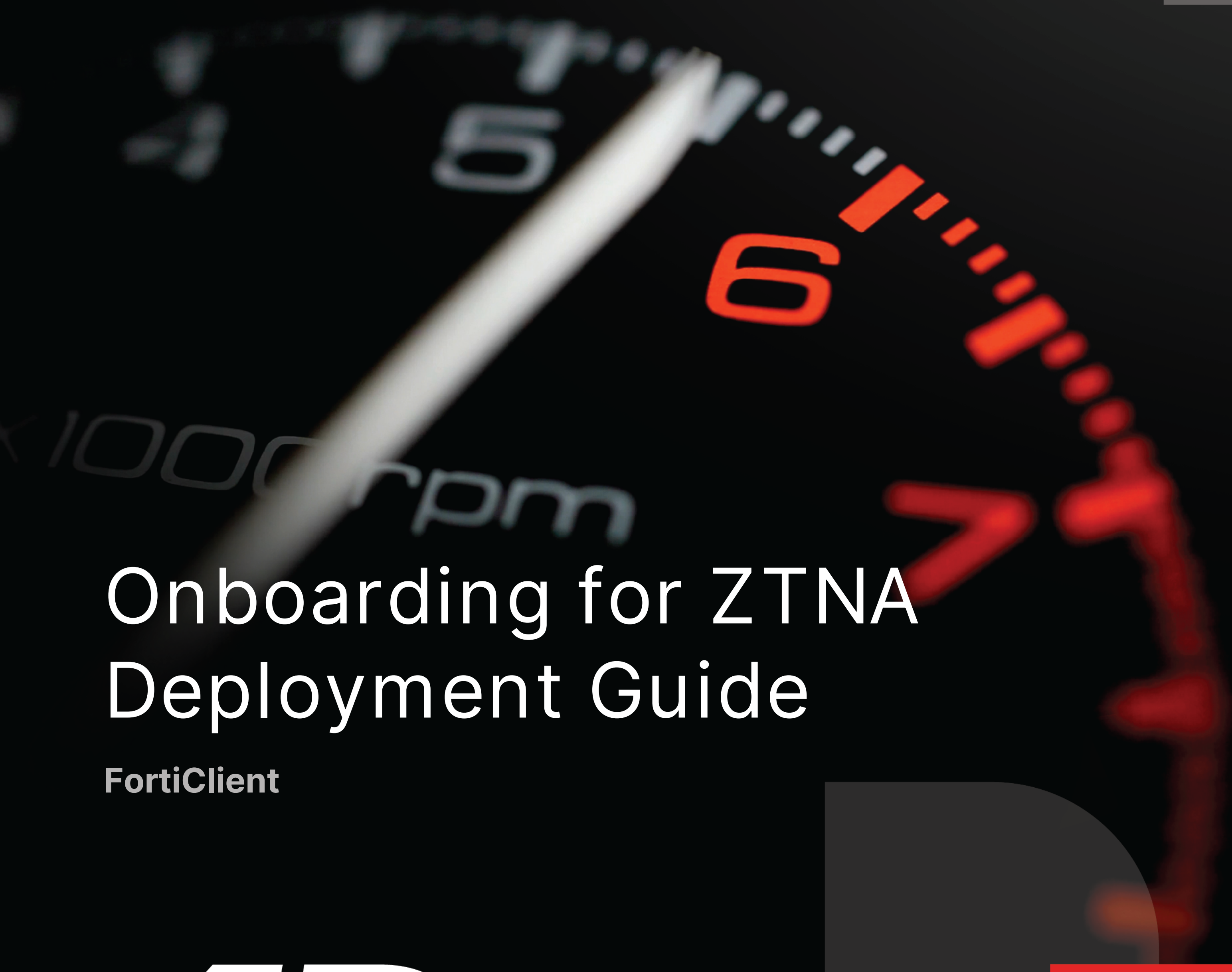


Onboarding for ZTNA Deployment Guide

FortiClient

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

Change log

Date	Change description
2024-06-03	Initial release.

Deployment overview

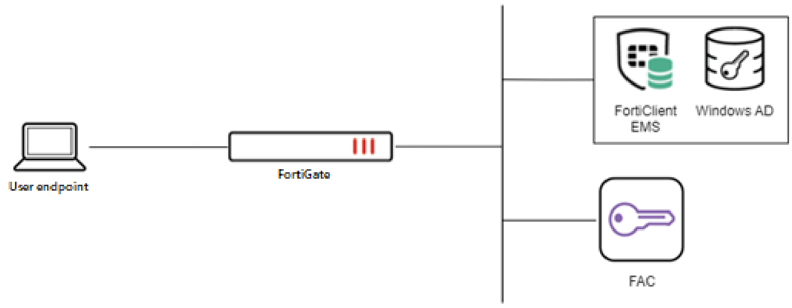
This document provides examples of how an administrator can require users to provide credentials to securely connect and register to EMS as part of enabling zero trust network access. Without requiring user authentication or an invite code, nothing prevents an unauthorized user from registering to your EMS, receiving your configurations, and possibly compromising your security. This deployment guide shows the best practices to securely onboard users to EMS using an invitation code as well as user authentication.

This document includes the following examples:

- Local authentication
- Active Directory (AD) LDAP authentication
- SAML authentication

This document only provides configuration to leverage the aforementioned options for EMS and FortiClient. If you are using LDAP or SAML authentication, it is expected you have existing configuration in your environment for the related systems, such as AD and identity provider.

A simple topology is used to explain the process for each option:



Intended audience

This guide is aimed at administrators who have working knowledge of the option they will implement, such as LDAP or SAML, and want the EMS and FortiClient configuration required to complete the onboarding. Administrators also need familiarity with generating certificates to secure the connection between FortiClient and EMS.

About this guide

For greater security and use with user-based licensing, configuring user onboarding with verification is recommended. By enforcing user verification during the onboarding process, 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 deployment options that this guide discusses are one implementation of each option. There are some features which are not used, and you may need to adapt some steps to suit your environment. It is recommended that readers also review supplementary material found in product administration guides, example guides, cookbooks, release notes, and other documents where appropriate on the Fortinet Document Library.

Design considerations

Authentication

Authentication methods are the main content of this guide. Each has benefits and drawbacks all while accomplishing the same task: adding users to EMS. The method you choose should be the one which best integrates with your current environment. For example, if you do not have any previously existing SAML infrastructure, such as an identity provider (IdP), you should consider another method.

Invite distribution

This guide also leverages an SMTP server to send invites to users. It does not cover the SMTP server setup, only the related settings in EMS. The guide shows the invite being sent to one address. To send an invite to multiple addresses, you may enter them manually or leverage a distribution list to send it to a group of users. You may also elect to distribute the invites through some other means of your choosing.

FortiClient installation

This guide does not cover FortiClient installation. This guide assumes FortiClient to be already installed on the end users' devices. If you require the client to be installed, the invite that EMS created contains a link to download the installer. This requires install privileges that the end user may not have and should be taken into account. See Initially deploying FortiClient software to endpoints for more options.

For information on deploying FortiClient to a large number of endpoints at once, please review the FortiClient EMS Administration Guide or one of the standalone deployment guides for Intune, Jamf, or Workspace ONE.

Success criteria

Once complete, EMS is populated with user identities so that when a user attempts to register, they must verify themselves to EMS. Once confirmed, the EMS administrator may continue to implement zero trust network access (ZTNA) by configuring the application gateway, policies, and even IP/MAC-based access control for Internet access. For details on ZTNA deployment, see the ZTNA Deployment Guide.

Product requirements

This deployment requires the following product versions:

Product	Version
FortiClient	7.2.0 and later
EMS	
FortiAuthenticator	6.4.6
Windows Server	2016
Windows PC	Windows 10

Deployment procedures

The following provides an overview of the procedure:

Preparing EMS

This section covers the required configuration that each onboarding method uses. This includes:

Configuring an SMTP server for invite distribution

You may skip this step if you intend to distribute the invites through some other method, such as copying the invite and emailing through a different system.

To configure an SMTP server for invite distribution:

1. Go to *System Settings > SMTP Server*.
2. In the *Server* field, enter your server IP address or FQDN.
3. Configure *Security* if applicable.
4. Specify the *From* and *Reply-to* email addresses.

Selecting a registration address

The registration address, or *Listen* address, is the address that FortiClient endpoints use when attempting to register to the EMS. Keep in mind the reachability of this address with regards to the location of the invited users. If users connect to EMS from outside your organization, you must plan to have this address publicly reachable.

To configure your Listen address in EMS:

1. Go to *System Settings > EMS Settings*.
2. Use the *Listen on IP* dropdown list to select the IP address to listen on.
3. You may also use the *Use FQDN* checkbox to allow FortiClient endpoints to connect using the IP address in the *Listen on IP* field or the specified FQDN.

For details on listen on IP and using an FQDN, see Configuring EMS settings.

Installing a certificate to secure communication between FortiClient and EMS

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

To upload a server certificate issued by your desired public or private CA:

1. Go to *System Settings > EMS Server Certificates*.
2. Select *Add* in the top right to upload a certificate to EMS.
3. For *Type*, select *Upload PKCS12* or *Upload PEM*.
4. Upload the certificate and enter the certificate password or private key.
5. Click *Upload*.
6. Go to *System Settings > EMS Settings*.
7. From the *Endpoint Control certificate* dropdown list, select the certificate that you added.
8. Save.

Enforcing user verification

You must enable this option in *EMS Settings* to require users to authenticate.

To enforce user verification:

1. Go to *System Settings > EMS Settings*.
2. Enable *Enforce User Verification*.
3. A warning appears. The following sections outline the steps that the warning outlines. Click *Yes*.
4. Click *Save*.

Creating a ZTNA tag

Zero trust network access (ZTNA) is an access control method that uses client device identification, authentication, and Zero Trust tags to provide role-based application access. It gives administrators the flexibility to manage network access for on-net local users and off-net remote users.

The following creates a simple ZTNA tag which EMS applies to endpoints after they successfully authenticate with EMS.

To create a ZTNA tag:

1. In EMS, go to *Zero Trust Tags > Zero Trust Tagging Rules*, and select *Add* in the top right.
2. Create a tagging rule set as follows:
   a. In the *Name* field, enter Verified.
   b. In the *Tag Endpoint As* field, enter Verified in the text box and press `Enter` to create the tag.
   c. In the *Rules* section, select *Add Rule* in the top right. Configure the following:
      i. For *OS*, select *Windows*.
      ii. From the *Rule Type* dropdown list, select *User Identity*.
      iii. For *User Identity*, select *Verified User*.
   d. Save.
3. Save the rule set.

Configuring EMS for each onboarding option

Select one of the following for user onboarding:

- Local users on page 10
- LDAP/AD authentication on page 11
- SAML authentication using LDAP domain user account on page 12

Local users

You can configure local users. Users can provide credentials that match a configured local user to connect their FortiClient to FortiClient EMS. This is mainly useful for environments that do not use Active Directory or SAML.

To add a local user:

1. Go to *User Management > Local Users*.
2. Click *Add*.
3. In the *Username* field, enter the desired username.
4. In the *Password* and *Confirm Password* fields, enter a password that conforms to the displayed password rules.
5. (Optional) In the *Comments* field, enter any desired notes.
6. Click *Save*.

LDAP/AD authentication

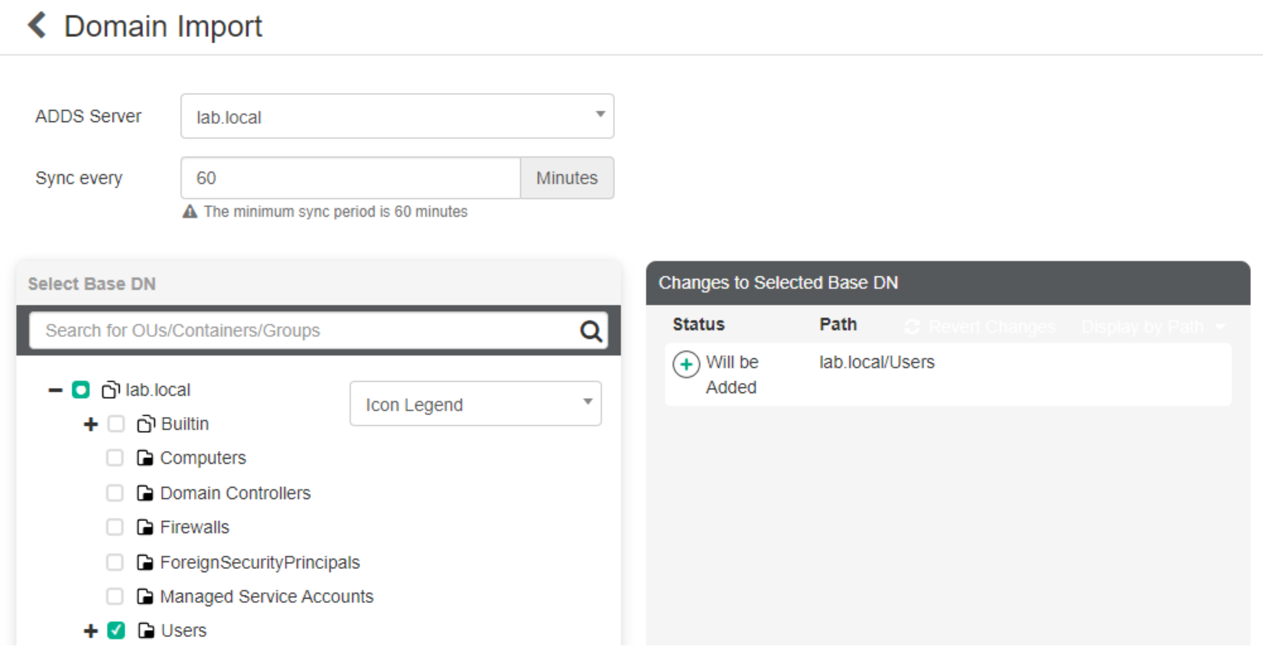
The following provides an example of configuring user verification when using an Active Directory (AD) server for authentication:

To add the LDAP/AD server to EMS:

1. Go to *Administration > Authentication Servers*.
2. Click *Add > ADDS*.
3. In the *IP address/Hostname* field, enter the server IP address.
4. In the *Username* and *Password* fields, provide the credentials required to access the LDAP server.
5. Enable LDAPS connection and upload a certificate authority certificate or server certificate file in PEM or DER format.
6. If needed, configure other fields.
7. Click *Test*.
8. After the test succeeds, click *Save*. After a few minutes, EMS imports devices from the LDAP server.

To add users to EMS:

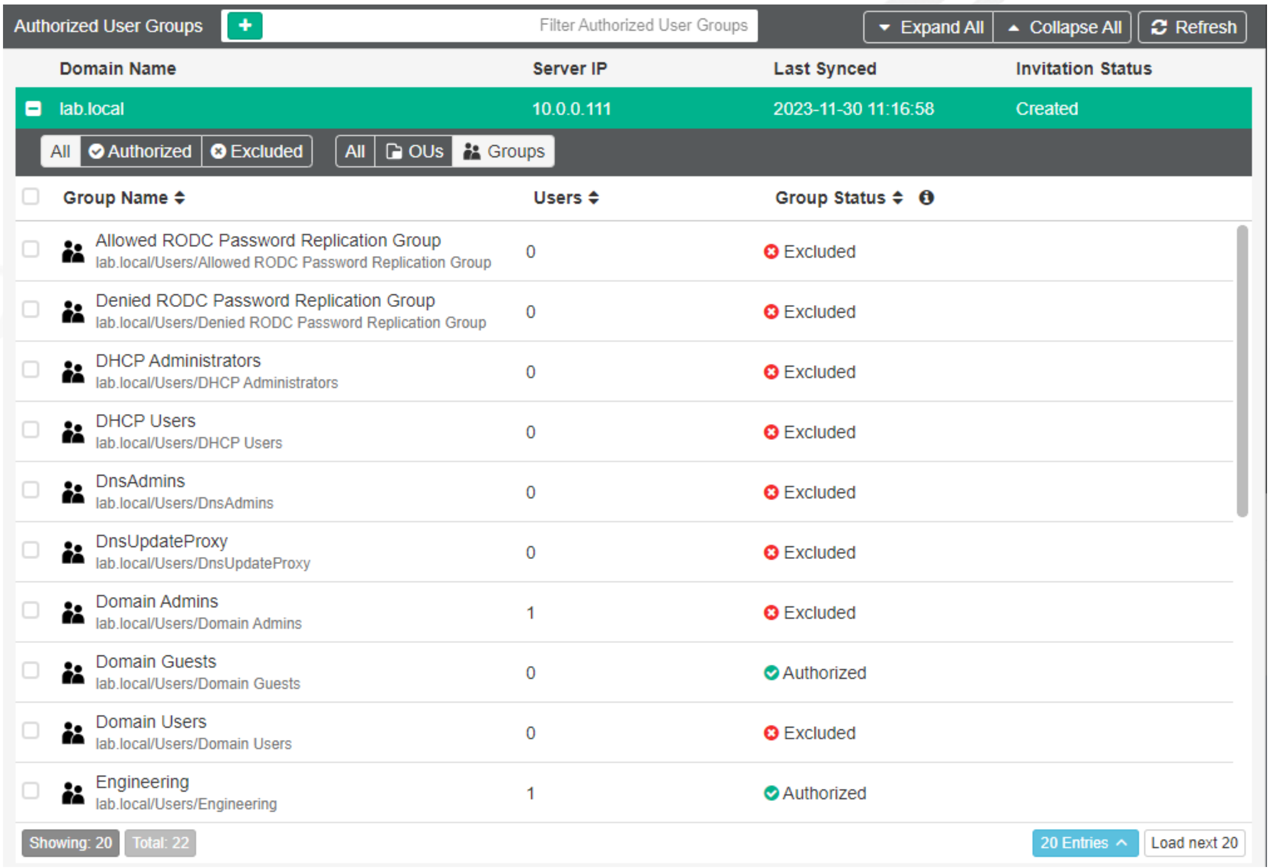
1. Go to *Endpoints > Manage Domains*, then click *Add* in the top right to select *ADDS*.
2. Select the server that you defined in the previous step.
3. Adjust the sync if desired.
4. Use the checkbox to select the organizational units/containers/groups to import to EMS. The next section allows you to select which users from within these groups to invite.



To specify which user groups to onboard:

1. Go to *User Management > Authorized User Groups*.
2. Click the + next to your domain to expand the domain.
3. Use the checkbox next to the group names to select the user groups that you do not want to onboard.
4. Select *Exclude* in the top right to remove these groups from user onboarding.

5. Select *Yes* in the popup.



SAML authentication using LDAP domain user account

SAML authentication allows for an identity provider (IdP) to authenticate identities, while end users make authentication requests to a service provider (SP). The IdP can be a cloud provider like Microsoft Entra ID, Okta, or FortiTrust Identity; or an on-premise authentication server such as a FortiAuthenticator. Furthermore, you may store the underlying user identities within an Active Directory (AD).

In the following configuration example:

- User identities and credentials are stored on an AD
- FortiClient EMS acts as the SP (the device the endpoints want to register to) which forwards the authentication requests to the IdP
- FortiAuthenticator acts as the IdP to authenticate end user’s authentication requests against the AD
- FortiClient EMS also acts as the SP in which it authorizes the users within a specific domain

To use SAML authentication:

1. Import the desired AD domain by following the steps in LDAP/AD authentication on page 11.
2. Go to *User Management > SAML Configuration* and click *Add*.
3. For *Authorization Type*, select *LDAP*.
4. From the *Domain* dropdown list, select the imported domain from the step 1.

5. Configure the following *Service Provider Settings*:

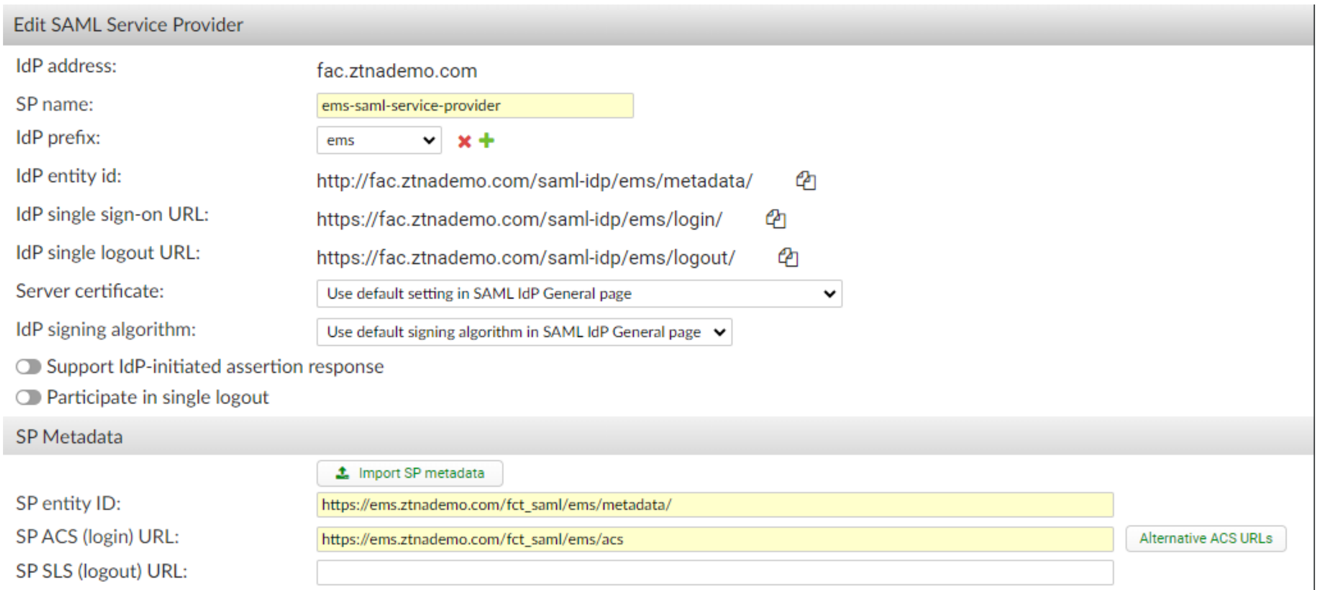
Setting	Description
SP Address	Specify a URL, or select *Use Current URL*.
Prefix	Specify a prefix, such as ems.

6. Note the *SP Entity ID* and *SP ACS (login) URL*. You must provide them to the IdP.
7. Under *Identity Provider Settings*, enter your FortiAuthenticator details as follows:

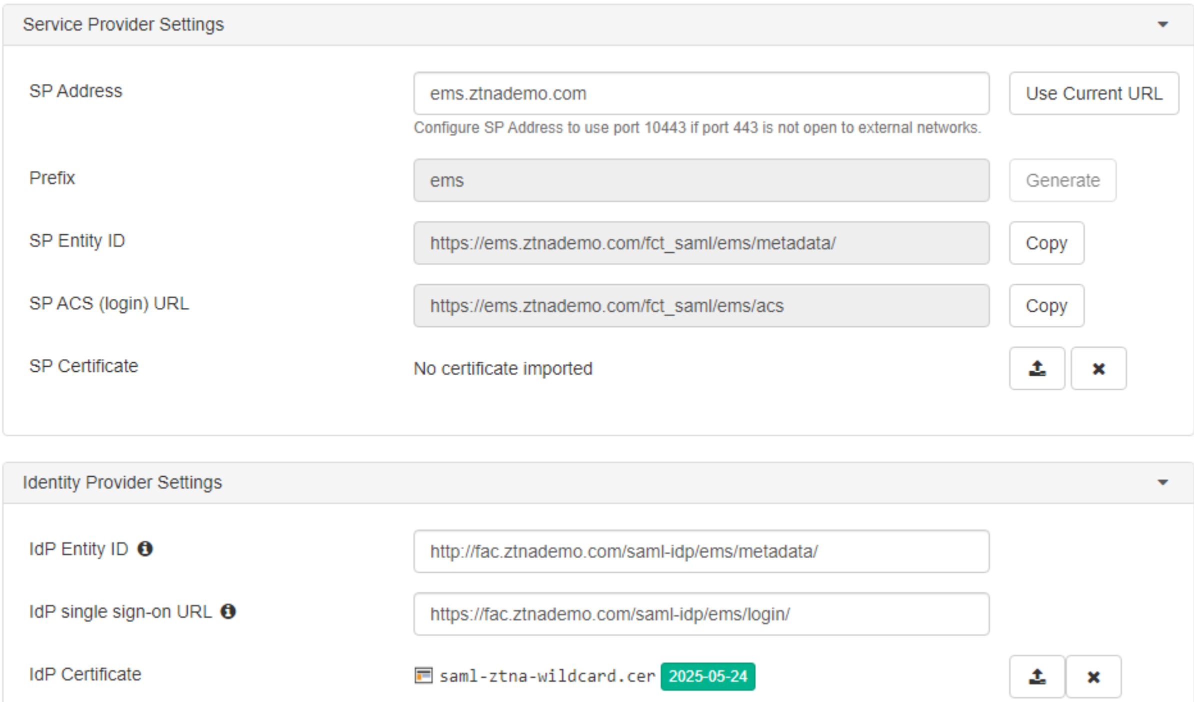
Setting	Description
IdP single sign-on URL	• Provided by the IdP • Ends with /login/
IdP Entity ID	• Provided by the IdP • Ends with /metadata/
IdP Certificate	Upload the same certificate that you configured in the IdP.

8. Configure your IdP with the EMS SP settings configured in step 5 and saved in step 6.
9. Click *Test*. A checkmark appears next to the IdP certificate when the test succeeds. Save.

FortiAuthenticator SAML configuration



EMS SAML configuration



Inviting and onboarding users and verifying user registration

Inviting users to join EMS

The following creates an invitation for users to join EMS. You can send this invitation to anyone, but only those who you added in Configuring EMS for each onboarding option on page 10 can authenticate. This step covers how to create the invite and provides a distribution method.

To create an invitation:

1. Go to *User Management > Invitations*.
2. Click *Add*.
3. Configure the invitation:
    a. From the *EMS Listen Address* dropdown list, select the desired address.
    b. To send the code to a single recipient, select *Individual*. Otherwise, select *Bulk*.
    c. Enable *Send Email Notifications*. You can only enable this option if you have configured SMTP settings.
    d. In the *Include FortiClient Installer* field, click the + icon to create a new installer to add a deployment package to the invitation. The invitation email includes a link that the user can download the configured deployment package from. For details on installers, see FortiClient Installer.
    e. In the *Email Recipients* field, enter the desired end user email addresses.
    f. If desired, enable *Send SMS notifications*.
    g. If desired, enable *Expiring*.
    h. In the *Expiry date* field, set the expiry date.

i. Select the *Verification Type* which matches the authentication type you configured in Configuring EMS for each onboarding option on page 10.

4. Save.

Deploying FortiClient

Before the endpoint can connect to EMS, you must install FortiClient. You can find the installer on the Fortinet downloads page, however you may also create a custom installer through EMS which enables you to pre-configure some FortiClient settings such as the EMS profile, VPN tunnels, ZTNA tags and destinations, and EMS registration address/FQDN. Users can download custom installers created using EMS directly, or administrators may elect to download the installer and distribute them through another method, such as a shared drive. Regardless of where the installer comes from, installing FortiClient requires administrative privileges. If end users do not have this permission, you will need to leverage additional software such as SCCM or Group Policy.

Downloading custom FortiClient from EMS

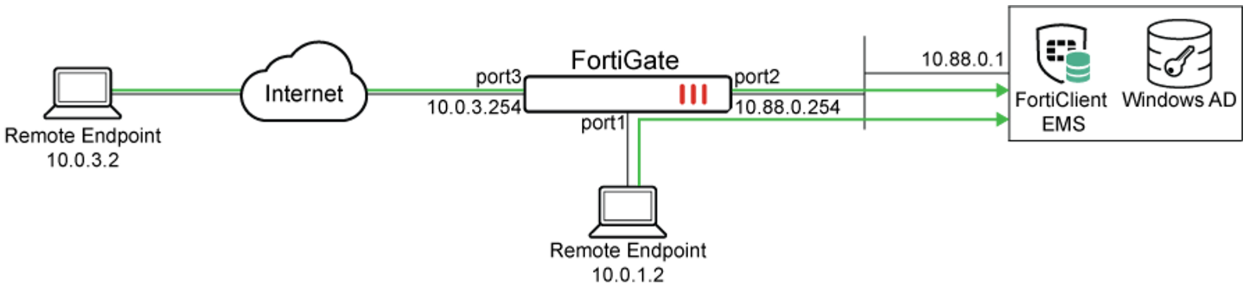
If users will download FortiClient directly from EMS, there are a few requirements:

- A certificate is used by the service hosting the installers. This certificate must be trusted by the endpoint in order to establish a secure connection. For information on where to configure this certificate, see the Web server section of EMS Server Certificates.
- The installers are hosted on TCP port 10443. This port will need to be reachable by the user. If the user is external, you may need to implement a virtual IP address and firewall policy to allow access.
- Users must be given the download URL. This is included in invitations.

Registering users

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, the proper firewall policies will need to be configured.

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

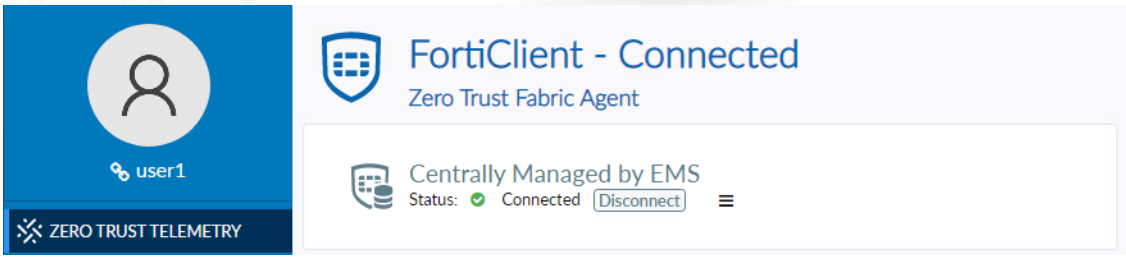


You must configure the following:

- Virtual IP address and firewall policy on the FortiGate to allow external connections to FortiClient EMS on 10.88.0.1:8013. If you require FortiClient download, also allow the HTTPS port, which is 443 by default.
- Firewall policy allowing internal subnets to connect to FortiClient EMS.
- FortiClient FQDN must be resolvable internally and remotely. This may require you to register the FQDN on a public DNS.

To register a user:

1. Open the invitation email and do one of the following:
   a. Click *Register to EMS*. Follow the instructions to register to EMS.
   b. Copy the invitation code. Enter the invitation code on the FortiClient *Zero Trust Telemetry* tab, and click *Connect*.
2. In the popup, provide the credentials matching your selected authorization type, then click *Login*. FortiClient proceeds with the registration process after authentication succeeds. After FortiClient successfully registers to EMS, the username in FortiClient changes to the verified user account, and a chain icon appears beside the username to indicate that FortiClient is registered with a verified user.



Verifying users in EMS

After a user has successfully registered to EMS, you can verify this from EMS by checking the following.

To verify users in EMS:

1. In EMS, go to *Endpoints > Invitations*. The *Active Users* column indicates how many users have successfully registered with the EMS.

Invitations — Add — Refresh

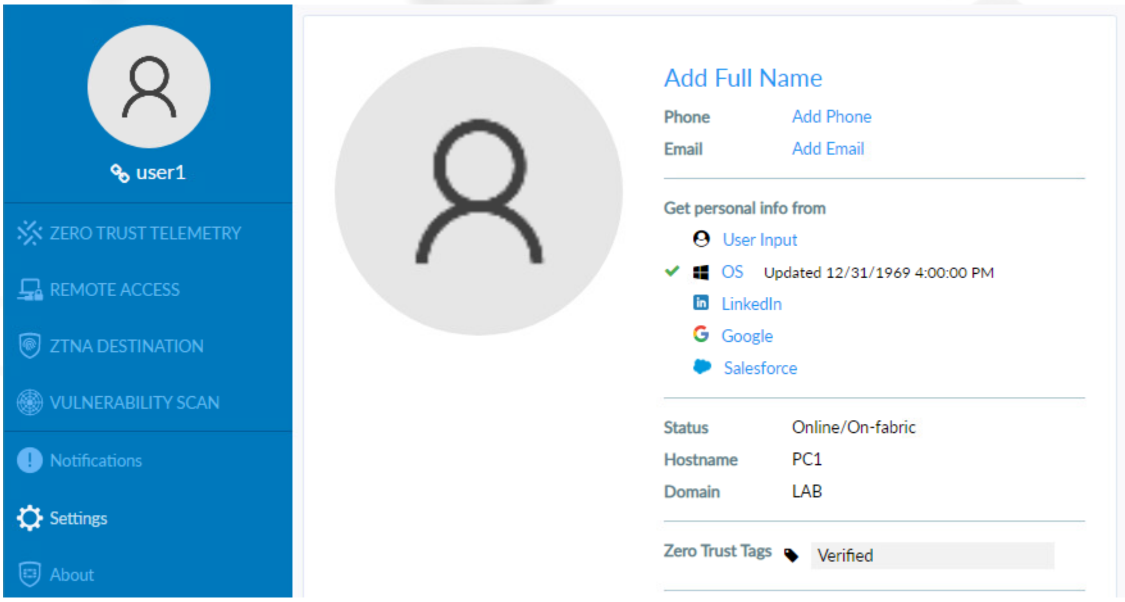
Name	Type	Active Users	Expiry Date	Verification Type
invite-001	Bulk	2		Domain

2. Go to *User Management* and select *Verified Users* to get a list of the users who have authenticated.
3. Click a user to see more details. The left pane displays the *Zero Trust Tags* indicating that this endpoint has a verified user.

You can also verify the tags on FortiClient if you enable the option to display tags on the FortiClient GUI.

To configure the ZTNA tag to display on the FortiClient:

1. Go to *Endpoint Profiles > System Settings*.
2. Edit the desired profile.
3. Ensure that *Advanced* is selected.
4. Under *UI*, enable *Show Zero Trust Tag on FortiClient GUI*.
5. Save.



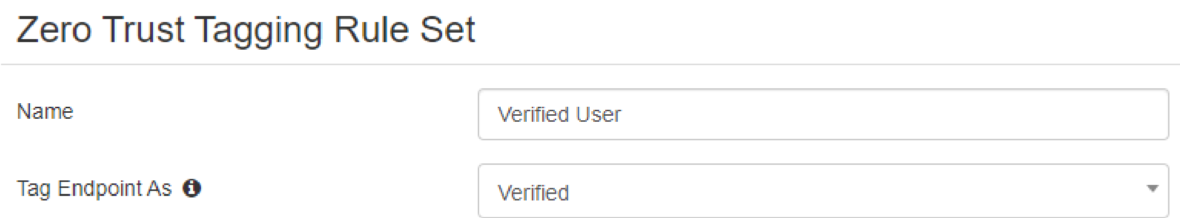
Next steps

With users successfully verified and onboarded, you can create and apply EMS zero trust network access (ZTNA) tagging rules can be created and applied to the users. You apply them in the same way as with unverified users following the same steps in Configuring EMS ZTNA tagging rules, but with the following benefits:

- Increased confidence of which users the tags are applied to
- Ability to use additional fields in a tagging rule.

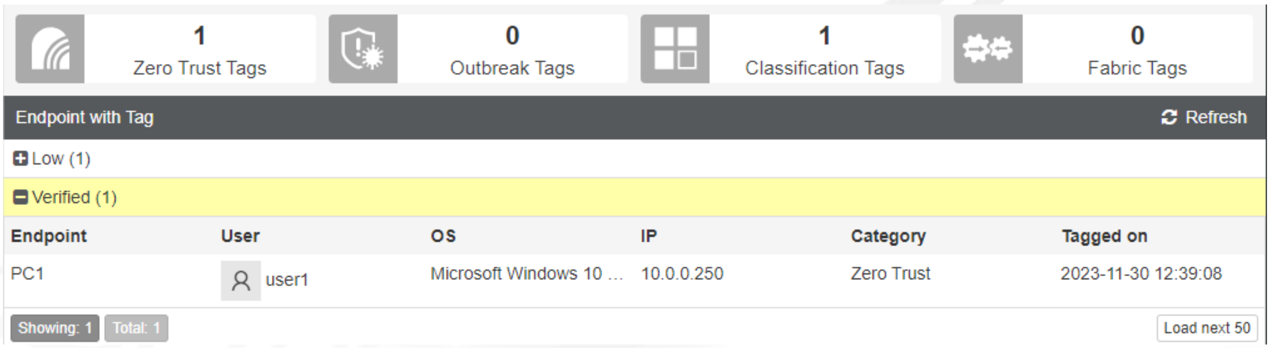
To configure a tagging rule for verified users in EMS:

1. Go to *Zero Trust Tags > Zero Trust Tagging Rules*.
2. Click *Add*.
3. Configure the *Name* and *Tag Endpoint As* fields as desired. For example, you could enter Verified for the tag value.



4. In the *Rules* table, select *Add Rule*.
5. From the *Rule Type* dropdown list, select *User Identity*.
6. From the *User Identity* dropdown list, select *Verified User*.
7. Click *Save* twice.
8. Go to *Zero Trust Tags > Zero Trust Tag Monitor*. After some time, the *Verified* tag appears with the tagged endpoint. You can now use this tag in your ZTNA deployment following the ZTNA Deployment

Guide.


1
Zero Trust Tags
0
Outbreak Tags
1
Classification Tags
0
Fabric Tags
Endpoint with Tag
Refresh
Low (1)
Verified (1)
Endpoint
User
OS
IP
Category
Tagged on
PC1
user1
Microsoft Windows 10 ...
10.0.0.250
Zero Trust
2023-11-30 12:39:08
Showing: 1
Total: 1
Load next 50

More information

Appendix A - Products used in this guide

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

Product	Model	Firmware
FortiClient EMS	N/A	7.2.1
FortiClient		

Appendix B - Documentation references

Feature documentation

- EMS Administration Guide:
  - Deployment & Installers
  - User Management
  - Zero Trust tagging rules
- Zero trust network access (ZTNA):
  - Endpoint posture check
  - Concept Guide

Best practices

- ZTNA solution hub
- ZTNA 4-D resources

www.fortinet.com

04-72-1038658-20240603