FORTINET

Deployment Guide

ZTNA for Web Applications

4D

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

Change Log

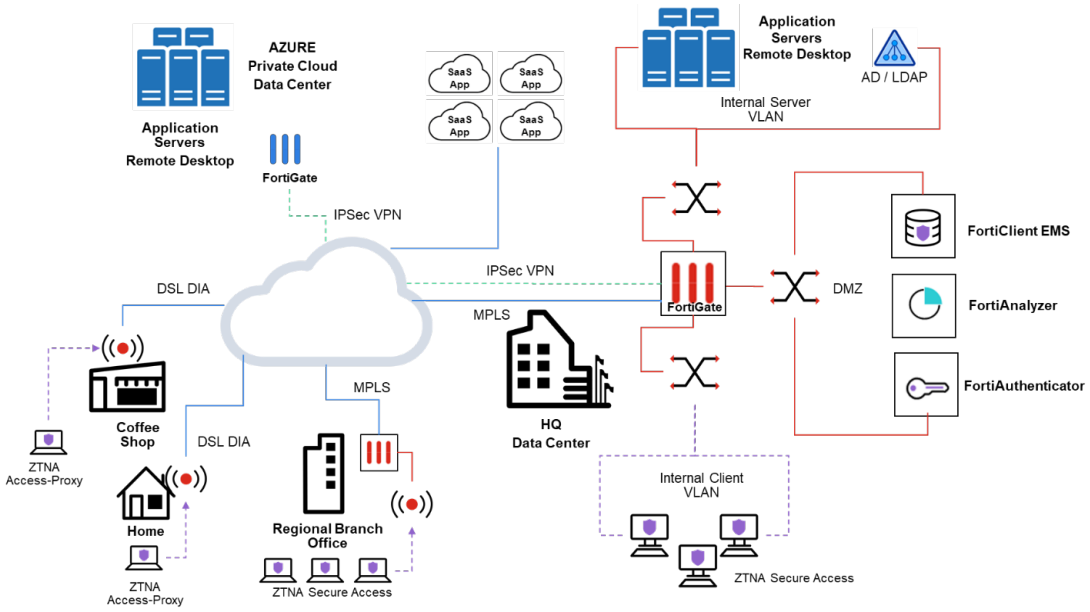
Date	Change Description
2025-05-27	Initial release.

Deployment overview

This document provides a deployment example of ZTNA for Web Applications's Zero Trust Network Access (ZTNA), covering the following solutions:

- ZTNA application gateway:
  - Fabric connection to FortiClient EMS
  - HTTPS access proxy for web applications
  - ZTNA IP/MAC based access control for local users accessing the web applications
  - No persistent connection, such as VPN, is necessary

Using a similar scenario and topology example from the ZTNA Architecture Guide, we will walk through deploying the core components necessary to complete the requirements above. The goal is to reduce the reliance on dial-up VPN by using ZTNA to unify remote access and local access to web applications using role-based access control concepts.



Intended audience

Mid-level network and security architects in companies of all sizes and verticals should find this guide helpful. A working knowledge of FortiOS, FortiClient, FortiClient EMS, and the ZTNA for Web Applications Security Fabric is helpful.

About this guide

This deployment guide describes the steps involved in deploying a specific architecture. Readers should first evaluate their environment to determine whether the architecture outlined in this guide suits them. It is advisable to

review the reference architecture guides, such as the ZTNA Architecture Guide, if readers are still in the process of selecting the right architecture. See also the ZTNA 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.

For comments and feedback, please visit Basic ZTNA Deployment on community.fortinet.com.

Design considerations

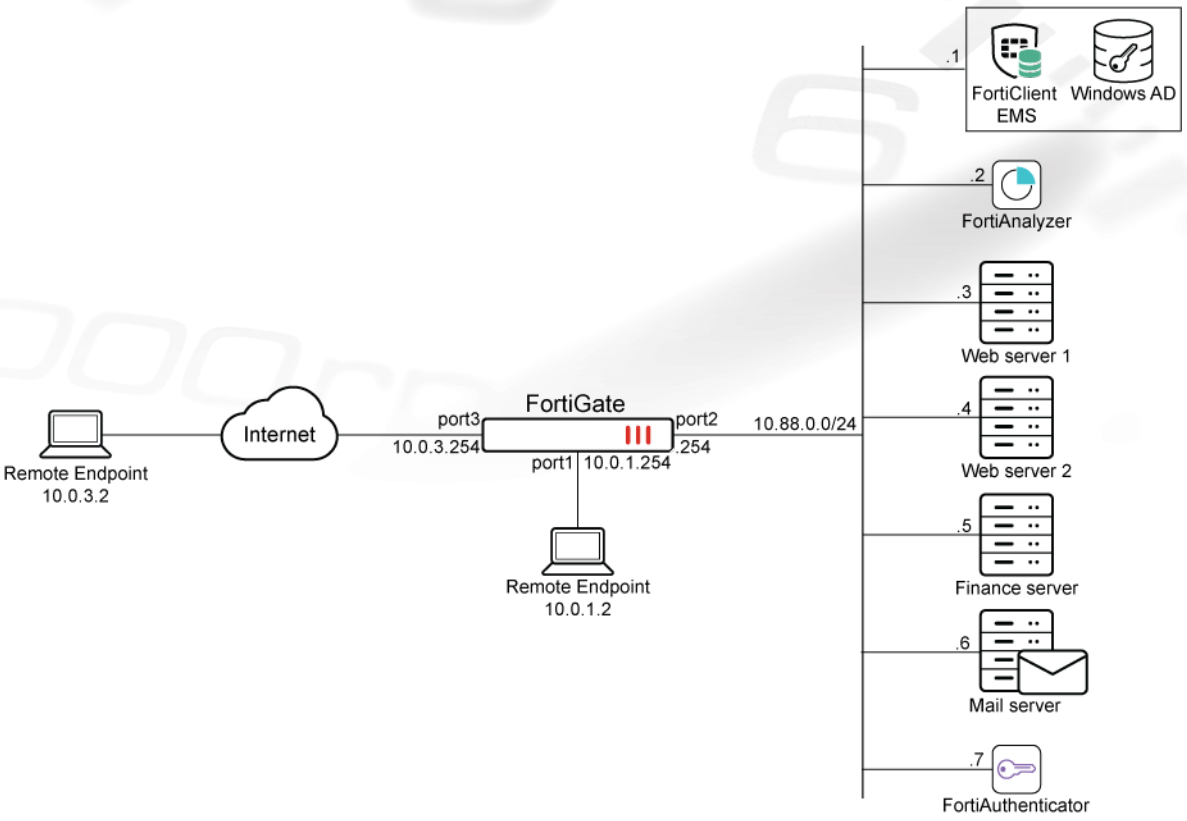
Traditionally, VPN is used to secure data flowing in an otherwise insecure connection. However, the method of access over VPN often doesn't account for the risk of infected or non-compliant endpoints infecting network devices. Also, endpoints must have a persistent tunnel in order to connect to the protected resources.

Migrating to Zero Trust Network Access allows administrators to control many of these factors by means of requiring client certificates and user authentication to authorize the access. Furthermore, security posture checks ensure that endpoint device health is monitored in real time while users are accessing resources.

When designing your Zero Trust Access solution, and in this case, ZTNA access to internal web applications, several things will need to be considered:

- What are the web applications that you want to allow for our users?
- How will users resolve the address to these web applications?
- What are the user groups that are allowed access to the web applications?
- Who will authenticate the users? Where does the authentication server reside?
- Where will users be accessing the web applications from?
- What are the required security postures for an endpoint to access the resources?
- Where is the optimal location for the EMS server?
- How do you provision and onboard FortiClient endpoints?

Answering these questions will help you make the design choices necessary to configure your ZTNA solution. Using the following simple topology, we will run through the design decisions that administrators will typically encounter.



ZTNA server mappings

Relevant questions:

- What are the web applications that you want to allow for our users?
- How will users resolve the address to these web applications?

Consider the web applications that you will be exposing for your users. Which resources are your users allowed to connect to? Which ones will need to be protected?

In the example topology, the web applications that need to be accessed can be broken down into:

Web server/application	Protected access
Web server 1	Yes
Web server 2	Yes
Finance server	Yes
Mail server	No, all users are allowed to access web mail from anywhere

The protected web servers and applications will become the ZTNA server mapping used in your ZTNA configurations.

Next, consider how users currently resolve the FQDN addresses of the web applications. When accessing the applications internally or through VPN, users can resolve the addresses using an internal DNS server. Essentially, the same FQDN resolves to the same private IP address internally or remotely.

When using ZTNA, a remote user accessing a protected web application must resolve the FQDN address of the resource to the HTTP access proxy address on the FortiGate. Therefore, a public DNS record must be configured.

Meanwhile, when resolving the FQDN address internally, clients can continue to use an internal DNS server to resolve the address to the server's private IP address.

User authentication

Relevant questions:

- What are the user groups that are allowed access to the web applications?
- Who will authenticate the users? Where does the authentication server reside?

Consider the user groups that are allowed to access each web application. Are the user groups clearly defined? Are the same user groups configured on your authentication server? To use the same user groups to control access, the FortiGate needs to be able to connect to the authentication server and synchronize the groups locally.

There are several ways to perform authentication on the FortiGate:

Method	Description
No Authentication	If your applications do not need to be segmented by user groups, you can consider not applying any authentication. However, all users will have access to your protected resources and logs will not be able to indicate the user who accessed the resources.
Local	Use local authentication only if you do not have any central authentication solution and you only have few users to authenticate on a single FortiGate.
Remote	Use remote authentication when you have a central authentication solution such as a Windows AD and one or more FortiGates need to connect to the authentication server. The connections are most commonly made through LDAPS and RADIUS locally to the authentication server.
SAML	Use SAML authentication when your Identity Provider (IdP) is remote or in the Cloud (such as Azure AD) or you rely on an IdP proxy to connect the FortiGate to the remote Identity Provider.

In the example topology, the Windows AD handles authentication for the entire *FortiAD.Info* domain. Using LDAPS, the FortiGate can connect directly to the Active Directory and synchronize the user groups.

In cases where the authentication server is not local to the FortiGate, the FortiGate can act as a Service Provider (SP) and redirect authentication to an IdP or an IdP proxy such as FortiTrust-ID.

ZTNA policies

Relevant questions:

- Where will users be accessing the web applications from?

It is assumed that users will be accessing the web applications remotely and from within the local network.

For remote users, access will be granted using simple or full ZTNA policies. These policies define the granular source and destination pairs that are allowed to connect. The ZTNA servers will be used in the ZTNA policies to map to web applications that are exposed to the end users. Client certificates will be checked to verify the endpoint devices, and security posture check can be performed using Security Posture tags. Finally, user authentication can be applied to control the user groups that have access to the ZTNA servers.

For local users, their optimal path will be to access the internal web applications directly instead of accessing them through the ZTNA application gateway. These policies can use Security Posture tags to perform security posture checks and user groups to granularly control the users who have access.

Managing endpoints and Security Posture tags using FortiClient EMS

Relevant questions:

- What are the required security postures for an endpoint to access the resources?
- Where is the optimal location for the EMS server?
- How do you provision and onboard FortiClient endpoints?

Security posture defines the rules and logic that determine whether an endpoint meets the device security requirements to access internal resources. This can be criteria related to the vulnerability status of the endpoint, the applications installed on it, the domain and user group it is joined to or many other factors. These rules are configured on the EMS server as Security Posture tags and pushed to the managed endpoints where they are evaluated. Security Posture tags identify the result of processing the ZTNA rules on the endpoints. They are used by the FortiGate in ZTNA policies for access control.

FortiClient EMS is used to manage and push configurations, Security Posture tags and client certificates to the endpoints. It also has a persistent connection to the FortiGate to communicate information about the endpoints to the FortiGate.

Therefore, consider the endpoints that will connect to your FortiClient EMS as well as FortiGates that will connect. Different locations you can consider include deploying the EMS server on-premise behind the FortiGate, deploying in the public Cloud or using FortiClient Cloud.

Deploying on-premise may be ideal when you have the resources necessary to manage the server internally. However, you will need to define firewall policies to allow proper access to EMS internally and remotely. Whereas FortiClient Cloud offers EMS as a service that can be accessed from anywhere.

Finally, consider how FortiClients will be provisioned, and how users can be securely onboarded to EMS. For smaller deployments, administrators can send invitations with FortiClient installers for users to download and install manually. For larger deployments, it may be more feasible to use a MDM solution to provision FortiClient instead.

Success criteria

In the ZTNA design, the goal is to enhance security by improving identity and posture checking of devices connecting to the internal network, and by reducing the attack surface of traditional dial-up VPN. In our use case, the following success criteria is detailed:

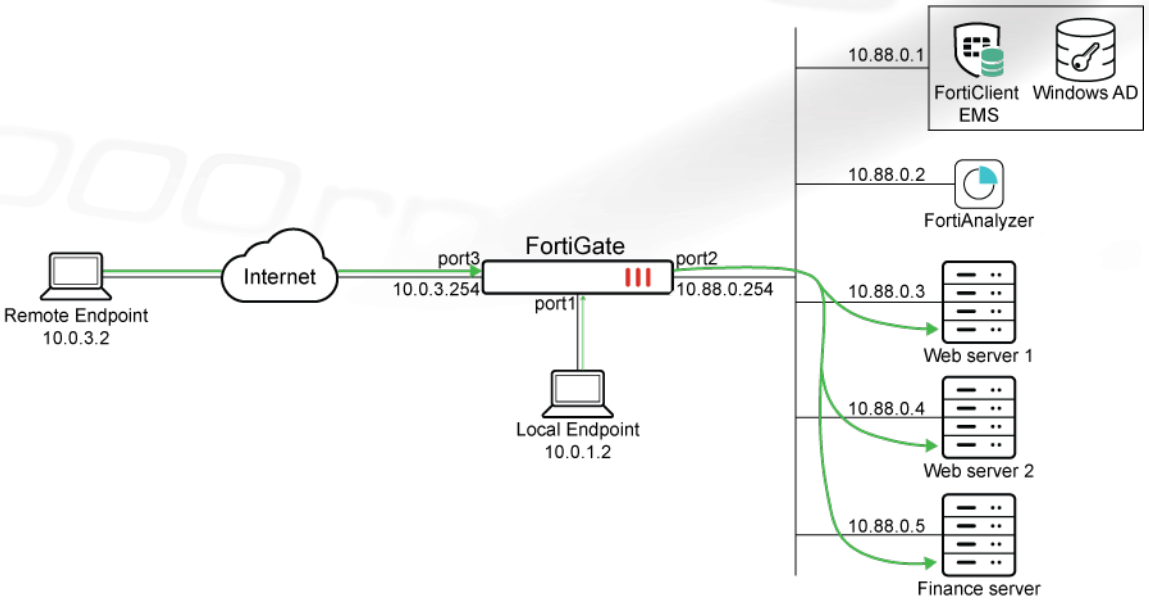
- Block unmanaged devices.
- Limit remote access to the internal network for web applications only.
- Allow only identified user groups access to only the specific applications that they need.
- Dynamically deny access to devices with critical vulnerabilities both on the internal network and remote locations.
- Dynamically allow access once the vulnerabilities are remediated.
- Reduce the reliance on dial-up VPN.

Product requirements

The following table lists the product requirements:

ZTNA Solution	Licensing	Description
FortiClient ZTNA client 7.0 and above	Review the FortiClient data sheet.	Available deployment techniques include: an existing software deployment tool (for example, SCCM), native deployment through FortiClient EMS (Windows only), and a manual download location accessible for outliers.
FortiClient Endpoint Management Server (EMS) 7.0 and above	Included with FortiClient ZTNA license.	FortiClient EMS must be accessible to clients from everywhere. In this design, FortiClient EMS is deployed in a DMZ. Active Directory integration to FortiClient EMS may also be necessary for client deployment and ease of applying different endpoint profiles to corresponding groups in AD.
FortiOS ZTNA Application Gateway 7.0 and above	Included with FortiOS. Minimum recommended bundle is Unified Threat Protection. Recommended bundle is Enterprise Protection.	Review FortiGate performance requirements, and ensure existing FortiGates meet those requirements. In this simple deployment example, the FortiGate and Security Fabric are central to all traffic and to protect traffic flow to critical resources.
FortiAuthenticator Identity and Access Management (IAM)	Review FortiAuthenticator data sheet.	When multiple FortiGates are deployed, FortiAuthenticator is desirable to consolidate and manage connections to IdPs, including Active Directory, LDAP, Radius, and SAML providers. In this use case, FortiAuthenticator is not strictly necessary, but is included in the deployment as an example for larger deployments.
FortiToken Multi-factor Authentication (MFA)	Review FortiToken data sheet.	MFA is recommended for connecting to any critical resources. In addition to device and user authentication, another factor of authentication that utilizes one-time passwords (OTP) is desirable to help protect against stolen credentials.
FortiAnalyzer	Review FortiAnalyzer data sheet. VM and hardware models available. License by anticipated log volume.	FortiAnalyzer is recommended for gathering logs, analyzing logs, and generating reports for ZTNA for Web Applications devices. FortiAnalyzer should be available from everywhere. FortiClient ZTNA sends logs directly to FortiAnalyzer.

Deployment procedures



In this deployment example, we will demonstrate remote and local access to protected web applications as indicated by the traffic arrows above. In this case, FortiGate has the necessary LDAP configurations to connect to the local Active Directory server for user authentication. Firewall policies are assumed to be configured on the FortiGate for accessing the FortiClient EMS from local and remote locations.

We will create two ZTNA servers for our ZTNA application gateway. One ZTNA server allows access to the Web servers for users that are part of the Remote-Allowed user group. Another ZTNA server allows access to the Finance server for the Finance group only.

Local access will use ZTNA IP/MAC based access control to apply Security Posture tags for security posture check. It will also restrict access to the user groups above.

The following is an overview of the procedure:

1. EMS server configurations on page 12
   a. Securing EMS communication on page 12
   b. Individual user onboarding on page 13
   c. Importing an Active Directory Domain on page 14
   d. Configuring EMS Security Posture tags on page 16
   e. Registering to FortiClient EMS and verifying Securtiy Posture tags on page 18
2. Connect the FortiGate to EMS on page 20
3. Applying user authentication on page 21
4. Configure ZTNA application gateway on the FortiGate on page 22
5. Configure ZTNA policies to control remote access on page 25
6. Verify ZTNA access to the web applications on page 27
7. Configure firewall policies with IP/MAC based access control for internet access on page 30

EMS server configurations

This section includes:

Securing EMS communication

In order to secure the connection between FortiClient endpoints and FortiClient EMS, as well as between the EMS server and the FortiGate, EMS must present a certificate that is trusted by the connecting entities.

By default, FortiClient EMS uses the certificate issued by FortiCare to each licensed EMS server for securing web server access and endpoint control. However, the certificate is not issued by a public CA and may not be natively trusted by connecting endpoints or the FortiGate.

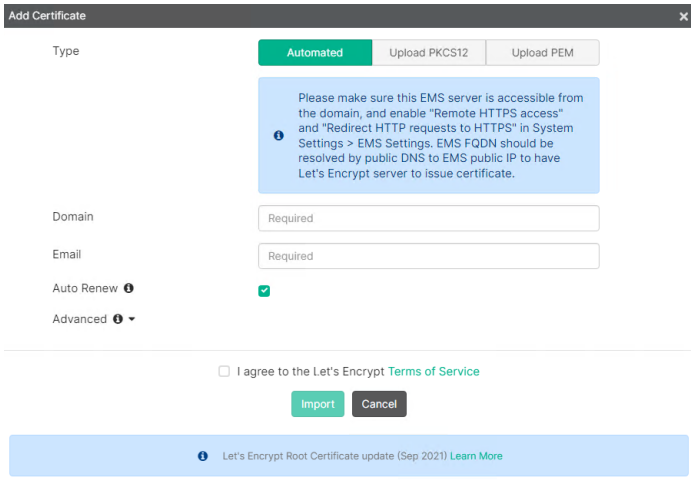
Therefore, it is recommended to either:

- Issue a server certificate to the EMS server by a public CA.
- Issue a server certificate to the EMS server using an ACME server.
- Issue a server certificate to the EMS server by a private CA that can be synchronized to all endpoints using a group policy.

For information about different kinds of EMS server certificates, see Server Certificates.

To issue a certificate through ACME or to upload an issued certificate:

1. Go to *System Settings* > *EMS Server Certificates*.
2. Click *Add*.
3. In the pop-up window, choose one of the certificate types.



4. Continue to configure as needed.
5. Click *Import* to upload the certificate.

For more information about uploading a certificate, see Adding an SSL certificate to FortiClient EMS.

To apply the uploaded certificate:

1. Go the *System Settings > EMS Settings* page to apply the newly uploaded certificate as the *Webserver certificate* and the *Endpoint Control certificate*.

The *Webserver certificate* is used for secure access to the web interface of EMS. This can be for administrative web access through the browser or connecting to the EMS API with the FortiGate EMS Fabric Connector. The *Endpoint Control certificate* secures the communication between EMS and FortiClient.

   a. Click the drop-down arrow next to *Webserver certificate* then select an uploaded certificate from the menu.
   b. Enable the option *Use Webserver certificate for Endpoint Control*.
   c. Click *Save* to save the changes.
      A warning appears to indicate the server must be restarted.
   d. Click *Yes* to continue.
2. After a few minutes, refresh the browser and return to the *System Settings > EMS Settings* page. The new certificate should now be applied.

Individual user onboarding

For greater security and for use with user-based licensing, user onboarding should be configured. This allows you the option to verify user identity during the registration process. By enforcing user verification, you can secure the connection between EMS and endpoints and block unknown users and endpoints from registering to EMS.

With user-based licensing, a user can register up to three endpoint devices under one user license.

The following types are supported:

Verification types	Description
None	End user does not need to provide any credentials to connect to EMS.
Local	End user must provide credentials that match a local user configured in *User Management > Local Users* to connect to EMS.
LDAP (Active Directory Domain)	End user must provide their domain credentials to connect to EMS. You must configure an Active Directory domain through LDAPS to configure this option.
SAML	End user must provide their credentials for an SAML identity provider, such as Azure Active Directory (AD), to connect to EMS.

No verification

This option is not recommended in production, because it allows any endpoint devices to register to EMS, potentially even malicious ones. Unknown devices that register to EMS take up unnecessary licenses, and synchronizes settings such as VPN tunnel configurations and ZTNA destinations that should not be exposed outside the organization.

In a controlled lab or staging environment, this option may be acceptable.

Local verification

This option is useful when the number of managed users is small or when no remote identity provider is available.

LDAP or SAML authentication

These are the most desirable options as they allow users to be synchronized from remote, or redirect the authentication to the SAML IdP in the case of SAML. Users credentials are not stored locally and end users do not need to remember another user credential and password. This is a very scalable solution for user onboarding.

For information on how to configure verification for user onboarding, see the User Management chapter in the EMS Administration Guide.

Importing an Active Directory Domain

If you manage your users in an Active Directory, integrating your EMS with the Active Directory using LDAP would be highly recommended.

In EMS 7.2.0 and above, adding an Active Directory Domain has been enhanced to ease the importing of specific OUs & User Groups using a “tree style” for selection. This can be used with User Onboarding to choose which groups should be allowed to onboard their FortiClient endpoints. Importing the OUs and User Groups also allows you to configure Security Posture tags that verify a User in an AD Group.

To import an Active Directory Domain:

1. Go to *Administration* > *Authentication Servers*.
   a. Click *Add* > *Active Directory*.
   b. In the *Active Directory* screen, fill in the following information to connect to Active Directory.

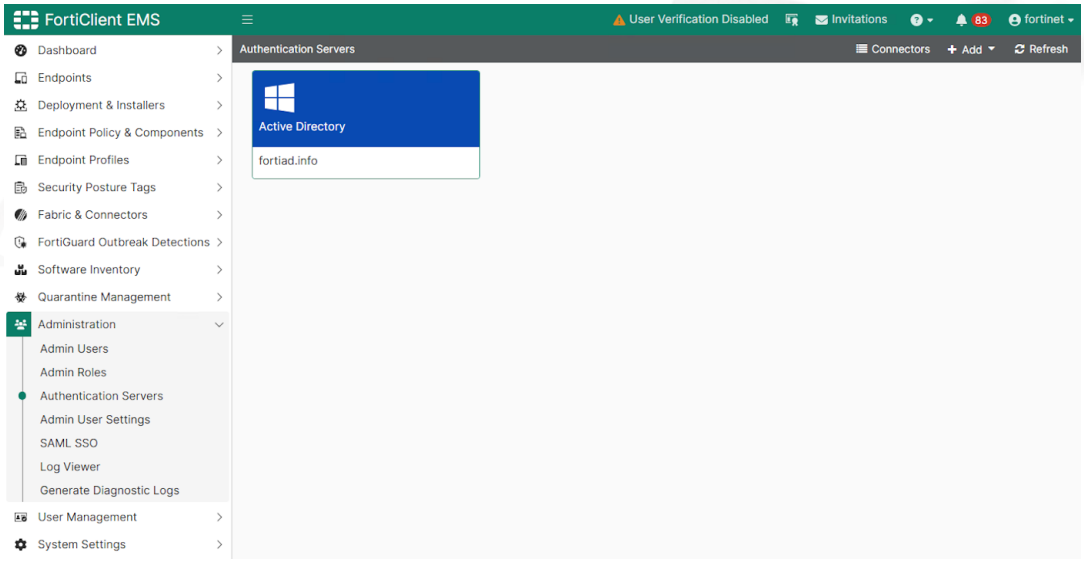
Field	Value
IP address/Hostname	IP address or hostname of the Active Directory server.
Port	636 (default port for LDAPS)
Username	Username for the LDAP bind*
Password	Password
LDAPS connection	Enabled (default)
Certificate	EMS must verify the chain of trust for the server certificate issued for the AD server. Import the necessary CA certificate if the AD server certificate was signed by a private CA.
Certificate hostname check	Verify the server hostname against the server certificate.
Alias	Optional field to name this server entry. If blank, then the name of the domain is the name for this server.

When configuring an LDAP connection to an Active Directory server, an administrator must provide Active Directory user credentials. Apply the principle of least privileges, namely, for the LDAP regular bind operation. Do not use credentials that provide full administrative access to the Windows server as this may compromise the security of the server.

c. Click *Test*.

d. Click *Save*.

Once connected, the card for the domain appears. For example, a card for the domain fortiad.info:



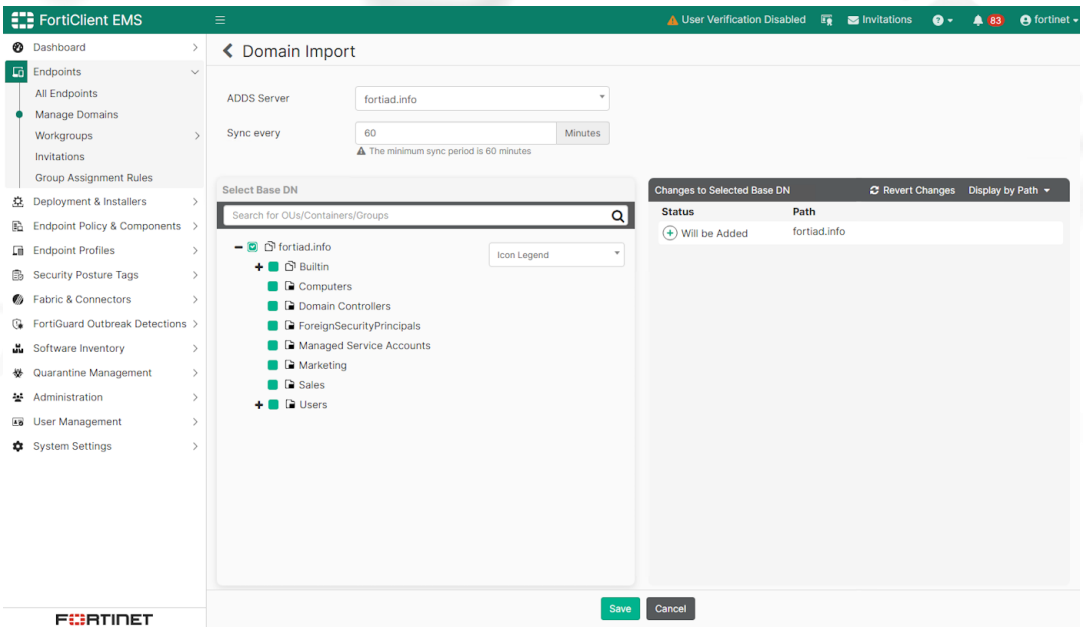
For more information, see Adding an AD server.

While the Authentication Server entry defines the connection to the AD server, you will also need to specify what you want to import from the server. With the new tree style view in EMS 7.2.0 and above, this can be as easy as selecting the Domian, OU, or Group directly for import.

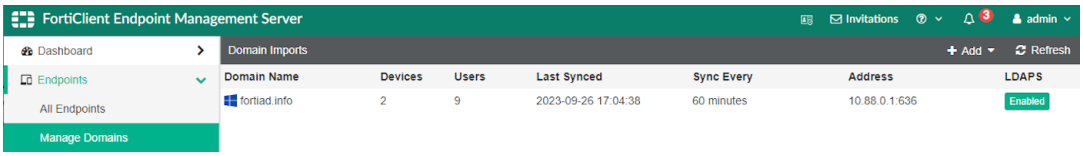
To import OUs, Groups, or the entire Domain:

1. Go to *Endpoints > Manage Domains*.
2. Click *Add > Active Directory*.
3. In the *Domain Import* screen, click the drop-down next to *ADDS Server*.
4. Select your domain.
5. The *Sync every* setting can be set to 60 minutes or above.
6. Under *Select Base DN*, the entire imported Domain will be displayed. Select either the entire domain, an OU/Container, or a Group.

   Once selected, the panel on the right displays the changes to the base DN that will be submitted.



7. Click *Save*.
8. Review the imported domain. The number of devices and users imported are displayed. Click once on your domain to display options such as *Edit*, *Delete*, and (Manual) *Sync*.



9. Under *Endpoints* > *Domains*, view the imported Domain, OUs, or Groups. Select an OU or Group to further view the endpoints. The endpoints can now be managed by the Group.

For more information, see Adding endpoints using an AD domain server.

Configuring EMS Security Posture tags

Security Posture tags define the security posture checks that should be performed on the FortiClient endpoints. They may reveal the current AD group status, whether the endpoint has AntiVirus software installed, whether it's logged on to a domain, various information about the device such as OS version, running processes or registry key value. They may also reveal the device's vulnerability level, the presence of a vulnerability by CVE, and other threat related posture on the device. These tags are valuable input to the FortiGate ZTNA application gateway as it passes them through the trust algorithm in order to make a policy decision and perform enforcement.

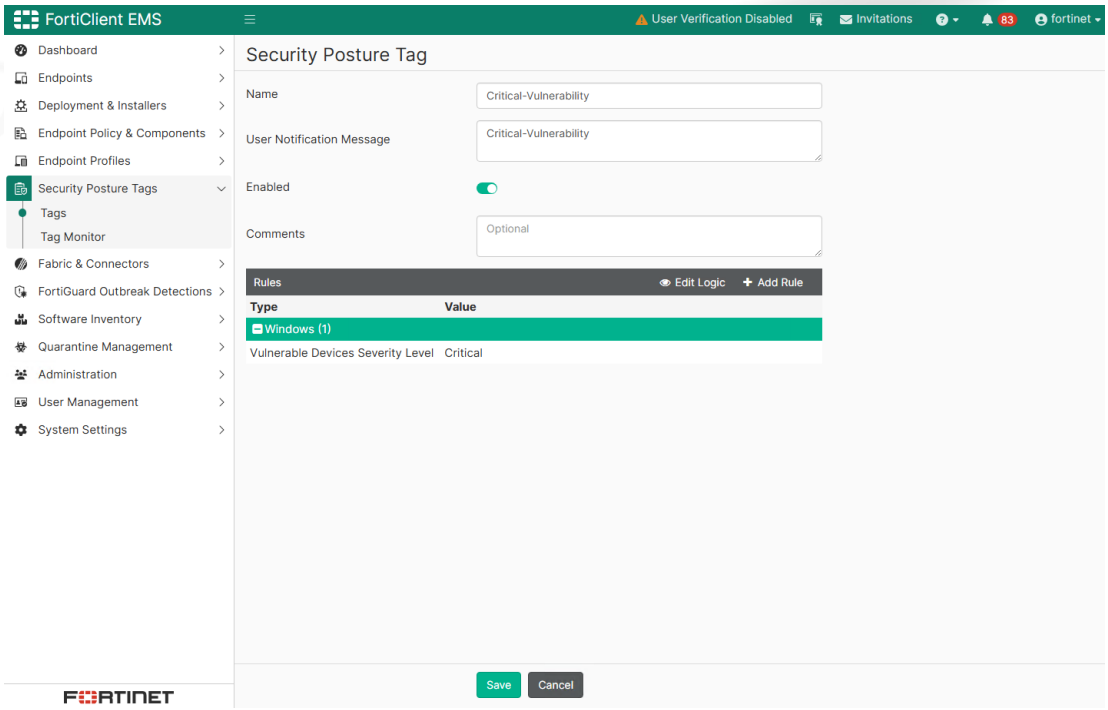
There are many tags to choose from and this will be very customized for each organization. For general steps on how to define tags, see Tags.

The following example demonstrates how to configure a rule for detecting the presence of a Critical vulnerability on an endpoint.

To configure a rule for detecting the presence of a Critical Vulnerability:

1. Go to *Security Posture Tags* > *Tags*.
2. Click *Create*.
3. Enter the name *Critical-Vulnerability*.
4. For *User Notification Message*, enter *Critical-Vulnerability*.
5. Under *Rules*, click *Add Rule*.

6. In the *Add New Rule* dialog, configure the following:
   a. Set *OS* as *Windows OS*.
   b. Set *Rule Type* as *Vulnerable Devices*.
   c. Set *Severity Level* as *Critical*.
   d. Click *Save*.
7. Click *Save* again.



To create another Security Posture tag for Domain Users:

1. Go to *Security Posture Tags* > *Tags*.
2. Click *Create*.
3. Enter the name *Domain-Users*.
4. For *User Notification Message*, enter *Domain-Users*.
5. Under *Rules*, click *Add Rule*.
6. In the *Add New Rule* dialog, configure the following:
   a. Set *OS* as *Windows OS*.
   b. Set *Rule Type* as *User in AD Group*.
   c. Disable *Evaluate on FortiClient*.
   d. Set *AD Group* as *Users/Domain Users*.
   e. Click *Save*.
7. Click *Save* again.

Additionally, it is useful to display the Security Posture tags in the FortiClient endpoint.

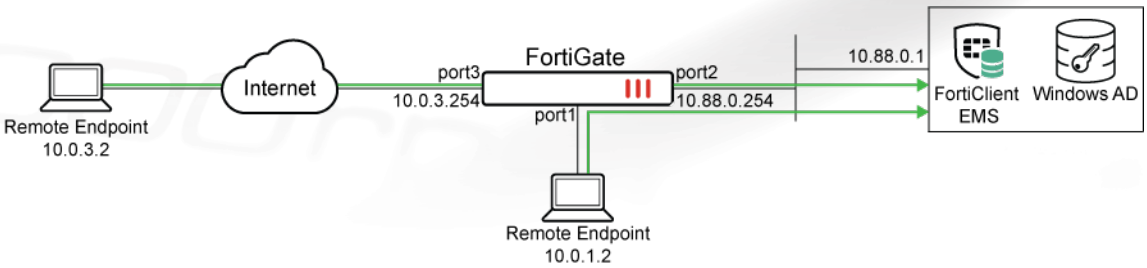
To configure the Security Posture tag to display on the FortiClient:

1. Go to *Endpoint Profiles* > *System Settings*.
2. Edit the *Default* profile under *System Settings*.
3. Ensure that *Advanced settings* is selected (top right of window).
4. Under *UI*, enable *Show Security Posture Tag on FortiClient GUI*.
5. Click *Save* to save changes.

Registering to FortiClient EMS and verifying Securtiy Posture tags

FortiClient endpoints need to be able to reach FortiClient EMS over the FortiClient telemetry port (TCP/8013 by default) in both On-net and Off-net situations. Depending on where FortiClient EMS is located, either on-premise or in the Cloud, such as FortiClient Cloud, the proper firewall policies will need to be configured.

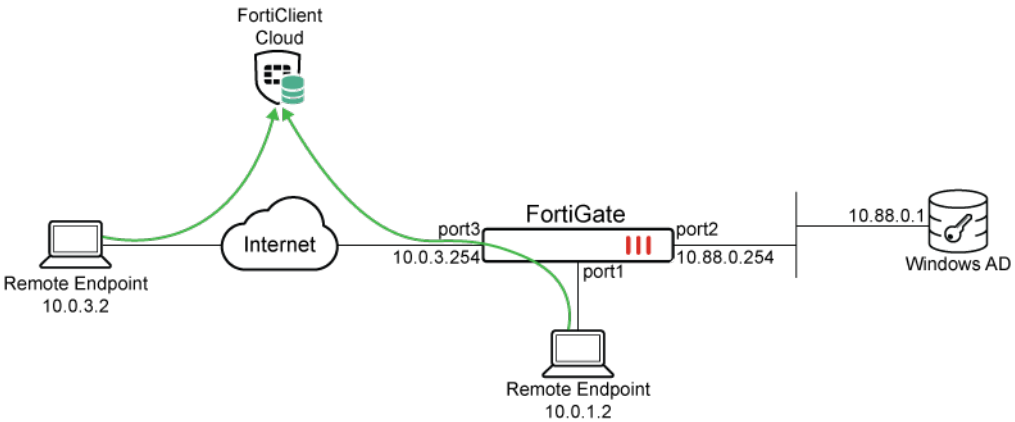
In the example topology below, FortiClient EMS is deployed on-premise:



The following will need to be configured:

- A VIP and firewall policy on the FortiGate to allow external connections to FortiClient EMS on 10.88.0.1:8013. If FortiClient download is needed, also allow the HTTPS port (443 by default).
- A firewall policy allowing internal subnets to connect to FortiClient EMS.
- The FQDN of the FortiClient needs to be resolvable internally and remotely. This may require the FQDN to be registered on a public DNS.

In this example topology below, FortiClient Cloud is used:



The following will need to be configured:

- A firewall policy allowing internal subnets to connect to FortiClient Cloud. If FortiClient download is needed, also allow the HTTPS port (443 by default).

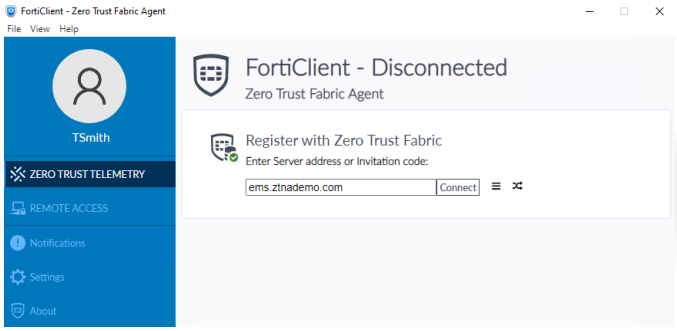
Registering users and endpoints to EMS

This step can be used to verify that users can successfully connect to EMS. Depending on whether user verification is needed and the need to send out an invitation link, users will use different codes to register on their FortiClient endpoint.

The following example demonstrates a basic endpoint registration to the ems.ztnademo.com server without any user authentication.

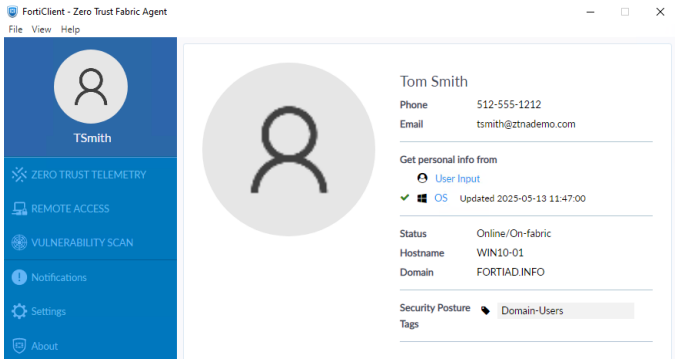
To register endpoints:

1. In the *Zero Trust Telemetry* page, enter the server address *ems.ztnademo.com*.
2. Click *Connect*.



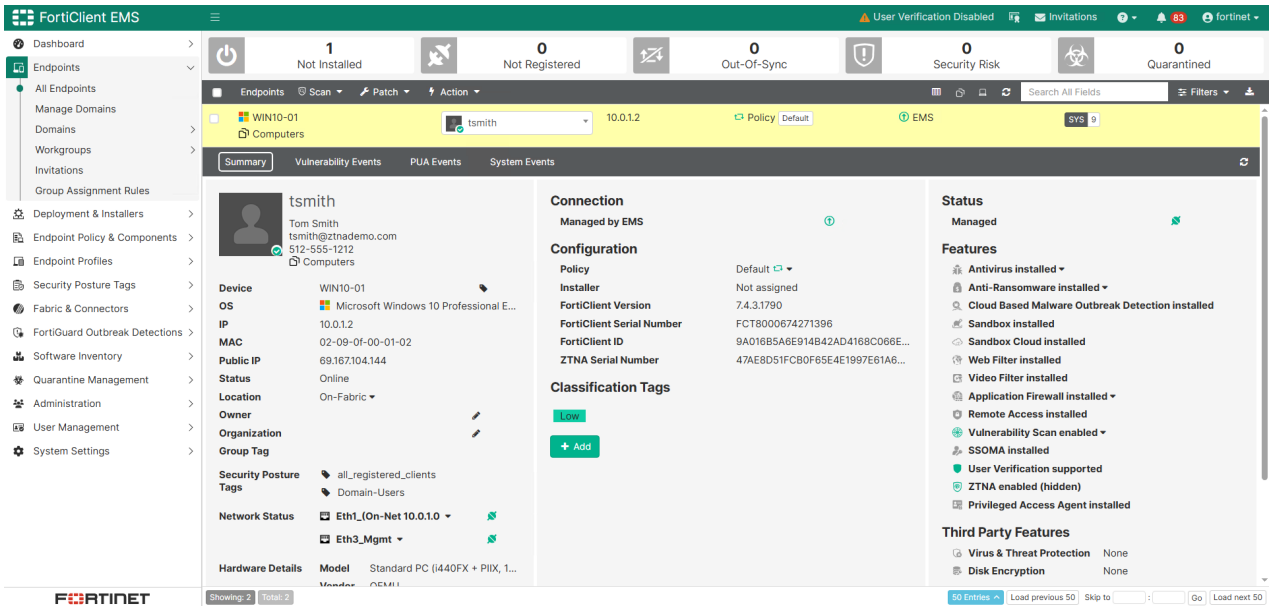
Once connected, a notification appears indicating settings have been pushed from EMS.

3. Shortly after, click on the avatar to view information about the device. Note that *Security Posture Tag Domain-Users* is added.



4. From FortiClient EMS, go to *Endpoints > All Endpoints*.
5. Select the *WIN10-01* computer.

Note that the device is successfully registered, and *Security Posture Tags* display the *Domain-Users* tag.

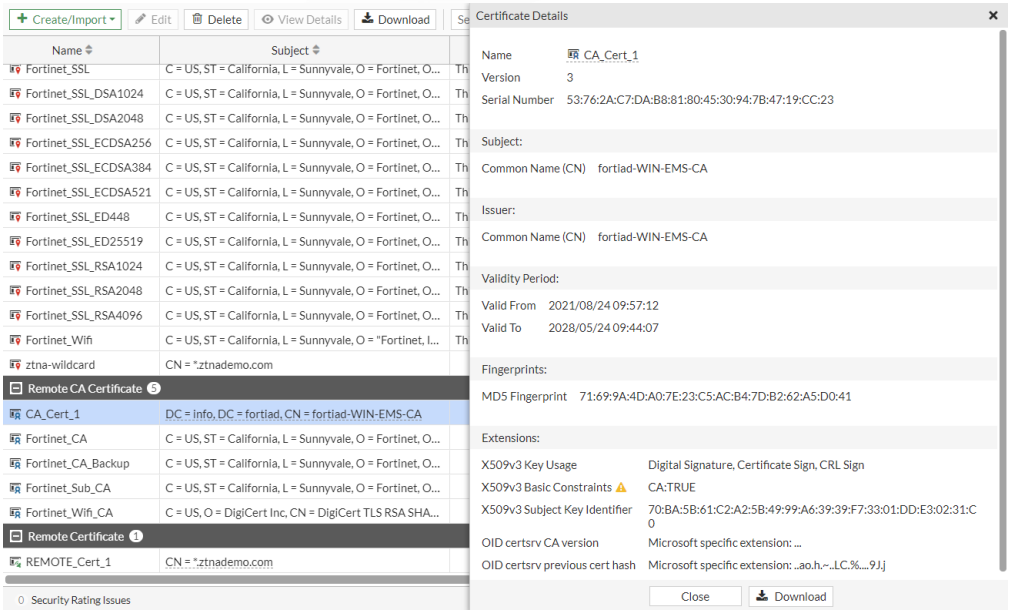


Connect the FortiGate to EMS

FortiGate must securely connect to FortiClient EMS in order to protect the synchronization of endpoint and Security Posture tag information. As such, the FortiGate must have a trusted certificate chain for the EMS server certificate. The first step before connecting to EMS is to upload the CA certificate, if the EMS server certificate is not signed by a public CA.

To manually upload the CA certificate on the FortiGate:

1. Go to *System* > *Certificates*.
2. Click *Create/Import* > *CA Certificate* to import a certificate.
   The imported certificate will appear under *Remote CA Certificate* as *CA_Cert_1*.



3. (Optional) The certificate can be renamed in the CLI using the following command:

```
config vpn certificate ca
    rename CA_Cert_1 to <new name of cert>
end
```

Next, using the Fabric Connector GUI on the FortiGate, configure the EMS fabric connector to connect to FortiClient EMS. As part of the connection process, the certificate chain to the EMS server certificate will be verified. Administrators must also examine the server certificate for authenticity and accept the certificate.

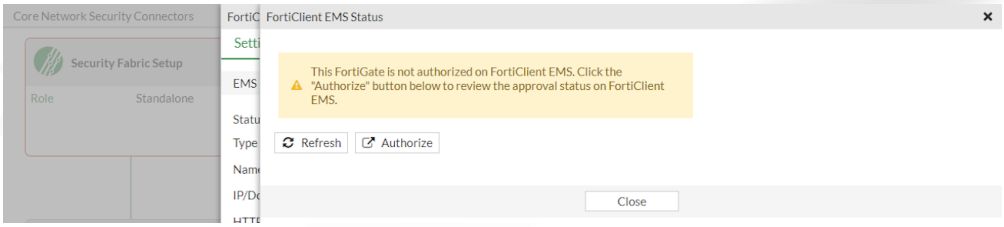
To configure the FortiGate EMS Fabric connector:

1. Go to *Security Fabric* > *Fabric Connectors*.
2. In the *Core Network Security Connectors* page, double-click *FortiClient EMS* to open the *FortiClient EMS Settings* pane.
3. Under *EMS 1*, enable the *Status*.
4. Configure the settings for your EMS server:

Name	Name
IP/Domain name	IP address or hostname of the EMS server
HTTPS port	443 (default)

EMS threat feed	Enable to receive malware hashes from EMS for use in the FortiGate AV
Synchronize firewall addresses	Must be enabled to pull Security Posture tags from EMS

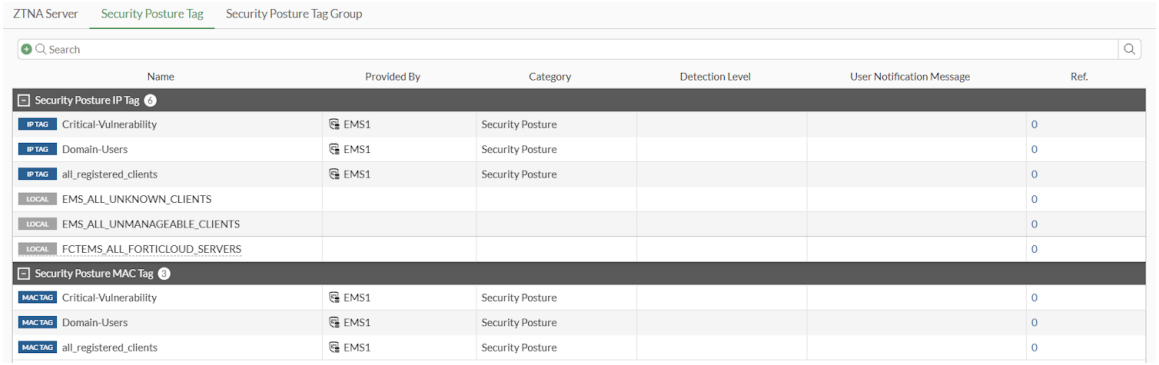
5. Click *OK*. A pane opens.
6. Verify the EMS server certificate, then click *Accept*. A second pane will appear.



7. Clicking on *Authorize* will open a window to launch the FortiClient EMS login page. You can authorize the FortiGate from there.
8. Alternatively, log in to EMS on another browser window to authorize.
9. Once logged in, a dialog is displayed requesting to authorize the FortiGate. Select *Authorize*.
10. Alternatively, navigate to *Administration* > *Fabric Devices* to authorize the FortiGate.

To verify Security Posture tags on the FortiGate:

1. Go to *Policy & Objects* > *ZTNA* and then navigate to the *Security Posture Tag* tab.
   Security Posture tags that were created in EMS are displayed on the page.



   The Security Posture tags do not have any matched endpoints yet. Once ZTNA policies are set up and a connection is made, the endpoints will be populated on their associated tags.

For more information about connecting the FortiGate to EMS, see Configuring FortiClient EMS.

Applying user authentication

By default, unauthenticated traffic is permitted to fall to the next matching policy. This means that unauthenticated users are only forced to authenticate against a policy when there are no other matching policies. However, to ensure strong access control, it is considered best practice to explicitly enable user authentication on all policies. In situations where an unauthenticated access policy is absolutely necessary, administrators can enforce authentication by setting `auth-on-demand` to `always`, which requires users to authenticate regardless of other matching policies. This approach, however, may disrupt passive methods like RSSO and FSSO, as FortiGate will no longer allow fallback to those policies.

The following deployment example uses an authentication scheme that utilizes the *Basic* method to authenticate the end users. It also assumes the use of a pre-defined LDAP server (*LDAP-fortiad*) for remote authentication as well as pre-configured LDAP user groups (*LDAP-Remote-Allowed-Group* and *LDAP-Finance*).

There are a variety of different supported methods of authentication by ZTNA such as SAML authentication or form authentication. They produce slightly different user experiences for the end-users. Furthermore, you can also choose to use different types of remote servers other than LDAP.

For more information, see the following topics:

- Authentication policy extensions
- ZTNA proxy access with SAML authentication example
- ZTNA access proxy with SAML and MFA using FortiAuthenticator example
- ZTNA session-based form authentication

To enforce firewall authentication on demand:

```
config user setting
    set auth-on-demand always
end
```

To configure an authentication scheme and authentication rule to apply basic authentication:

1. Go to *Policy & Objects* > *Authentication* and select *Authentication Schemes* from the top right.
2. Select *Authentication Rules* and click *Create New*.
   a. Configure the following:

Name	ZTNA-Auth-scheme
Method	Basic
User database	Other – *LDAP-fortiad*

   b. Click *OK*.
3. Click *Create New* > *Authentication Rules*.
   a. Configure the following:

Name	ZTNA-Auth-Rule
Source Address	all
Incoming Interface	WAN (port3)
Protocol	HTTP
Authentication Scheme	Enable – *ZTNA-Auth-Scheme*
IP-based Authentication	Enable
Enable This Rule	Enable

   b. Click *OK*.

Configure ZTNA application gateway on the FortiGate

We will create two ZTNA server objects to allow access to the Web Servers and the Finance Server. This is a design decision based on the following logic.

CONFIGURE ZTNA APPLICATION GATEWAY ON THE FORTIGATE

When each set of servers are accessible by a different set of users, we must create two sets of simple ZTNA policies to allow the proper user groups access to the server. Since simple ZTNA policies do not allow configuration of specific destinations, we must configure two ZTNA server objects to use in the two sets of ZTNA policies.

On the other hand, if you decide to create full ZTNA policies which allow you to specify a destination, you can create one ZTNA server object to map to the Web Servers and Finance Server. This method reduces the number of external ZTNA application gateway addresses you need.

To configure the HTTP access proxy server mapping for the Web servers in load-balancing mode:

1. On the FortiGate, go to *Policy & Objects* > *ZTNA*.
2. Click *Create New*.
3. Configure the following settings on the new ZTNA server:

Field	Value
Name	ZTNA-webserver
Connect On	
Interface	WAN (port3)
IP	10.0.3.10
Port	9043
Services and Servers	
Default certificate	ztna_wildcard

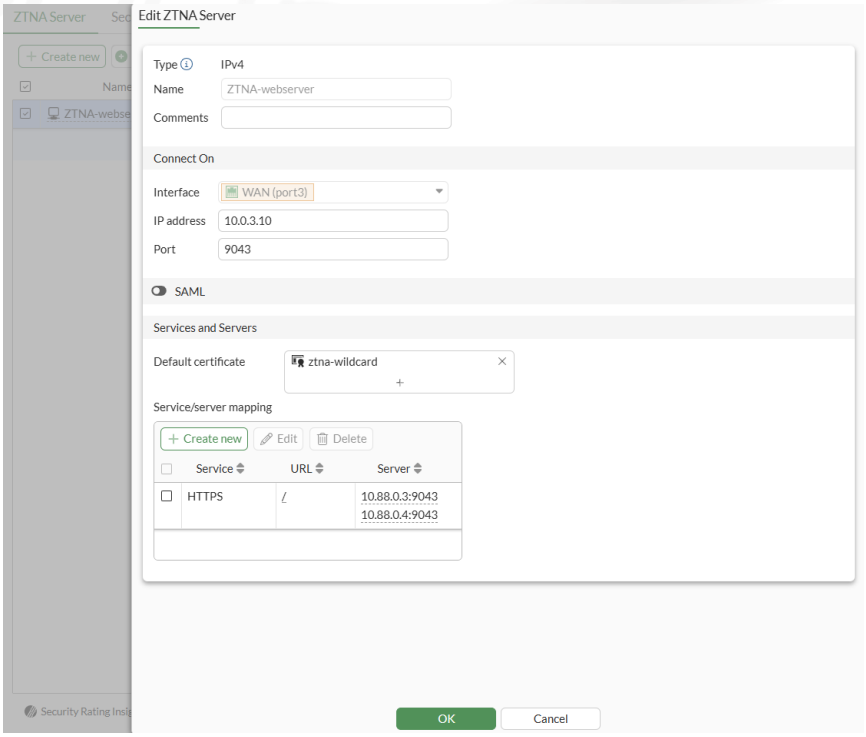
4. Under *Service/server mapping*, click *Create New*.
   a. Configure the following settings to map to the web servers:

Field	Value
Type	IPv4
Service	HTTPS
Virtual Host	Any Host
Match path by	Substring
Path	/
Server	
Address type	IP
IP address	10.88.0.3
Port	9043

5. Click *OK* to finish the ZTNA server setup.
6. Configure the following CLI settings to add server 2 and enable round robin load balancing:

```
config firewall access-proxy
    edit "ZTNA-webserver"
        config api-gateway
            edit 1
                config realservers
```

```
                edit 2
                    set ip 10.88.0.4
                    set port 9043
                next
            end
            set ldb-method round-robin
        next
    end
next
end
```



To configure the HTTP access proxy server mapping for the Finance server:

1. On the FortiGate, go to *Policy & Objects* > *ZTNA*.
2. Click *Create New*.
3. Configure the following settings on the new ZTNA server:

Field	Value
Name	ZTNA-financeserver
Connect On	
Interface	WAN (port3)
IP	10.0.3.11
Port	9043
Services and Servers	
Default certificate	ztna_wildcard

4. Under *Service/server mapping*, click *Create New*.

a. Configure the following settings to map to the web servers:

Field	Value
Type	IPv4
Service	HTTPS
Virtual Host	Any Host
Match path by	Substring
Path	/
Server	
Address type	Disable
IP address	10.88.0.5
Port	9043

b. Click *Create New* to create a new server mapping.

Field	Value
Type	IP
IP	10.88.0.5
Port	9043
Status	Active

c. Click *OK* to finish service/server mapping.

5. Click *OK* to finish the ZTNA server setup.

Configure ZTNA policies to control remote access

We will create one simple ZTNA policy to block access for devices with the *Critical-Vulnerability* tag, and two ZTNA policies to allow access for the respective user groups. The *Domain-Users* tag will be used in the allow policies to ensure connecting users are part of the domain.

To create a simple ZTNA policy to block devices:

1. Go to *Policy & Objects* > *Firewall Policy*.
2. Click *Create New*.

3. Create a policy to deny access to the ZTNA servers if the endpoint has critical vulnerabilities:

Field	Value
Name	ZTNA-vulnerable-deny
Type	ZTNA
Incoming Interface	WAN (port3)
Source	Address – *all*
User/group	User – *LDAP-Remote-Allowed-Group*, *LDAP-Finance*
Security Posture tag	Enable. (IP Tag) Critical-Vulnerability
ZTNA server	ZTNA-webserver ZTNA-financeserver
Schedule	always
Action	Deny
Log violation traffic	Enable
Enable this policy	Enable

4. Click *OK* to save.

To create a simple ZTNA policy to allow access to the Web servers:

1. Go to *Policy & Objects* > *Firewall Policy*.
2. Click *Create New*.
3. Create a policy to allow access to the *ZTNA-webserver* for users with the *Domain-Users* Security Posture tag:

Field	Value
Name	ZTNA-webserver-allow
Type	ZTNA
Incoming Interface	WAN (port3)
Source	Address – *all*
User/group	User – *LDAP-Remote-Allowed-Group*
Security Posture tag	Enable. (IP Tag) Domain-Users
ZTNA server	ZTNA-webserver
Schedule	always
Action	Accept
Logging Options	
Log allowed traffic	Enable. All Sessions
Enable this policy	Enable

4. Click *OK* to save.

To create a simple ZTNA policy to allow access to the Finance server:

1. Go to *Policy & Objects* > *Firewall Policy*.
2. Click *Create New*.
3. Create a policy to allow access to the *ZTNA-financeserver* for users with the *Domain-Users* Security Posture tag:

Field	Value
Name	ZTNA-finance-allow
Type	ZTNA
Incoming Interface	WAN (port3)
Source	Address – *all*
User/group	User – *LDAP-Finance*
Security Posture tag	Enable. (IP Tag) Domain-Users
ZTNA server	ZTNA-financeserver
Schedule	always
Action	Accept
Logging Options	
Log allowed traffic	Enable. All Sessions
Enable this policy	Enable

4. Click *OK* to save.

Verify ZTNA access to the web applications

Now that the ZTNA server objects and policies are configured, it is time to access the web applications. Remember to update external DNS servers to map the FQDN of the web applications to the ZTNA application gateway addresses.

In our example, the following DNS mappings are assumed to be created:

- *webserver.ztnademo.com* > 10.0.3.10
- *finance.ztnademo.com* > 10.0.3.11

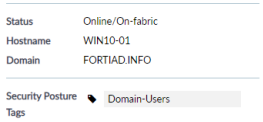
In a real network, the ZTNA application gateway addresses should be public IP addresses.

To verify ZTNA access without any critical vulnerabilities:

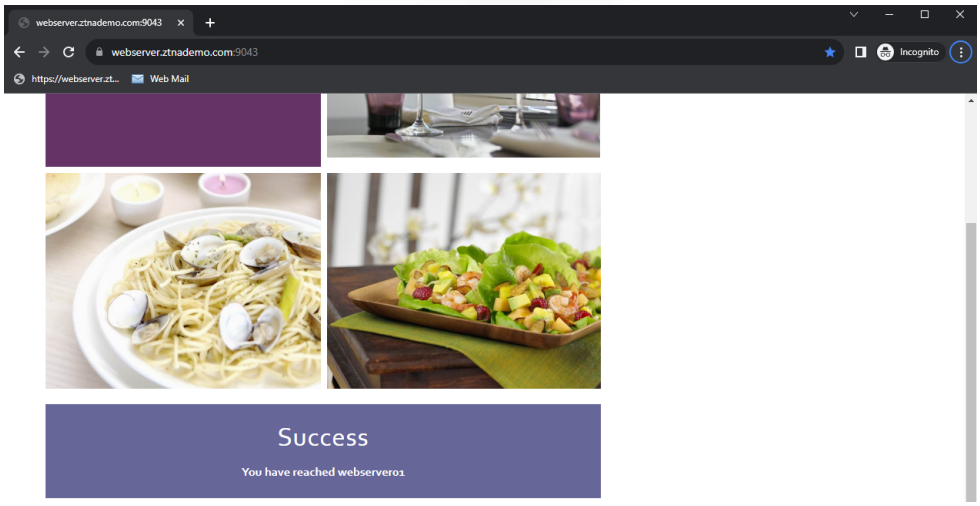
In this scenario, we will demonstrate accessing the web applications using a user that belongs to the *Remote-Allowed* group only. Access to the Web server will be allowed, and access to the Finance server will be denied.

1. From a remote endpoint, open FortiClient.
2. In the *Zero Trust Telemetry* page, enter *ems.ztnademo.com* as the server address.
3. Click *Connect*. Once connected, a notification appears indicating settings have been pushed from EMS.

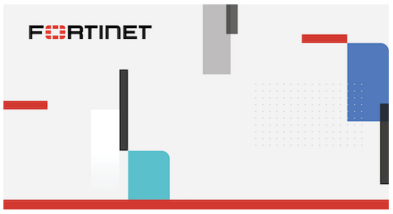
4. Shortly after, click on the avatar to view information about the device. Note that *Zero Trust Tags* displays that *Domain-Users* is added.



5. Open a browser.
6. Go to https://webserver.ztnademo.com:9043 to test access to Web server.
7. When prompted, select the client certificate issued by EMS and then click *OK*.
8. Next, you will be prompted for a username and password. Enter the credentials for the user.
   The webpage will load.



9. Go to https://finance.ztnademo.com:9043 to test access to the Finance server.
10. When prompted, select the client certificate issued by EMS and then click *OK*.
    This time, access will be denied for this user who is not part of the Finance user group.



ZTNA Policy Denied

Error Code:	069
Error Message:	The page you requested has been blocked because authorization failed.
User Name:	tsmith
Certificate Information:	Serial number: 56C041CDD6FCDF502E69E7DEF03000199A073E83
Device Information:	Endpoint device ID: 9A016B5A6E914B42AD4168C066EB04CA
Request Time:	1746124345; 2025-05-01 11:32:25 PDT

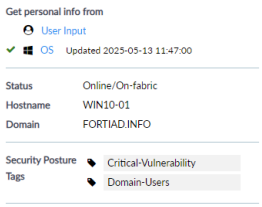
11. After the session is closed, go to the FortiGate and open *Log & Report > ZTNA Traffic*. Verify that a log was recorded for the allowed traffic and the denied traffic. The username *tsmith* is logged for both allowed and denied traffic.
12. Alternatively, use the CLI to display the ZTNA logs:

```
# execute log filter category 0
# execute log filter field subtype ztna
# execute log display
```

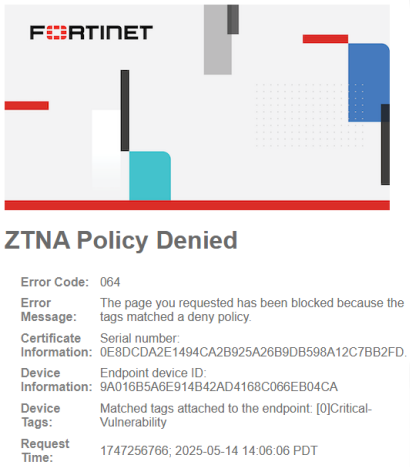
```
1: date=2025-05-01 time=16:40:36 eventtime=1695944436285310005 tz="-0700"
logid="0005000024" type="traffic" subtype="ztna" level="notice" vd="root"
srcip=10.0.3.2 srcport=33390 srcintf="port3" srcintfrole="wan" dstcountry="Reserved"
srccountry="Reserved" dstip=10.88.0.3 dstport=9043 dstintf="port2" dstintfrole="dmz"
sessionid=20961 srcuuid="b458a65a-f759-51ea-d7df-ef2e750026d1" dstuuid="62a8fb8a-5e52-
51ee-2e82-07f37c248ba1" service="tcp/9043" proxyapptype="ztna-proxy" proto=6
action="accept" policyid=18 policytype="policy" poluuid="4fe3f548-5e54-51ee-80de-
0b5b837eeebb" policyname="ZTNA-webserver-allow" appcat="unscanned" duration=365
user="tsmith" group="LDAP-Remote-Allowed-Group" authserver="LDAP-fortiad" gatewayid=1
realserverid=1 vip="ZTNA-webserver" vipincomingip=10.0.3.10 accessproxy="ZTNA-
webserver" clientdeviceid="9A016B5A6E914B42AD4168C066EB04CA"
clientdevicemanageable="manageable" clientdeviceems="FCTEMS8824006771"
clientdevicetags="Domain-Users/all_registered_clients" clientcert="yes"
emsconnection="online" wanin=305188 rcvdbyte=305188 wanout=4807 lanin=2975
sentbyte=2975 lanout=334408 fctuid="9A016B5A6E914B42AD4168C066EB04CA"

2: date=2025-05-01 time=16:35:52 eventtime=1695944152774403157 tz="-0700"
logid="0005000024" type="traffic" subtype="ztna" level="notice" vd="root"
srcip=10.0.3.2 srcport=33409 srcintf="port3" srcintfrole="wan" dstcountry="Reserved"
srccountry="Reserved" dstip=10.0.3.11 dstport=9043 dstintf="root"
dstintfrole="undefined" sessionid=20979 srcuuid="b458a65a-f759-51ea-d7df-ef2e750026d1"
service="tcp/9043" proxyapptype="ztna-proxy" proto=6 action="deny" policyid=0
policytype="policy" appcat="unscanned" duration=0 user="tsmith" authserver="LDAP-
fortiad" vip="ZTNA-financeserver" vipincomingip=10.0.3.11 accessproxy="ZTNA-
financeserver" clientdeviceid="9A016B5A6E914B42AD4168C066EB04CA"
clientdevicemanageable="manageable" clientdeviceems="FCTEMS8824006771"
clientdevicetags="Domain-Users/all_registered_clients" clientcert="yes"
emsconnection="online" msg="Traffic denied because failed to match a policy or proxy-
policy" wanin=0 rcvdbyte=0 wanout=0 lanin=2565 sentbyte=2565 lanout=33266
fctuid="9A016B5A6E914B42AD4168C066EB04CA" crscore=30 craction=131072 crlevel="high"
```


Verifying ZTNA access for endpoints with critical vulnerabilities

On a device that has a critical vulnerability detected, FortiClient will tag the device with the *Critical-Vulnerability* tag.



When accessing a protected web server, traffic will be blocked due to security posture check.

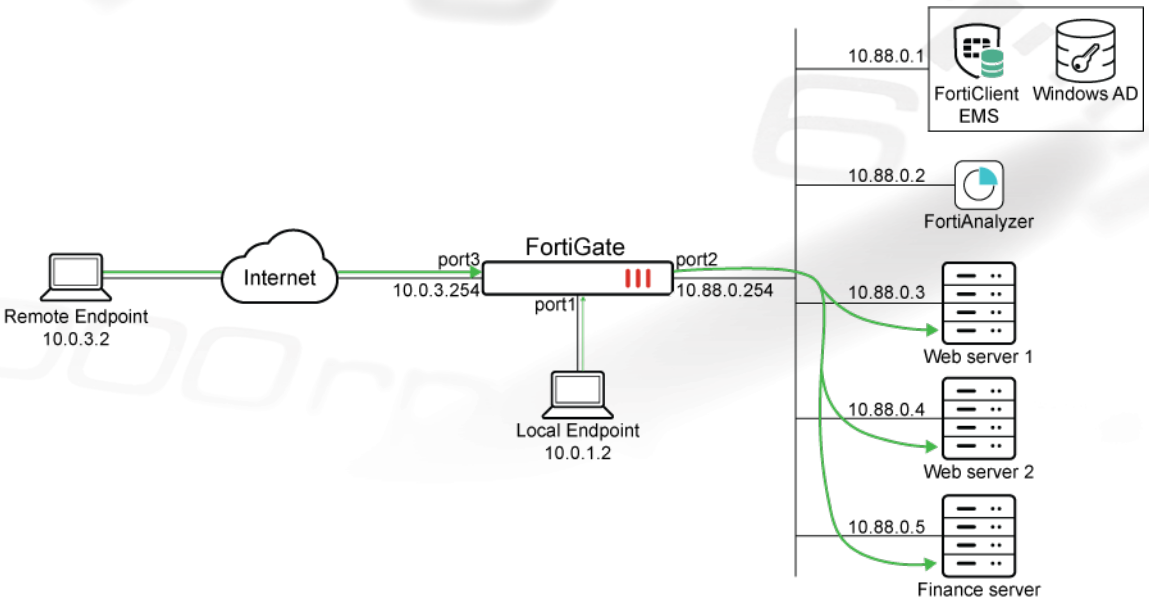


From the ZTNA traffic logs, we can see the denied traffic hitting the *ZTNA-vulnerable-deny* policy, and the user who tried to access it.

```
# execute log filter category 0
# execute log filter field subtype ztna
# execute log display

1: date=2025-05-01 time=16:32:45 eventtime=1696375965762959263 tz="-0700"
logid="0005000024" type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.0.3.2
srcport=5623 srcintf="port3" srcintfrole="wan" dstcountry="Reserved" srccountry="Reserved"
dstip=10.0.3.10 dstport=9043 dstintf="root" dstintfrole="undefined" sessionid=99053
srcuuid="b458a65a-f759-51ea-d7df-ef2e750026d1" dstuuid="62a8fb8a-5e52-51ee-2e82-
07f37c248ba1" service="tcp/9043" proxyapptype="ztna-proxy " proto=6 action="deny"
policyid=17 policytype="policy" poluuid="a21b3020-5e53-51ee-c587-b7d8384ed100"
policyname="ZTNA-vulnerable-deny" appcat="unscanned" duration=6 user="tsmith" group="LDAP-
Remote-Allowed-Group" authserver="LDAP-fortiad" vip="ZTNA-webserver"
vipincomingip=10.0.3.10 accessproxy="ZTNA-webserver"
clientdeviceid="9A016B5A6E914B42AD4168C066EB04CA" clientdevicemanageable="manageable"
clientdeviceems="FCTEMS8824006771" clientdevicetags="Critical-Vulnerability/all_registered_
clients/Domain-Users" clientcert="yes" emsconnection="online" msg="Traffic denied because
proxy-policy action is deny. Matched tag: EMS1_ZTNA_Critical-Vulnerability" wanin=0
rcvdbyte=0 wanout=0 lanin=2680 sentbyte=2680 lanout=62887
fctuid="9A016B5A6E914B42AD4168C066EB04CA" crscore=30 craction=131072 crlevel="high"
```

Configure firewall policies with IP/MAC based access control for internet access

The user permissions to access internal resources from remote and from within the corporate network should remain the same. However, the path in which the traffic takes will be different.



When we examine our topology, remote endpoints access the web application through a ZTNA application gateway on port3. However, for local endpoints, accessing the ZTNA application from port1 to port3, and then accessing the web application through port2 is inefficient and unnecessary.

Therefore, in this section we will demonstrate configuring IP/MAC based access control to provide the same user permissions for local endpoints accessing web applications directly from port1 to port2.

To configure a firewall policy to block devices with Critical Vulnerabilities:

1. Go to *Policy & Objects* > *Firewall Policy*.
2. Click *Create New*.
3. Configure the following deny policy:

a. Create a policy to deny access to the web servers if the endpoint has *Critical-Vulnerabilites*:

Field	Value
Name	Local-Deny-Access-Critical-Vuln
Type	Standard
Incoming Interface	port1
Outgoing Interface	port2
Source	Address – *all* User – *LDAP-Remote-Allowed-Group*, *LDAP-Finance*
Security posture tag	Enabled. (IP Tag) Critical-Vulnerability
Destination	Webserver1 (Address object for 10.88.0.3) Webserver2 (Address object for 10.88.0.4) Finance (Address object for 10.88.0.5)
Schedule	always
Service	ALL
Action	Deny
Log violation traffic	Enable
Enable this policy	Enable

b. Click *OK* to save.

To configure firewall policies to allow access for devices that pass ZTNA security posture check:

1. Go to *Policy & Objects* > *Firewall Policy*.
2. Click *Create New*.
3. Configure the following allow policies:
   a. Create a policy to allow access to the web servers for users belonging to the *LDAP-Remote-Allowed* group and has the *Domain-Users* Security Posture tag:

Field	Value
Name	Local-Allowed-Webservers
Type	Standard
Incoming Interface	port1
Outgoing Interface	port2
Source	Address – *all* User – *LDAP-Remote-Allowed-Group*
Security posture tag	Enable. (IP Tag) Domain-Users
Destination	Webserver1 Webserver2
Schedule	always

Field	Value
Service	ALL
Action	Accept
NAT	Disable
Logging Options	
Log allowed traffic	All Sessions
Enable this policy	Enable

b. Click *OK* to save.

c. Create a policy to allow access to the Finance servers for users belonging to the *LDAP-Finance* group and has the *Domain-Users* Security Posture tag:

Field	Value
Name	Local-Allowed-Finance
Type	Standard
Incoming Interface	port1
Outgoing Interface	port2
Source	Address – *all* User – *LDAP-Finance*
Security posture tage	Enable. (IP Tag) Domain-Users
Destination	Finance
Schedule	always
Service	ALL
Action	Accept
NAT	Disable
Logging Options	
Log allowed traffic	All Sessions
Enable this policy	Enable

d. Click *OK* to save.

Verify ZTNA access to the web applications

Accessing the web applications internally using the same FQDN addresses means that the DNS mappings are configured to point to the actual IP of the servers.

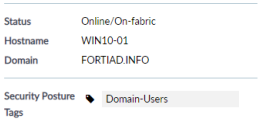
In our example, the following DNS mappings are assumed to be created in an internal DNS server:

- *webserver.ztnademo.com* > 10.88.0.3
- *finance.ztnademo.com* > 10.88.0.5

To verify accessing the Finance server from internal:

In this scenario, we will demonstrate accessing the web applications using a user that belongs to both the *Remote-Allowed* group and the *Finance* group. Access to the Web server and access to the Finance server will be allowed.

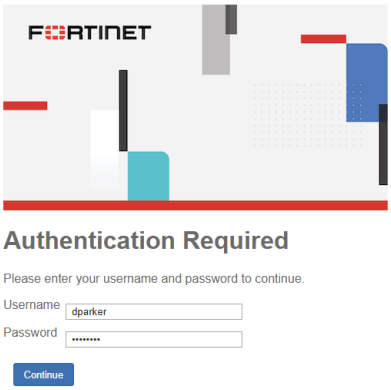
1. From a local endpoint, open FortiClient.
2. In the *Zero Trust Telemetry* page, enter *ems.ztnademo.com* as the server address.
3. Click *Connect*. Once connected, a notification appears indicating settings have been pushed from EMS.
4. Shortly after, click on the avatar to view information about the device. Note that *Zero Trust Tags* displays that *Domain-Users* is added.



5. Open a browser.
6. Go to https://webserver.ztnademo.com:9043 to test access to Web server.

In this example, the port used is 9043 so users must take an extra step to trigger authentication over port 443 first.

7. Next, you will be prompted for a username and password. Enter the credentials for the user.



The Web server webpage will load.

8. Go to https://finance.ztnademo.com:9043 to test access to the Finance server. The Finance server webpage will load.
9. After the session is closed, go to the FortiGate and open *Log & Report > Forward Traffic*. Verify that a log was recorded for the allowed traffic. The username *dparker* is logged for both allowed and denied traffic.
10. Alternatively, use the CLI to display the Forward logs:

```
# execute log filter category 0
# execute log filter field subtype forward
# execute log filter field srcip 10.0.1.2
# execute log display

...
2: date=2025-05-01 time=15:49:30 eventtime=1696373370478461357 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.0.1.2 srcport=28145 srcintf="port1" srcintfrole="undefined" dstip=10.88.0.5
```

dstport=9043 dstintf="port2" dstintfrole="dmz" srcuuid="b458a65a-f759-51ea-d7df-ef2e750026d1" dstuuid="6b38e638-0775-51ec-1333-bc27ff2d5b8d" emstag="EMS1_ZTNA_Domain-Users" srccountry="Reserved" dstcountry="Reserved" sessionid=98046 proto=6 action="close" policyid=22 policytype="policy" poluuid="7693847e-623c-51ee-2021-a105aa9c6c1a" policyname="Local-Allowed-Finance" user="dparker" group="LDAP-Finance" authserver="LDAP-fortiad" service="tcp/9043" trandisp="noop" appcat="unscanned" duration=113 sentbyte=3535 rcvdbyte=33360 sentpkt=32 rcvdpkt=43 fctuid="9A016B5A6E914B42AD4168C066EB04CA" unauthuser="tsmith" unauthusersource="forticlient" srcdomain="fortiad.info" srcremote=69.167.105.212 mastersrcmac="02:09:0f:00:01:02" srcmac="02:09:0f:00:01:02" srcserver=0

…

4: date=2025-05-01 time=15:49:12 eventtime=1696373352638475272 tz="-0700" logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" srcip=10.0.1.2 srcport=28117 srcintf="port1" srcintfrole="undefined" dstip=10.88.0.3 dstport=9043 dstintf="port2" dstintfrole="dmz" srcuuid="b458a65a-f759-51ea-d7df-ef2e750026d1" dstuuid="3a951b32-0775-51ec-59c8-7a5207859839" emstag="EMS1_ZTNA_Domain-Users" srccountry="Reserved" dstcountry="Reserved" sessionid=98033 proto=6 action="server-rst" policyid=21 policytype="policy" poluuid="11e5fd9a-623c-51ee-a638-b8d26f632985" policyname="Local-Allowed-Webservers" user="dparker" group="LDAP-Remote-Allowed-Group" authserver="LDAP-fortiad" service="tcp/9043" trandisp="noop" duration=150 sentbyte=2802 rcvdbyte=312041 sentpkt=29 rcvdpkt=226 appcat="unscanned" sentdelta=0 rcvddelta=40 fctuid="9A016B5A6E914B42AD4168C066EB04CA" unauthuser="tsmith" unauthusersource="forticlient" srcdomain="fortiad.info" srcremote=69.167.105.212 mastersrcmac="02:09:0f:00:01:02" srcmac="02:09:0f:00:01:02" srcserver=0

More information

This section includes:

Appendix A: Products used in this guide

The following product models and firmware were used in this guide:

Product	Model	Firmware
FortiClient EMS		v7.4.3
FortiClient		v7.4.3
FortiOS		v7.6.3

Appendix B: Documentation references

Feature documentation

- FortiOS Admin Guide > ZTNA chapter
- ZTNA Reference Guide > Endpoint Posture Check
- FortiClient Admin Guide > Zero Trust Tags

Best practices

- Zero Trust Network Access solution hub
- Zero Trust Network Access 4-D resources
  - ZTNA Concept Guide
  - ZTNA Architecture Guide

www.fortinet.com

01-763-1154682-20250527