

# ESET **SECURE AUTHENTICATION**

Verifying ESA RADIUS Functionality

## 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](http://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](http://www.eset.eu/support)

Customer Care North America: [www.eset.com/support](http://www.eset.com/support)

REV. 7/22/2013

# Contents

- 1. Overview.....4
- 2. Make sure your ESA RADIUS Service is running4
- 3. Configure your RADIUS Server.....5
- 4. Verify functionality (localhost).....6
- 5. Verify network connectivity from another machine (optional).....7
- 6. Troubleshooting.....7
  - 6.1 I received an Access-Reject.....7
  - 6.2 I received a connection error.....8
  - 6.3 I experienced timeouts .....9

# 1. Overview

This document describes the necessary steps for verifying the connectivity of your ESA RADIUS server. The RADIUS standard requires that each client connecting to the RADIUS server be explicitly configured as a **RADIUS Client**.

Troubleshooting a RADIUS server consists of the following steps:

- Verifying that your RADIUS server is listening for incoming requests
- Testing connectivity to the RADIUS server from your localhost
- Testing connectivity to the RADIUS server over the network

The last two steps require the NTRadPing utility, which must be downloaded [here](#).

To complete the tests in this guide, you will need an Active Directory (AD) user account for testing purposes. The user **Alice** is referred to throughout this guide as the AD user account used for testing. The static AD password Esa132 is used as the password for this testing account for the purposes of this guide.

**NOTE:** Make sure that **Alice** has no 2FA methods enabled in the ADUC before you begin.

Note that this guide was written for a deployment scenario where the ESA RADIUS Server is running on the same server as the ESA Core Authentication Service.

## 2. Make sure your ESA RADIUS Service is running

1. Open your Windows Services console, and verify that the **ESET Secure Authentication RADIUS Service** is in the Running state, as shown in **Figure 1**.
2. Verify that no other processes are listening on UDP 1812. Note that if your ESA RADIUS Service fails to start, it may be because a different process is listening on UDP 1812.
  - a. Open a command prompt and enter the following command:  

```
C:\>netstat -a -p udp -b | more
```
  - b. Verify that *EIP.Radius.WindowsService.exe* is the only service listening on UDP1812
  - c. If there are other processes listening on UDP 1812, you will not be able to use ESA's 2FA for VPN logins, so these processes must be stopped.

Active Connections

Proto	Local Address	Foreign Address	State
UDP	O.O.O.O:1812	*.*.*.*	

[EIP.Radius.WindowsService.exe]

- d. If there are any processes listening on UDP 1812, you will not be able to use ESA's 2FA for VPN logins, so these processes must be killed.

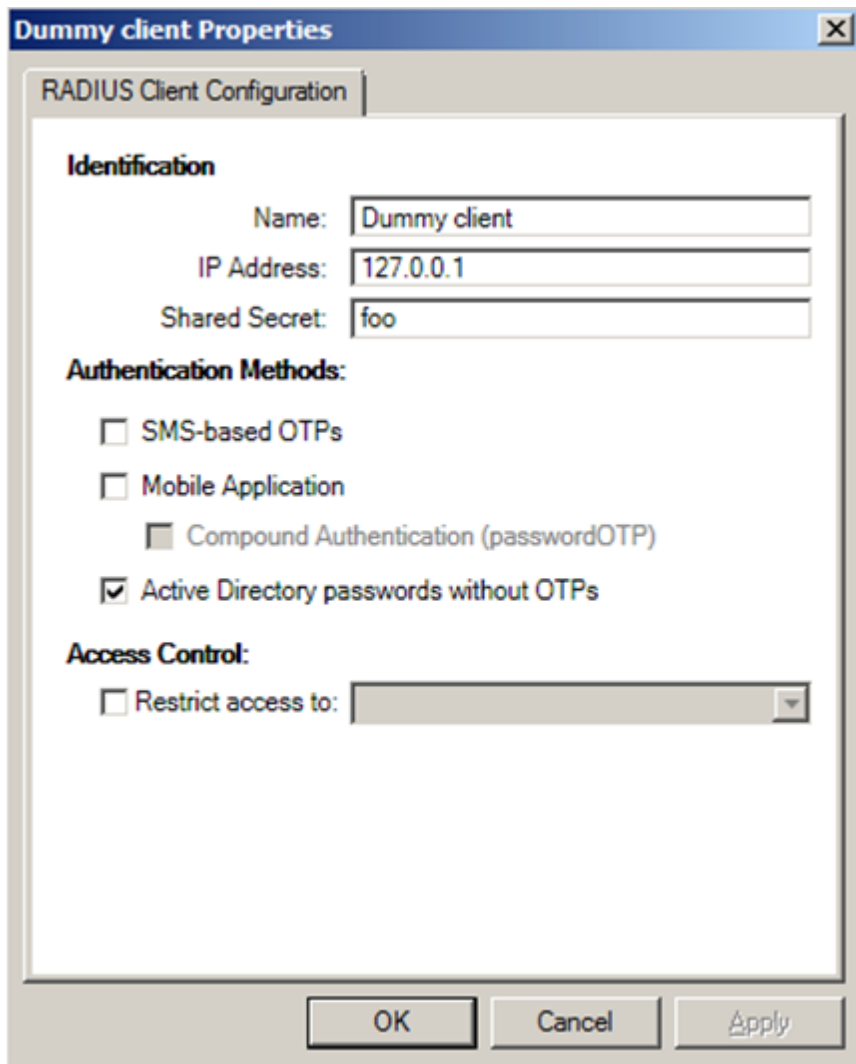
DS Role Server	This service ...	Manual
Encrypting File System (EFS)	Provides th...	Manual (Trig...
ESET Secure Authentication Core Service	Running	Automatic
ESET Secure Authentication NTLM Proxy Service	Running	Automatic
ESET Secure Authentication RADIUS Service	Running	Automatic
Extensible Authentication Protocol	The Extensi...	Manual
File Replication	Configuring...	Disabled

Figure 1: Verify that the ESET Secure Authentication RADIUS Service is Running

### 3. Configure your RADIUS Server

Follow the steps below to configure a dummy RADIUS client:

1. Launch the ESA Management Console (**Start > Administrative Tools > ESET Secure Authentication**) and ensure that an active ESA license is being used by the installation (the status of the license may be viewed by clicking your domain).
2. Expand **RADIUS Servers** and right-click your RADIUS server name. Select **Add Client**.
3. Double-click the New Client.
4. Fill out the details as shown in the following screenshot:



The screenshot shows a Windows-style dialog box titled "Dummy client Properties". It has a tab labeled "RADIUS Client Configuration". The dialog is divided into three sections: "Identification", "Authentication Methods", and "Access Control".

**Identification**

- Name:
- IP Address:
- Shared Secret:

**Authentication Methods:**

- ☐ SMS-based OTPs
- ☐ Mobile Application
  - ☐ Compound Authentication (passwordOTP)
- ☒ Active Directory passwords without OTPs

**Access Control:**

- ☐ Restrict access to:

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

Click **Apply**, then click **OK** twice. Restart your RADIUS service using the regular Windows Services utility.

## 4. Verify functionality (localhost)

1. Launch NTRadPing and fill out the values as shown in the following screenshot:

NTRadPing 1.5 - RADIUS Server Testing Tool  
© 1999-2003 Master Soft SpA - Italy - All rights reserved  
<http://www.dialways.com/>

ms MASTERSOFT DIALWAYS

RADIUS Server/port: 127.0.0.1 1812  
Reply timeout (sec.): 3 Retries: 6  
RADIUS Secret key: foo  
User-Name: alice  
Password:   
Request type: Authentication Request 0  
Additional RADIUS Attributes:   
RADIUS Server reply:   
Add Remove Clear list Load... Save... Send Help... Close

2. Click **Send**.

3. Verify that you received an **Access-Accept** response:

RADIUS Server reply:

Sending authentication request to server 127.0.0.1:1812  
Transmitting packet, code=1 id=0 length=45  
received response from the server in 109 milliseconds  
reply packet code=2 id=0 length=20  
response: Access-Accept  
----- attribute dump -----  
Send Help... Close

4. If you received a response other than **Access-Accept**, proceed to the troubleshooting section.

## 5. Verify network connectivity from another machine (optional)

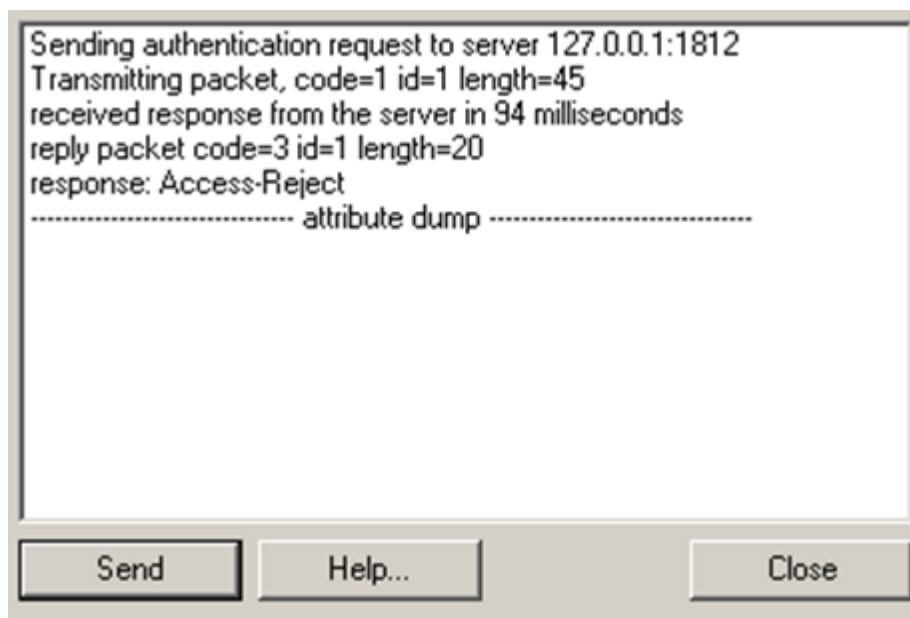
This step is useful to make sure that there are no networking issues between your machines.

1. If you received an **Access Accept** response during the first test and you are using Microsoft RRAS/NPS as your VPN server, repeat the steps for localhost testing but launch NTRadPing on your RRAS server and follow steps a and b below:
  - a. Change the NTRadPing IP address to point to your ESA RADIUS server.
  - b. Change the IP address of your **Dummy Client** to match your RRAS server.
2. If you are using a dedicated VPN appliance, perform the steps detailed above using another machine on the same network segment as your VPN appliance.

## 6. Troubleshooting

### 6.1 I received an Access-Reject

**Symptom:** you receive the following response:

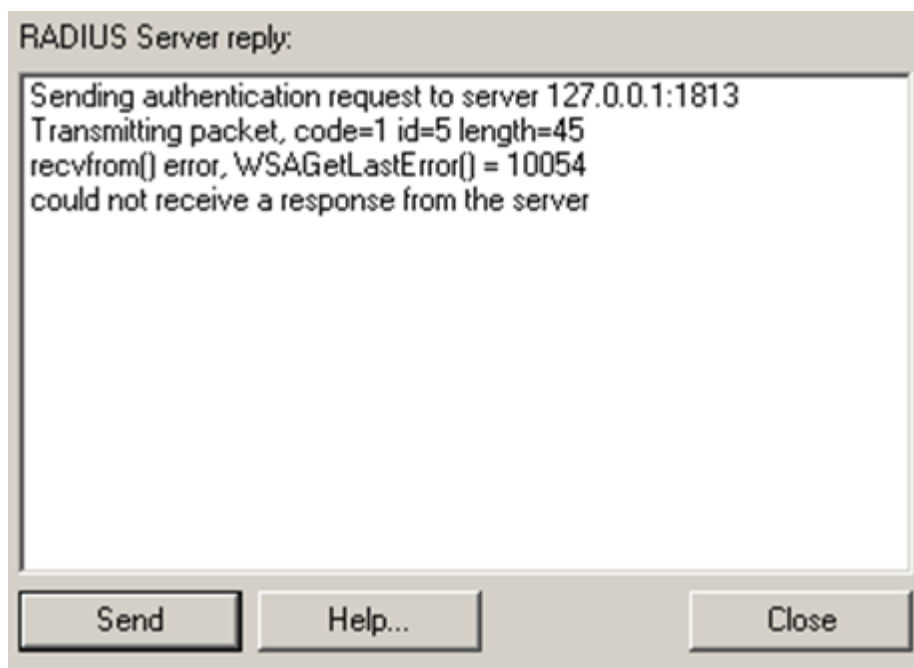


**Steps to resolve:** Verify the following:

1. Ensure you have typed alice's password into the Password field correctly. Retry by clicking the **Send** button again.
2. Ensure that alice's AD password is indeed what you are typing in. Reset the password if necessary.
3. Verify that in the ADUC, Alice does not have any 2FA methods enabled, ensure that Mobile Application and SMS OTPs are NOT selected.
4. Ensure that alice is not locked out, and unlock the account if necessary.
5. Double check your RADIUS configuration and your NTRadPing configuration.
6. If after completing the steps above you issue is still not resolved, contact ESET Customer Care and provide them with your RADIUS logfile, located in C:\ProgramData\ESET Secure Authentication\.

## 6.2 I received a connection error

**Symptom:** Instead of Access-Accept, you experience the following:



**Steps to resolve:**

1. Verify that your ESA RADIUS Service is in the **Started** state.
2. Ensure that you have entered the correct details into NTRadPing, as per the screenshot in section [Verify functionality \(localhost\)](#).
3. Verify that your RADIUS server is listening on the correct port. Launch a command prompt and run the following command:

```
netstat -a -p UDP -b C:\temp.txt
```

4. Open the file C:\temp.txt and verify that the following entries exist for your RADIUS server:

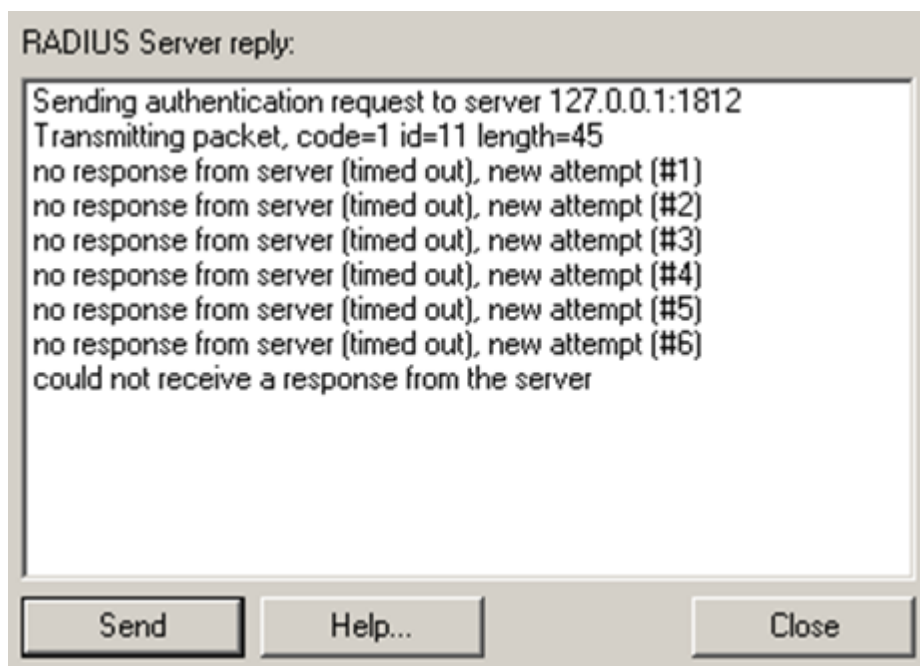
Proto	Local Address	Foreign Address	State
UDP	O.O.O.O:1812	*.*.*.*	
[EIP.Radius.WindowsService.exe]			

5. If none of the above solve the issue, contact ESET Customer Care and provide them with your RADIUS logfile, located in C:\ProgramData\ESET Secure Authentication\



## 6.3 I experienced timeouts

**Symptom:** Instead of Access-Accept, you receive the following:



**Steps to resolve:**

1. Ensure that you have created the dummy RADIUS client with the correct IP address, as per the instructions in the section [Configure your RADIUS Server](#).
2. Ensure that you have entered the correct details into NTRadPing, as per the screenshot in section [Verify functionality \(localhost\)](#).
3. Verify that your RADIUS server is listening on the correct port. Launch a command prompt and run the following command:

```
netstat -a -p UDP -b C:\temp.txt
```

4. Open the file C:\temp.txt and verify that there is an entry for your RADIUS server which looks like this:

Proto	Local Address	Foreign Address	State
UDP	0.0.0.0:1812	*.*	
[EIP.Radius.WindowsService.exe]			

5. If after performing the steps above your issue is still not resolved, contact ESET Customer Care and provide them with your RADIUS logfile, located in C:\ProgramData\ESET Secure Authentication\.