

ESET **SECURE** **AUTHENTICATION**

Microsoft RRAS with NPS PPTP VPN
Integration Guide

ESET **SECURE AUTHENTICATION**

Copyright . 2013 by ESET, spol. s r.o.

ESET Secure Authentication was developed by ESET, spol. s r.o.

For more information visit www.eset.com.

All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.

ESET, spol. s r.o. reserves the right to change any of the described application software without prior notice.

Customer Care Worldwide: www.eset.eu/support

Customer Care North America: www.eset.com/support

REV. 7/22/2013

Contents

1. Overview.....	4
2. Prerequisites.....	5
3. Integration Instructions.....	6
4. Troubleshooting.....	7

1. Overview

This document describes how to enable ESET Secure Authentication (ESA) Two-Factor Authentication (2-FA) for a Microsoft NPS enabled RRAS VPN.

Since Microsoft RRAS does not perform encryption of the VPN connection when the PAP protocol is used, it is not recommended that you use **Compound Authentication**. Furthermore, since users are able to log in without entering their AD password if **Mobile Application** is selected, it is strongly recommended that you enforce a PIN on the Mobile Application under **Basic Settings** in the ESA Management Console, as shown in **Figure 2**.

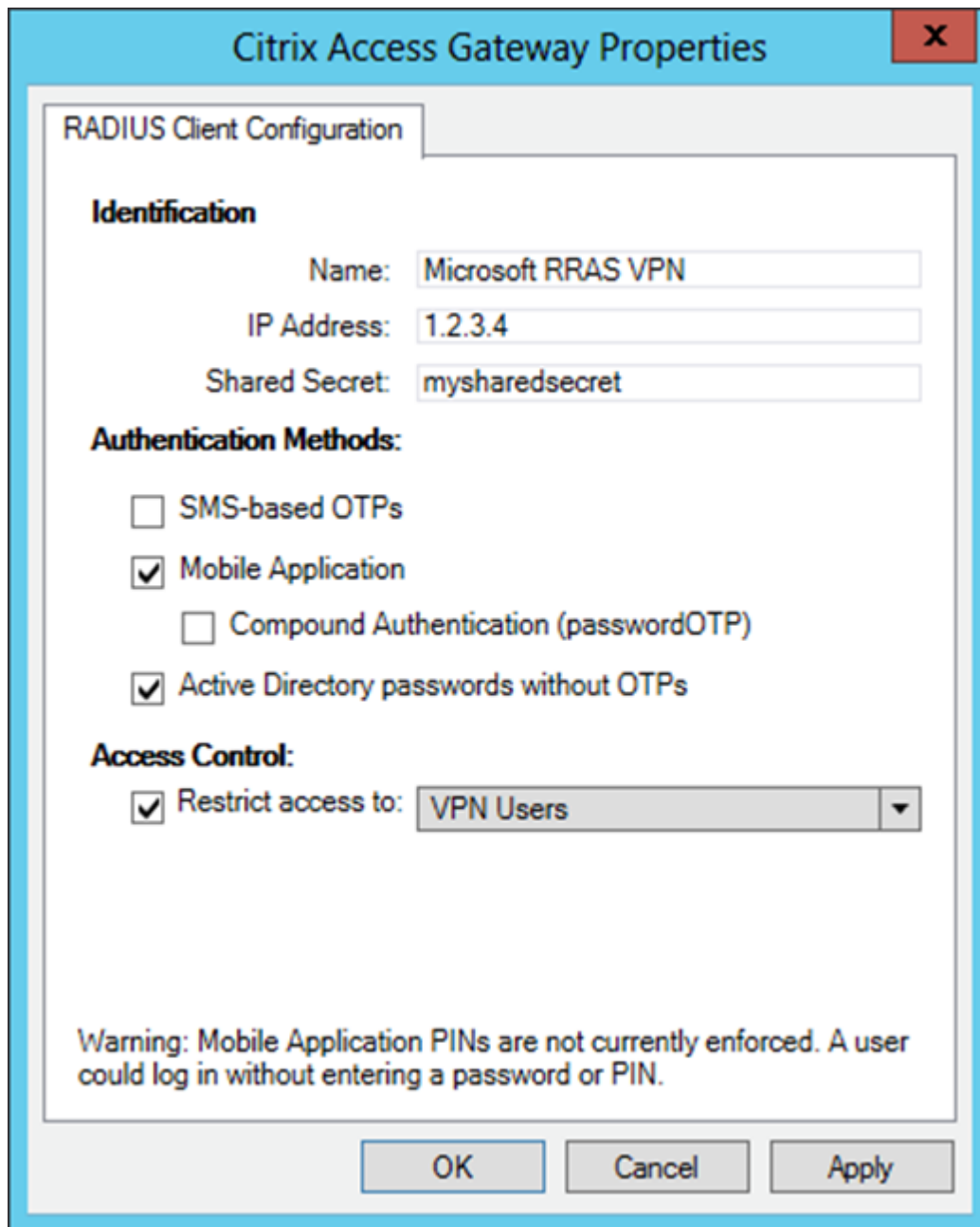
2. Prerequisites

Configuring the VPN for 2FA requires:

- A functional ESA RADIUS server that has your Microsoft RRAS with NPS VPN Server configured as a client, as shown in **Figure 1**.

Note: To prevent locking any existing, non-2FA enabled AD users out of your VPN, we recommend that you allow Active Directory passwords without OTPs during the transitioning phase. It is also recommended that you limit VPN access to a security group (for example **VPNusers**).

- A Microsoft RRAS with NPS VPN Server



The screenshot shows the 'Citrix Access Gateway Properties' dialog box with the 'RADIUS Client Configuration' tab selected. The 'Identification' section contains three text boxes: 'Name' with 'Microsoft RRAS VPN', 'IP Address' with '1.2.3.4', and 'Shared Secret' with 'mysharedsecret'. The 'Authentication Methods' section has four checkboxes: 'SMS-based OTPs' (unchecked), 'Mobile Application' (checked), 'Compound Authentication (passwordOTP)' (unchecked), and 'Active Directory passwords without OTPs' (checked). The 'Access Control' section has one checked checkbox 'Restrict access to:' followed by a dropdown menu showing 'VPN Users'. At the bottom, there is a warning message: 'Warning: Mobile Application PINs are not currently enforced. A user could log in without entering a password or PIN.' and three buttons: 'OK', 'Cancel', and 'Apply'.

Figure 1

Figure 1 shows the RADIUS client settings for your Microsoft RRAS with NPS VPN device. Note that the check boxes next to **Mobile Application** and **Active Directory passwords without OTPs** must be selected and the **IP address** is the internal address of your RRAS Server.

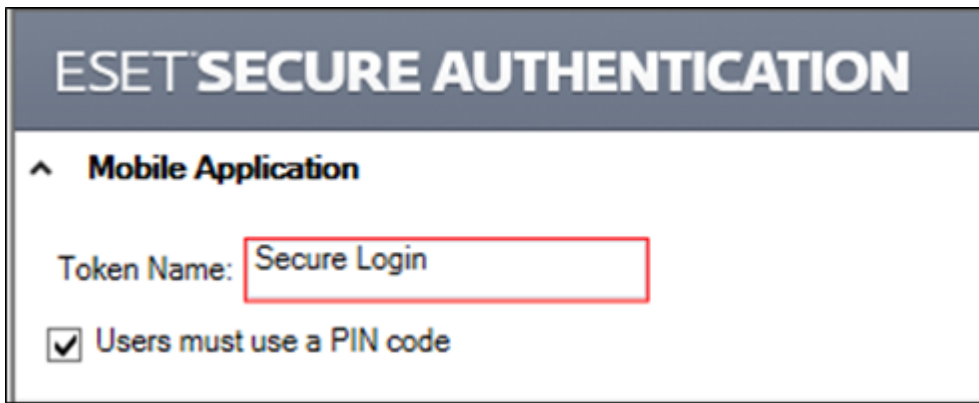


Figure 2

Figure 2: It is strongly recommended that you enforce PIN usage on the **Mobile Application** when not using **Compound** or **SMS authentication**.

3. Integration Instructions

1. Configure your RADIUS server in NPS:
 - a. Under **NPS** in **Server Manager**, expand **RADIUS Clients and Servers**.
 - b. Select **Remote RADIUS Server Groups**.
 - c. Create a new group from the context menu.
 - i. Enter a name for the group, for example, **ESA RADIUS Server Group**.
 - ii. Click **Add** to add a RADIUS Server.
 - iii. In the **Address** Tab: Type the IP Address of the ESA RADIUS Server in the **Server** Field.
 - iv. In the **Authentication/Accounting** Tab: Ensure that the port is 1812; enter the shared secret as shown in **Figure 1**.
 - v. In the **Load Balancing** Tab: Increase the **Number of seconds before request is considered dropped... / timeout** field to 30 seconds.
2. Configure the NPS Server to delegate authentication to ESA
 - a. Navigate to **Policies > Connection Request Policies**.
 - b. Create a new policy from the context menu.
 - c. In the **Overview** Tab:
 - i. Set the policy Name for example to **ESA RADIUS Authentication**.
 - ii. Set the policy **Type** to **Remote Access Server** (VPN Dial-up).
 - d. In the **Conditions** Tab:
 - i. Specify conditions as needed (e.g. date/time > any).
 - e. In the **Settings** Tab:
 - i. Navigate to Forwarding **Connection Request -> Authentication**.
 - ii. Select **Forward requests**.
 - iii. Select the **ESA RADIUS Servers Group** created in Step 1.
3. Test the authentication:
 - a. Launch the native Microsoft VPN client.
 - b. Make sure that the VPN type has been set to **PPTP**.
 - c. Make sure that **Maximum Encryption** has been selected.

- d. Make sure that the **Authentication Protocol** has been set to **MS-CHAPv2** (and all others checkboxes have been deselected).
- e. Enter the credentials of your test user from step 1:
 - i. Make sure that you are using a user that has been enabled for Mobile Application 2FA using ESA.
 - ii. In the password field, enter the OTP generated by the Mobile Application.

4. Troubleshooting

If you are unable to authenticate via the ESA RADIUS server, ensure 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. If you are still unable to connect, revert to an existing sign-in configuration (that does not use 2FA) and verify that you are able to connect.
3. If you are able to connect using the old settings, restore the new settings and verify that the firewall is not blocking UDP 1812 between you VPN device and your RADIUS server.
4. If you are still unable to connect, contact ESET technical support.