ESET
SECURE
AUTHENTICATION

VMware Horizon View
Integration Guide
1. Overview

This document describes how to enable Two-Factor Authentication (2FA) for a VMware Horizon View (formerly known as VMware View) installation using ESET Secure Authentication (ESA).

This integration guide utilizes **VPN validates AD user name and password** VPN type for this particular VPN appliance. If you wish to utilize other VPN type, refer to the [generic description of VPN types](#) and verify with the vendor if the VPN appliance supports it.

Note that this document describes how to configure VMware Horizon View Two Factor Authentication using ESA Mobile Application OTPs. It is also possible to use SMS OTPs, but the steps required for this are not explained here.

2. Prerequisites

Configuring VMware Horizon View for 2FA requires:

- A functional ESA RADIUS server that has the View Connection Server configured as a client, as shown in **Figure 1**.

**NOTE**: Only mobile application OTPs are required, since the VMware Connection Server authenticates the AD username and password in addition to requesting the second factor. For this reason you may disregard the warning at the bottom of the **New Client Properties** window.

- VMware Horizon View 5.1 or later

![VMWare View Connection Server Properties](image)

**Figure 1**

This picture shows the ESA RADIUS client configuration for VMware Horizon View Connection Server. Note that the check box next to **Mobile Application** must be selected and the **IP address** is the internal address of your VMWare Horizon View appliance.
3. Integration instructions

1. Configure the VMware Connection server:
   a. Log into your View Connection Server from a web browser. The default URL is https://hostname/admin.
   b. Navigate to View Configuration > Servers > Connection Servers.
   c. Select the Connection Server and click Edit. Under Authentication -> Advanced Authentication, select RADIUS from the 2-factor authentication drop-down menu.
   d. Ensure that the check box next to Enforce 2-factor and Windows user name matching is selected. This ensures that the Windows login prompt after RADIUS authentication will force the username to be the same as the RADIUS username.
   e. From the Authenticator drop-down menu, select Create New Authenticator, as shown in Figure 2.

![Figure 2](image)

   f. Set your preferred label and description. Set the hostname/address to be your ESA RADIUS server’s. Ensure the authentication port is 1812.
   g. Set the accounting port to 0 (the number zero).
   h. Set the authentication type to PAP.
   i. Enter the shared secret you used during the configuration of the client (as shown in Figure 1).
   j. Set the server timeout to 10 seconds.
   k. Figure 3 provides a reference against which to check your settings.
   l. If desired, add a second RADIUS server under the secondary authentication server tab (note that you will need to install ESA RADIUS on that server).

2. Test the connection:
   a. Launch the VMware Horizon View Client.
   b. Connect to your VMware Connection Server.
   c. In the Username field, enter a user that has been configured to use the ESA 2FA Mobile application.
d. In the **Passcode** field, enter a One-time Password (OTP) generated by the user’s Mobile application.

e. Authentication should succeed, and you will be prompted for your password. Enter your Active Directory (AD) password.

![Edit RADIUS Authenticator](image)

**Figure 3**

This screenshot shows how to configure RADIUS 2FA for a View Connection server.

4. **Troubleshooting**

If you are unable to authenticate via the ESA RADIUS server, ensure that you have performed the following steps:

1. Run a smoke test against your RADIUS server, as described in the [Verifying ESA RADIUS Functionality](#) document.
2. Delete the **Dummy Client** RADIUS client, and create a new client for your VMware Horizon View Connection Server, as shown in **Figure 1**.
3. Repeat the NTRadPing test, but run NTRadPing from your VMware Connection Server instead. This will verify that it has network connectivity to the RADIUS server.
4. Double check that you have used the correct IP addresses for your connection server and RADIUS server.
5. If you are still unable to connect, verify that your VMware installation is functional without 2FA before enabling 2FA.
6. If you are still unable to connect, contact ESET Customer Care.