allow resolving hostnames for external and internal domains.
5. Download and install FortiClient on the Windows endpoints.
6. Using the invitation code, connect FortiClient to FortiSASE to activate the SASE license and provision the FortiSASE VPN tunnel.
7. In FortiClient, connect to the FortiSASE tunnel using the username and password assigned to each user.
8. Test access to the Internet using a remote device.

Deployment procedures

Provisioning your FortiSASE instance

Ensure that you have purchased the contract to provision FortiSASE, then do the following:

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 endpoints that the widget lists is the number of VPN users that are entitled to use this service.

Configuring remote authentication and onboarding users

Depending on the authentication source, the user configuration steps differ. The example shows configuring FortiSASE endpoint mode with a single sign on (SSO) connection with Microsoft Entra ID via SAML, where Entra ID is the identity provider (IdP) and FortiSASE is the service provider (SP). This feature allows end users to connect to VPN by logging in with their Entra ID credentials.



Other methods of user authentication do not work once you enable SAML SSO.

For configuring other authentication sources, see [Authentication Sources and Access](#).

Configuring FortiSASE with Entra ID SSO

Before completing the following steps, see [Configuring with Entra ID SSO: SAML configuration fields](#) for details on how Microsoft Entra ID SAML fields map to FortiSASE SAML fields.

To configure FortiSASE with Entra ID SSO:

1. In FortiSASE, go to *Configuration > VPN User SSO*. The first step of the SSO configuration wizard displays the entity ID, SSO URL, and single logout URL. You use these values to configure FortiSASE as an SP in Azure. Copy these values.
2. Create and configure your FortiSASE environment in Azure:
 - a. In the Azure portal, go to *Entra ID > Enterprise applications > New application*.
 - b. Search for and select FortiSASE.
 - c. Click *Create*.
 - d. Assign Entra ID users and groups to FortiSASE.
 - e. Go to *Set up single sign on*.
 - f. For the SSO method, select *SAML*.
 - g. In *Basic Configuration*, enter the values that you copied in step 1 in the *Identifier (Entity ID)*, *Reply URL*, *Sign on URL*, and *Logout URL* fields. Click *Save*.
3. Obtain the IdP information from Azure:
 - a. The *SAML Signing Certificate* box contains links to download the SAML certificate. Download the certificate.
 - b. The *Set up <FortiSASE instance name>* box lists the IdP information that you must provide to FortiSASE. Copy the values in the *Login URL*, *Entra ID Identifier*, and *Logout URL* fields.
4. Configure the IdP information in FortiSASE:
 - a. In FortiSASE, click *Next* in the SSO wizard. In the *IdP Entity ID*, *IdP Single Sign-On URL*, *IdP Single Log-Out URL* fields, paste the values that you copied from the *Entra ID Identifier*, *Login URL*, and *Logout URL* fields, respectively.
 - b. From the *IdP Certificate* dropdown list, select *Create*, then upload the certificate that you downloaded. Click *Next*.
5. Review the SAML configuration, then click *Submit*.
6. Invite Entra ID users to FortiSASE:
 - a. (Optional) Create a user group using the steps in [Defining a user group of Entra ID SAML SSO users on page 10](#).
 - b. In *Configuration > VPN User SSO*, click *Onboard Users*.
 - c. Under *Invite Users*, enter the email addresses of the users that you want to add to FortiSASE.
 - d. Click *Send*. FortiSASE sends invitation emails to these users so that they can download FortiClient and connect to FortiSASE.

Defining a user group of Entra ID SAML SSO users

To define a group of Microsoft Entra ID SAML single sign on (SSO) users, create a user group in FortiSASE.

To define a user group of Entra ID SAML SSO users:

1. Go to *Configuration > Users*.
2. Click *Create > User Group*.
3. In the *Users* field, click *+*.
4. In the *Select Entries* pane, select the desired users to add to this user group.
5. In the *Remote Groups* field, select *Create*.
6. From the *Remote Server* dropdown list, select the desired server.
7. In the *Groups* field, add the desired Entra ID group IDs. Click *OK*. For details on finding the group IDs in Entra ID for group matching, see [Finding the group ID for SAML group matching on page 11](#).
8. Click *OK*.

Finding the group ID for SAML group matching

Enable and configure SAML group matching if you only want to allow Microsoft Entra ID users of a certain group to authenticate. Otherwise, leave this setting disabled. You can define more granular groups when you configure user group settings.

To find the Entra ID Group ObjectID in Entra ID:

1. In the left pane of the Azure portal (three horizontal lines), select *Entra ID*. Under *Manage*, select *Groups*.
2. The default view shows all groups. Find the desired group and note the Object Id.

For details on creating a new security group, see *Create a security group for the test user* in [Tutorial: Microsoft Entra SSO Integration with FortiGate SSL VPN](#).

You can find the full list of group claims in [Configure group claims for applications by using Microsoft Entra ID](#).

Configuring security settings and VPN policies in FortiSASE

This deployment guide demonstrates enabling SSL deep inspection and configuring application control as examples of how to configure FortiSASE security components that are applied to each Allow policy.

Configuring security settings

You can configure FortiSASE security components settings and view logs for each component in *Security*. FortiSASE applies enabled security components to each Allow policy in *Policies*. You can configure some exemptions and overrides for some security components.

FortiSASE has the following security features:

- Antivirus
- Web Filter
- DNS Filter
- Intrusion prevention
- File filter
- Data leak prevention
- Application control
- SSL Inspection

For details on configuring these FortiSASE security components, see [Security](#).

For any FortiSASE security component:

- You can enable it by clicking on the toggle on the top-right corner of the security component's widget.
- You can click *Customize* for any enabled security component to configure further settings.
- You can click *View All* to view all detected threats and the count for each threat.
- You can click *View Logs* to view logs corresponding to detected threats.

Configuring SSL deep inspection

By default, FortiSASE uses SSL certificate inspection which inspects only the header information up to the SSL/TLS layer. Certificate inspection verifies the identity of web servers by analyzing the SSL/TLS negotiations by looking at the server certificate and TLS connection parameters only. However, while certificate inspection is more straightforward and does not require installation of a CA certificate on the endpoints, it does not inspect the content or payload encrypted by SSL/TLS.

While HTTPS offers protection on the Internet by applying SSL encryption to web traffic, malicious traffic can also use SSL encryption to get around your network's normal defenses. For example, you may download a file containing a virus during an e-commerce session or receive a phishing email containing a seemingly harmless download that, when launched, creates an encrypted session to a command and control (C&C) server and downloads malware onto your computer.

Therefore, SSL deep inspection can be used to protect the infiltration described above by scanning for malicious content in your HTTPS web traffic or identifying phishing content in encrypted mail exchanges. SSL deep inspection can also defend against the exfiltration process while an infected host calls home to a C&C server or leaks company secrets over encrypted sessions.

By enabling SSL deep inspection, FortiSASE decrypts and inspects the content to find threats and block them. It then re-encrypts the content and sends it to the real recipient. You can configure exemptions for deep inspection.

When you use deep inspection, FortiSASE serves as the intermediary to connect to the SSL server on behalf of the client. It decrypts and inspects the content to find threats and block them. The recipient is presented with a certificate issued by FortiSASE using its default or custom CA certificate, instead of the real server certificate. Since FortiClient receives the CA certificate automatically from FortiSASE and installs this to the trusted certificate store, endpoint users do not see any certificate browser warnings.

To configure SSL deep inspection:

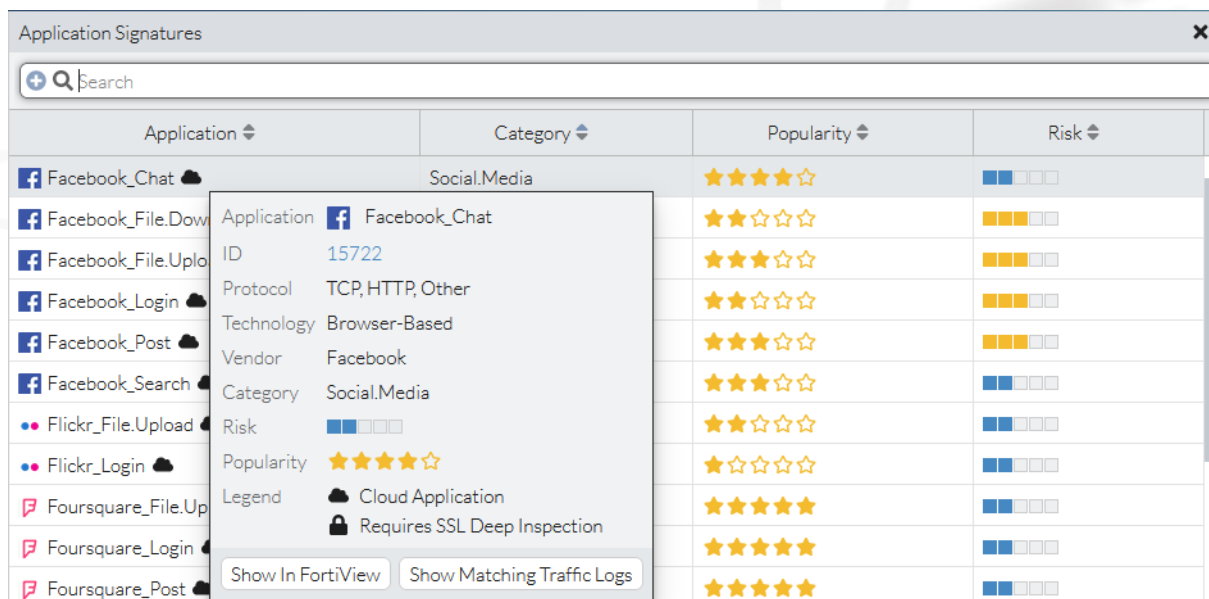
1. Go to *Configuration > Security*.
2. Note that *SSL Inspection* is always enabled and cannot be disabled. By default, FortiSASE uses certificate inspection. In the *SSL Inspection* widget, click *Customize*.
3. The *SSL Inspection* pane displays the SSL inspection modes that can be configured.
 - a. Select *Deep Inspection*.
 - b. Under *Inspection Options* select the CA Certificate (the default). You can upload your own organization's CA certificate by selecting the dropdown list next to *CA Certificate* and clicking *Create*. Follow the steps in the *Create* pane to upload your own CA certificate.
4. Click *OK*. After configuring the above SSL deep inspection settings, the FortiSASE Endpoint Management Service automatically deploys the CA certificate to FortiClient endpoints that FortiSASE manages.

Configuring Application Control

Applying Application control allows you to allow and block applications by category. FortiSASE can recognize network traffic generated by a large number of applications. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic, even if the traffic uses non-standard ports or protocols. Application control supports traffic detection using the HTTP protocol (versions 1.0, 1.1, and 2.0).

Cloud applications can only be detected by FortiSASE when SSL deep inspection is enabled. Cloud application signatures are indicated by the cloud icon next to the category.

When viewing cloud signatures within a category in more detail and selecting a specific cloud signature, the SSL deep inspection requirement is indicated by the lock icon within the tooltip window that appears. The screenshot shows that the Facebook Chat cloud application within the Social Media category requires SSL deep inspection to be detected by FortiSASE Application Control.



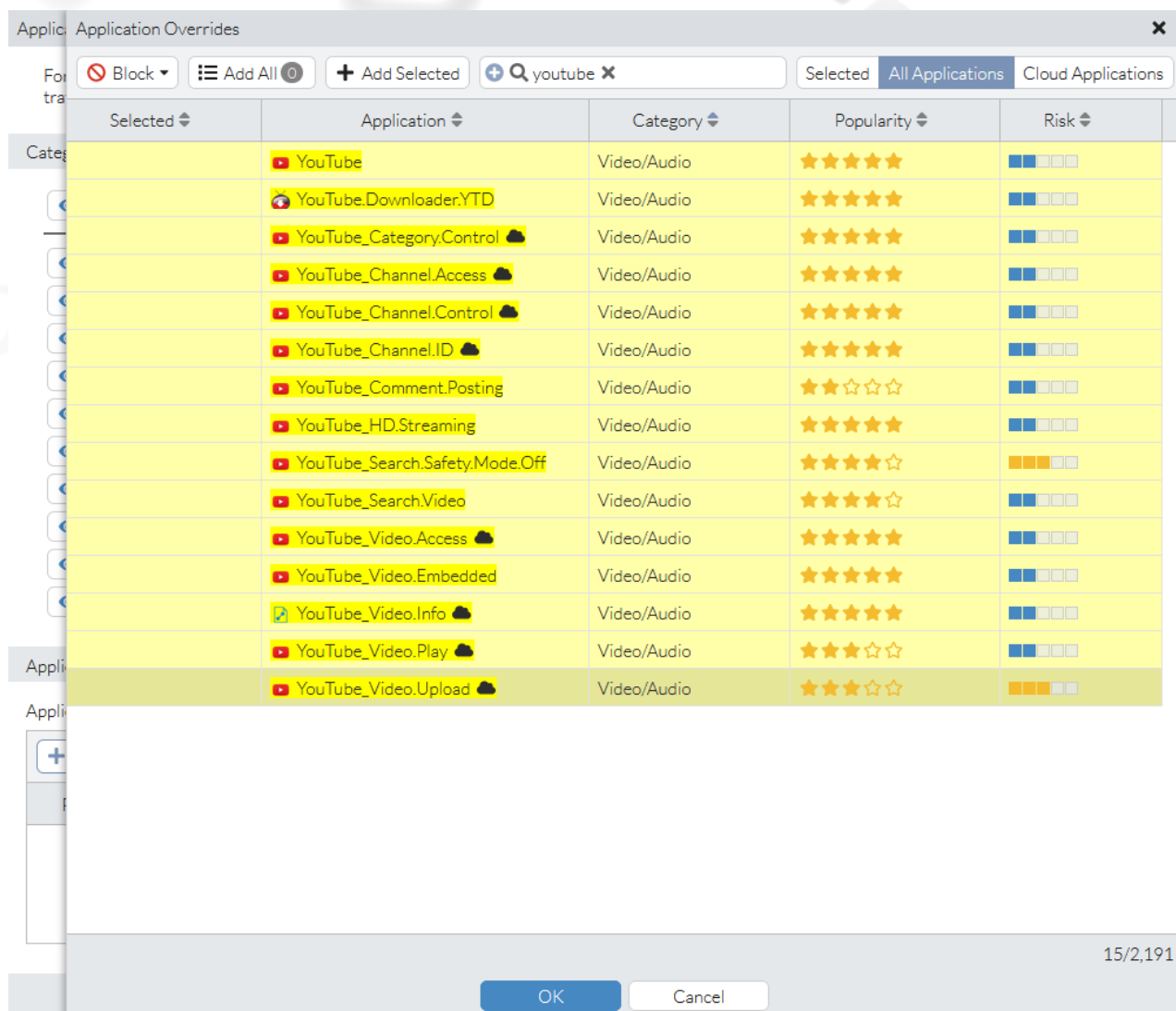
In this example configuration, the Video/Audio category is allowed, but YouTube related applications are overridden and blocked.

To configure application control:

1. Go to *Configuration > Security*.
2. Enable *Application Control*.
3. In the *Application Control* widget, click *Customize*.
4. The *Application Control* pane displays the application categories. You can configure one of the following actions for each category:

Type	Description
Allow	Passes the traffic to the web filters, antivirus inspection engine, and DLP inspection engine.
Monitor	Processes the traffic the same way as the Allow action. For the Monitor action, FortiSASE generates a log message each time it establishes a matching traffic pattern.
Block	Denies or blocks attempts to access any application that belongs to the category. A replacement message displays.

5. In *Application Overrides*, you can configure actions for individual applications, overriding the action configured for their category. Click *Create*. Select the desired action from the dropdown list in the upper left corner, select the desired applications, then click *OK*. You can search for the desired applications, and filter the list to show only cloud applications. The *Application Overrides* pane denotes cloud applications with a cloud icon, such as for the YouTube_Category.Control application in the following screenshot. The following example allows the Video/Audio category, and blocks YouTube.



6. Click OK.

Adding VPN policies to perform granular firewall actions and inspection

You can add multiple policies to perform granular firewall actions and inspection. This example configures a VPN policy to allow a set of remote users to access *.fortinet.com and blocks the same remote users from accessing all traffic to *.netflix.com.

VPN policy name	Description
RemoteHomeOffice-DenyNetflix	Blocks remote employees (members of the Remote-Home-Office VPN user group) from accessing *.netflix.com.
RemoteHomeOffice-AllowFortinet	Allows remote employees (members of the Remote-Home-Office VPN user group) to access *.fortinet.com.

The following provides instructions for configuring the described policies. You may want to configure similar policies, modifying settings based on your environment.

This example assumes that you have created the Remote-Home-Office VPN user group and you have already added one or more of your users to this group already using the steps in [Defining a user group of Entra ID SAML SSO users on page 10](#).



For proper group matching, ensure that you follow the steps in [Defining a user group of Entra ID SAML SSO users on page 10](#) and specify group IDs in the *Remote Groups* section of the *Create New User Group* and *Edit User Group* dialogs. You should not specify Group IDs using the *SAML Group Matching* option in *Configuration > VPN User SSO > Configure Service Provider*.

To add policies to perform granular firewall actions and inspection:

1. Go to *Configuration > VPN Policies*.
2. Create the RemoteHomeOffice-DenyNetflix VPN policy:
 - a. Click *Create*.
 - b. For *Source Scope*, select *VPN Users*.
 - c. For *User*, select *Specify*: Click +, and select the *Remote-Home-Office* user group from the *Select Entries* pane.
 - d. In the *Destination* field, select *Specify*, click +, then do the following:
 - i. On the *Host* tab, click *Create*.
 - ii. Select *IPv4 Host*.
 - iii. In the *Name* field, enter the desired name.
 - iv. From the *Type* dropdown list, select *FQDN*.
 - v. In the *FQDN* field, enter *.netflix.com. When using wildcard FQDNs, FortiSASE caches the FQDN address's IP addresses based on matching DNS responses.
 - vi. Click *OK*.
 - vii. Select the newly created Netflix host.
 - e. In the *Service* field, click +. On the *Select Entries* pane, select *ALL*.
 - f. Leave all other fields at their default values.
 - g. Click *OK*.
3. Create the RemoteHomeOffice-AllowFortinet VPN policy:
 - a. Click *Create*.
 - b. For *User*, select *Specify*. Click +, and select the *Remote-Home-Office* user group from the *Select Entries* pane.
 - c. In the *Destination* field, click +, then do the following:
 - i. On the *Host* tab, click *Create*.
 - ii. Select *IPv4 Host*.
 - iii. In the *Name* field, enter the desired name.
 - iv. From the *Type* dropdown list, select *FQDN*.
 - v. In the *FQDN* field, enter *.fortinet.com. When using wildcard FQDNs, FortiSASE caches the FQDN address's IP addresses based on matching DNS responses.
 - vi. Click *OK*.
 - vii. Select the newly created Fortinet host.
 - d. In the *Service* field, click +. On the *Select Entries* pane, select *ALL*.
 - e. For *Action*, select *Accept*.
 - f. Leave all other fields at their default values.
 - g. Click *OK*.

4. In *Configuration > VPN Policies*, ensure that you order the policies so that RemoteHomeOffice-DenyNetflix VPN policy is before the RemoteHomeOffice-AllowFortinet VPN policy, and that those VPN policies are before the Allow-All VPN policy.

When a session is initiated through the VPN tunnel, FortiSASE analyzes the connection and performs a VPN policy match. FortiSASE performs the match from top down and compares the session with the configured VPN policy parameters.

Configuring a security profile group and applying it to a policy

You can create security profile groups, which allow you to group different security profile settings together. You can then configure the profile group as part of a policy.

For example, consider the RemoteHomeOffice-AllowFortinet example policy above, which allows remote employees (members of the Remote-Home-Office VPN user group) to access *.fortinet.com. Consider that you also want to monitor these employees' access to Cloud/IT applications using Application Control, while disabling Application Control for all other employees. You can achieve this by creating a new security profile group with the desired Application Control settings, and configuring this profile group as part of the RemoteHomeOffice-AllowFortinet policy. Application Control remains disabled for policies that have another security profile group applied.

The following provides steps for configuring the described scenario.



This scenario assumes that Application Control is disabled for policies that have another security profile group applied. Therefore, before proceeding with the following steps, you must disable Application Control on the default profile group if you followed the steps in [Configuring Application Control on page 12](#).

This example assumes that the Remote-Home-Office VPN user group has been created and one or more of your users have been added to this group already using the steps provided in [Defining a user group of Entra ID SAML SSO users on page 10](#).



For proper group matching, ensure that you follow the steps in [Defining a user group of Entra ID SAML SSO users on page 10](#) and specify group IDs in the *Remote Groups* section of the *Create New User Group* and *Edit User Group* dialogs. You should not specify group IDs using the *SAML Group Matching* option in *Configuration > VPN User SSO > Configure Service Provider*.

To create a security profile group and configure it in a policy:

1. Go to *Configuration > Security*.
2. From the *Profile Group* dropdown list in the top right corner, click *Create*.
3. In the *Name* field, enter the desired name. This example uses "Cloud IT" as the group name.
4. In the *Initial Configuration* field, do one of the following:
 - a. Select *Basic* to configure the new group with basic security settings (File Filter, Data Leak Prevention, and Application Control disabled while other features are enabled)
 - b. Select *Based On* to configure the new group with the same settings as an existing security profile group. From the dropdown list, select the desired group.
5. Click *OK*.
6. Configure Application Control to monitor employees' access of Cloud/IT applications by enabling Application Control. By default, once enabled, Application Control monitors access of Cloud/IT applications.

7. Configure the profile group in a policy:
 - a. Go to *Configuration > Traffic > Policies*.
 - b. Select the RemoteHomeOffice-AllowFortinet policy.
 - c. In the *Profile Group* field, select *Specify*. From the dropdown list, select *Cloud IT*. The *Profile Group* field is only available for policies where the *Action* is configured as *Accept*.
 - d. Click *OK*.

Configuring DNS Settings

Agent-based remote users use *VPN Implicit DNS Rule* in FortiSASE under *Configuration > DNS* to resolve hostnames for internal and external domains.

By default, FortiSASE deployments use FortiGuard DNS as the default DNS server.

You can configure the *VPN Implicit DNS Rule* and configure *Default DNS Server* with one of the following options and then click *OK* to save the change:

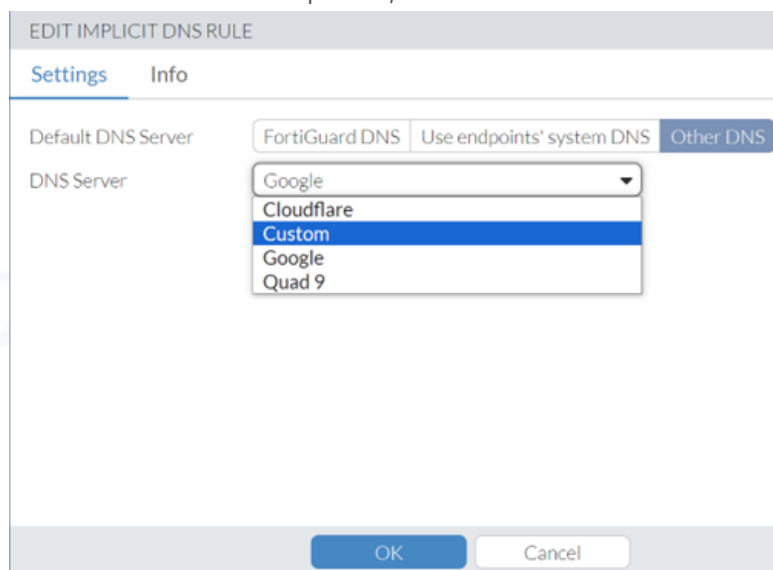
DNS Server		Description	Primary and Secondary DNS Server IP Address
FortiGuard DNS		Use FortiGuard DNS	208.91.112.53 208.91.112.52
Use endpoints' system DNS		Use the system DNS setting already configured on the agent-based endpoints	IP addresses specific to endpoints
Other DNS		Use a public DNS server other than FortiGuard DNS	IP addresses specific to public DNS server
	CloudFlare	Use the CloudFlare public DNS server	1.1.1.1 1.0.0.1
	Custom	Enable to specify your own custom primary and secondary DNS servers.	Specify IP address of primary and secondary DNS.
	Google	Use the Google public DNS server	8.8.8.8 8.8.4.4
	Quad 9	Use the Quad 9 public DNS server	9.9.9.9 149.112.112.112

For example, you can edit the VPN implicit DNS rule to use a custom DNS server as follows:

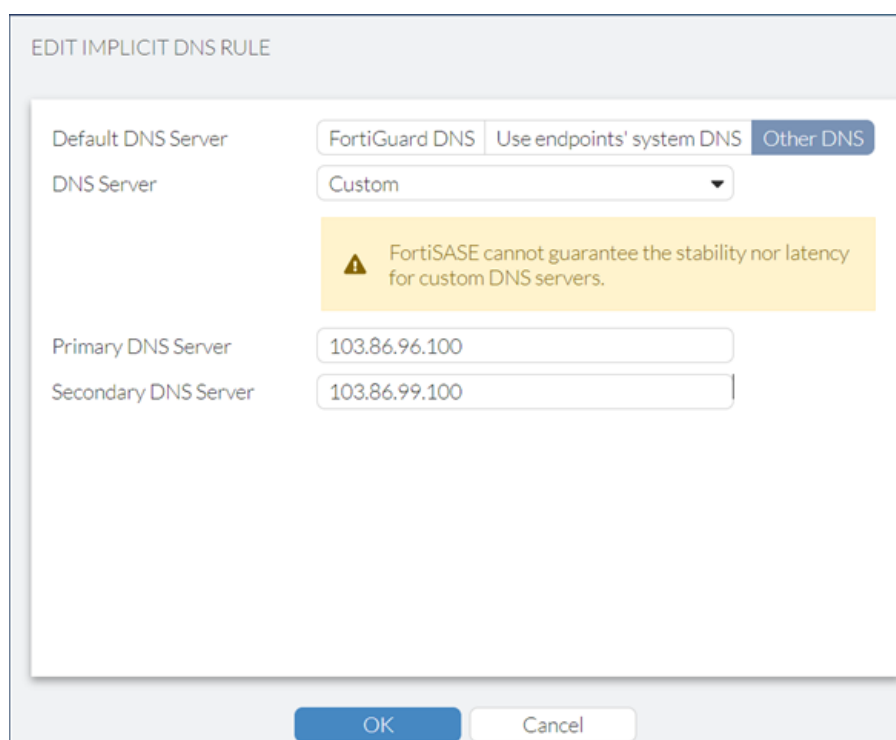
To configure a custom DNS server:

1. Go to *Configuration > DNS*, select *VPN Implicit DNS Rule*, and click *Edit*.
2. In the *Edit Implicit DNS Rule* page, for *Default DNS Server*, select *Other DNS*.

3. From the *DNS Server* dropdown, select *Custom*.



4. In the *Primary DNS Server* and *Secondary DNS Server* fields, enter the respective IP addresses for the servers of your choice.



5. Click *OK*.

Using FortiGuard DNS or another public DNS service is sufficient for most agent-based Secure Internet Access (SIA) use cases that simply require agent-based remote users to resolve hostnames for external domains.

Split DNS Rules

FortiSASE agent-based users often need to resolve internal hostnames that public DNS servers cannot resolve in scenarios including but not limited to:

- When users are located within the organization's local network, also known as being on-net, and users must use an internal DNS server instead of a public DNS server.
- When users are located remotely, FortiSASE Private Access has been configured with secure private access (SPA) hubs, and users must use an internal DNS server behind the SPA hub.

To support these scenarios, you can configure FortiSASE DNS settings for split DNS using *Split DNS Rules*.

Split DNS works as follows:

- Selectively use an internal DNS server only when it is necessary to resolve hostnames for the specified internal domain(s).
- Resolve all other hostnames for external domains using the implicit DNS rule.

Split DNS is more efficient than sending all DNS requests to internal DNS servers. Split DNS reduces any potential latency and downtime with using internal DNS servers for resolving public hostnames if any issues arise with these limited availability and limited resource internal DNS server deployments. For resolving hostnames for external domains, split DNS leverages the redundancy, extensive resources, and geographical coverage of public DNS servers with anycast capabilities.



For the scenario with on-net users who must use an internal DNS server to resolve hostnames for the internal domain, configuring split DNS using an internal DNS server with a private IP address and without an SPA hub configured in FortiSASE yields inconsistent results. When an SPA hub is not configured in FortiSASE, ensure that split DNS is configured using an internal DNS server with a public IP address.

Split DNS supports using an internal DNS server with a private IP address only when an SPA hub is configured in FortiSASE.

To secure DNS requests, the DNS-over-HTTPS (DoH) protocol secures DNS requests and replies sent and received over HTTPS and works with public DNS servers that support this protocol. DoH is enabled by default on modern web browsers including Chrome, Edge, and Firefox and is supported by Google's public DNS servers, which is the default for upgraded FortiSASE deployments. Therefore, for split DNS rules to work with DNS servers that support DoH, SSL deep inspection must be enabled for agent-based remote users on FortiSASE.

Prerequisites

SSL Deep Inspection

Split DNS requires SSL deep inspection to be enabled on FortiSASE so that FortiSASE can intercept the DNS traffic.

- To confirm SSL deep inspection is enabled, go to *Configuration > Security* and under the *SSL Inspection* widget ensure *Deep Inspection* is displayed.
- To enable SSL deep inspection, go to *Configuration > Security* and in the *SSL Inspection* widget click on *Customize*. In the *SSL Inspection* pane, select *Deep Inspection* and click *OK*.

See [Certificate and deep inspection modes](#) for further details on deep inspection.

Access to Internal DNS Server

Ensure that your FortiSASE remote users have access to the internal DNS server.



For the scenario with on-net users who must use an internal DNS server to resolve hostnames for the internal domain, configuring split DNS using an internal DNS server with a private IP address and without an SPA hub configured in FortiSASE yields inconsistent results. When an SPA hub is not configured in FortiSASE, ensure that split DNS is configured using an internal DNS server with a public IP address.

Split DNS supports using an internal DNS server with a private IP address only when an SPA hub is configured in FortiSASE.

Configuring Split DNS Rules

To configure Split DNS Rules:

1. Go to *Configuration > DNS*.
2. Click *Create*.

CREATE DNS RULE

For optimal functionality of DNS rules, enable SSL Deep Inspection for all profiles.

Primary DNS Server

Secondary DNS Server

Domains


+

OK

Cancel

3. In the *Create DNS Rule* pane, enter the *Primary DNS Server*, (optional) *Secondary DNS Server*, and one or more *Domains*. Click *+* to add more fields to enter in additional domains. Click *OK*.

CREATE DNS RULE

 For optimal functionality of DNS rules, enable SSL Deep Inspection for all profiles.

Primary DNS Server

10.10.10.10

Secondary DNS Server

10.10.10.11

Domains

domain1.com

+

OK

Cancel

4. Observe that the split DNS rule has been created and is displayed in the table.

+ Create

Edit

Delete

Q Search

Q

	Domains	Primary DNS Server	Secondary DNS Server
<div><div></div><div>DNS Rule 1</div></div>			
<div><div></div><div>domain1.com</div></div>	10.10.10.10	10.10.10.11	
<div><div></div><div>Implicit DNS Rule 2</div></div>			
<div><div></div><div>VPN</div></div>	FortiGuard DNS		
<div><div></div><div>SWG and Thin-Edge</div></div>	FortiGuard DNS		



If you are using split DNS to resolve local domains using an internal DNS server with an SPA hub configured, then the Web Filter or DNS Filter blocks access to these local domains from FortiClient remote users if the Newly Observed Domain category is set to Block in the respective security component. In this case, you must create URL Filter entries for the Web Filter or Domain Filter entries for the DNS Filter to allow access to these local domains.

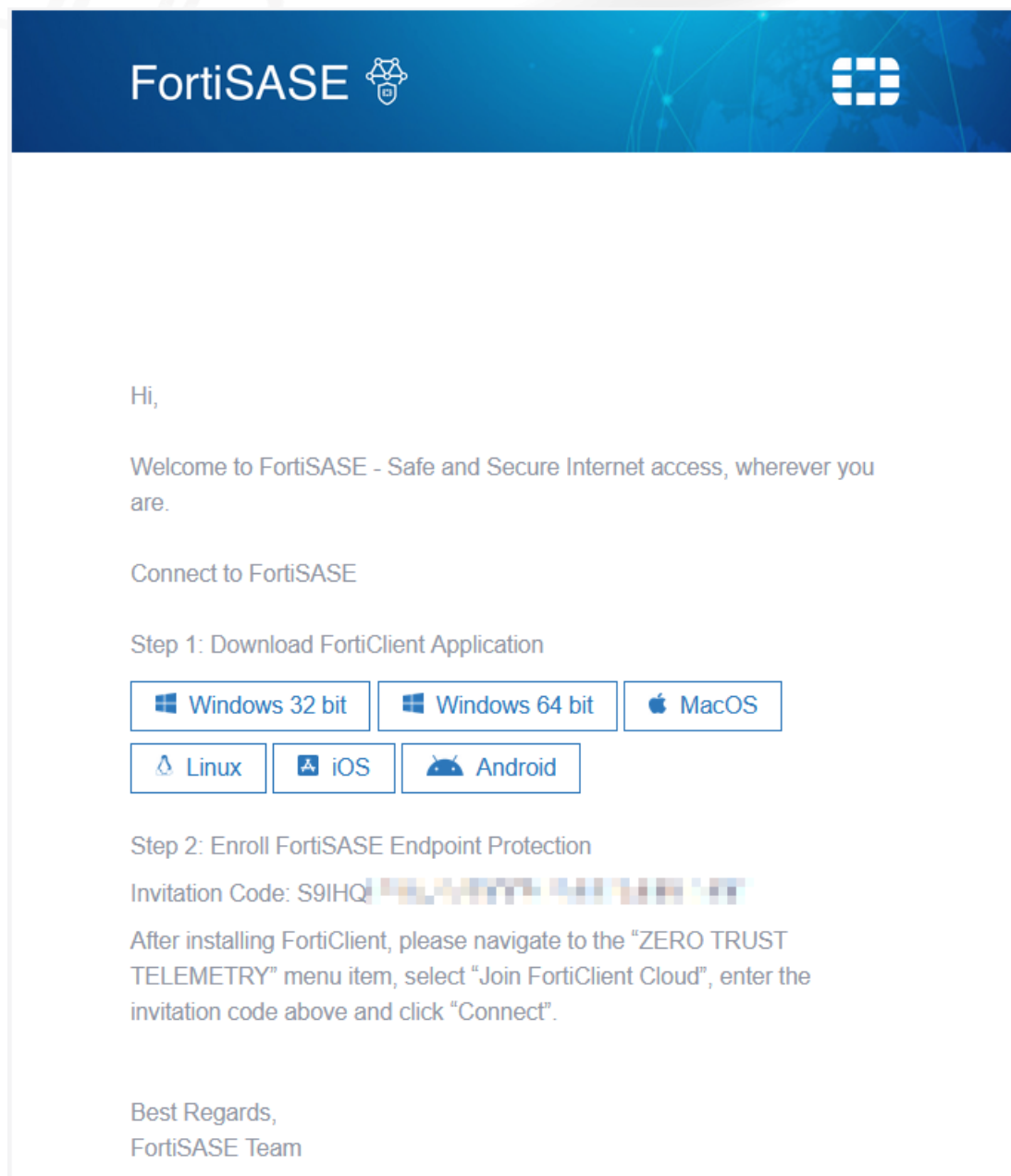


If you are using split DNS to resolve local domains using an internal DNS server with an SPA hub configured, to ensure access to the internal DNS server from FortiClient remote users you must have a Private Access policy configured that allows DNS requests to that specific server.

Downloading and installing FortiClient on Windows endpoints

As part of configuring authentication, the FortiSASE administrator can click *Onboard Users* from *Configuration > VPN User SSO*. Alternatively, administrators can click *Onboard Users* from the *Remote User Management* widget within the *Dashboard > Status* page. In either case, FortiSASE sends an onboarding email to remote end users with a download link for FortiClient for Windows, and an invitation code that is unique to your FortiSASE deployment.

An example of one of these onboarding emails is provided:



To download FortiClient, click the link in the email and then double-click on the installer file, following the prompts to complete FortiClient installation.

Connecting FortiClient to FortiSASE and provisioning the FortiSASE VPN tunnel

To connect FortiClient to FortiSASE, that is, to enroll FortiSASE Endpoint Protection, copy the invitation code from the onboarding email and paste it in FortiClient under the *Zero Trust Telemetry > Register with Zero Trust Fabric* field, and then click *Connect*.

When FortiClient has registered successfully, under *Remote Access* you should see the VPN name displayed as Secure Internet Access. After this step, your endpoint is being managed by the FortiSASE Endpoint Management Service.

Connecting a user's endpoint to the FortiSASE tunnel using FortiClient and verifying Entra ID SAML SSO configuration

In FortiClient, connect to the FortiSASE tunnel using the secure Internet access (SIA) connection (selected by default) and verify the Microsoft Entra ID SAML single sign on (SSO) configuration, using these steps:

To connect a user's endpoint to the FortiSASE tunnel using FortiClient and verify Entra ID SAML SSO configuration:

1. In FortiClient on an endpoint, go to *Remote Access*. The tab should display a *SAML Login* button.
2. Click *SAML Login*.
3. In the Entra ID prompt, sign in with your Entra ID SAML SSO credentials to connect to the FortiSASE tunnel.



FortiSASE does not send the SAML SSO credentials in the onboarding email. Your administrator should have provided this information to you beforehand through other means, which may include email.

Once the SIA connection with FortiSASE has been established, then FortiSASE is now securing all your Internet traffic.

Testing SIA using a managed FortiClient endpoint

Testing from a managed FortiClient endpoint for granular VPN policies configured on default profile

If your user belongs to the Remote-Home-Office user group and you have configured the granular VPN policies on the default profile as [Adding VPN policies to perform granular firewall actions and inspection](#) describes, you can test these granular VPN policies as follows:

1. Use the steps in the previous section to connect a user's endpoint to the FortiSASE tunnel using FortiClient.
2. From a web browser on the user's endpoint, access www.fortinet.com.
3. FortiSASE attempts to match the RemoteHomeOffice-DenyNetflix, but the traffic is not for *.netflix.com.

4. Then, FortiSASE attempts to match the next VPN policy, the RemoteHomeOffice-AllowFortinet policy, which matches. FortiSASE allows the user access to www.fortinet.com.

Testing from a managed FortiClient endpoint for Application Control enabled

You can test one of the following examples when Application Control is enabled to block YouTube.com:

- Your user belongs to the Remote-Home-Office user group with a non-default security profile defined with Application Control enabled as Configuring a Security Profile Group and Applying it to a Policy describes.
- Application control is defined in the Default Profile as described in Configuring Application Control.

Verifying endpoint connectivity on FortiSASE

To verify endpoint connectivity on FortiSASE:

1. Log into FortiSASE as the administrator.
2. Go to *Dashboards > Status*, expand the *User Connection Monitor* widget, and confirm the user that you used to establish a connection to FortiSASE is online.
3. Go to *Dashboards > Status*, expand the *Managed Endpoints* widget and confirm the endpoint that you used to establish a connection to FortiSASE is online.
4. Go to *Analytics > Traffic > Internet Access Traffic* to see logs for your Internet access activity. You can double-click the log to see details.
5. Alternatively, you can view data for access attempts on the FortiView Sources dashboard. You can view the application, destination, and VPN policy information.
6. You can view data for cloud application access attempts on the Cloud Applications dashboard. Go to *Dashboards > FortiView Cloud Applications* to see the cloud traffic information detected by SSL deep inspection and Application Control.

More information

Appendix A: Products used in this guide

For a list of product models and firmware that this guide uses, see [Product integration and support](#).

Appendix B: Documentation references

Feature documentation

Product document	Specific chapter if available
FortiSASE Admin Guide	<ul style="list-style-type: none">• Endpoint mode• Dashboards• Configuration• Analytics
FortiClient 7.0 Admin Guide	<ul style="list-style-type: none">• Provisioning preparation• Manually installing FortiClient on computers

4-D resources: SASE

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



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 Chief Legal Officer, 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.