Release Notes

FreeRadius Authy Multifactor Authentication

Table of Contents

1 Introduction

1.1 Purpose

This guide will provide a step-by-step introduction to utilizing Authy's Time-based One Time Password (TOTP) and OneTouch features in a FreeRadius environment. The primary function of the features mentioned in this document is for the use with OpenVPN and Cisco AnyConnect Virtual Private Network (VPN) servers that will utilize FreeRadius for backend authentication. This document assumes the working environment is Linux based.

1.2 Intended Audience

This document is written for administrators to implement a multifactor authentication solution to FreeRadius using Authy. This document assumes the administrators have familiarity with the FreeRadius functionality and will be able to make decisions to the configuration if there are any conflicts with the in-place system. This document will also assume the appropriate administrators will be able to configure a VPN solution to utilize FreeRadius.

2 Before You Install

Prerequisites for installing and running the Authy MFA module for FreeRadius.

2.1 FreeRadius

A FreeRadius installation with the mlm_perl module available. The module is first available for FreeRadius 3.0.12.

2.2 Operating Systems

The Authy MFA module is working on the following operating systems:

- Red Hat Enterprise Linux 6.X

2.3 Clients

The Authy MFA module is working on the following clients using RADIUS authentication:

- OpenVPN 2.3.13 with the radius plugin
- Cisco Anyconnect using a Cisco ASA 5512-X router

2.4 Java Environment

The Authy MFA module allows for usage of a callback application, which is written in Java. The callback application is working on Java Runtime Environment 7.

3 Limitations and Known Issues

3.1 Limitations

- Two modules are offered to retrieve Authy ID from a user store – LDAP and CSV. Other ID stores are not currently implemented.
- The current implementations of the FreeRadius module and callback application are intended to be single node installations. These applications do not currently account for clustering, failover, or any high-availability functions.
- There is no message relayed to the user when OneTouch flow is initiated. The user must be aware OneTouch request has been generated and approve or deny the request appropriately.

3.2 Known Issues

- The client must have an appropriate server response timeout set so the user can approve or deny OneTouch requests. Typically server response timeouts are set short on clients as a long server response wait time can indicate a connection failure but the server using the module is waiting on human input before responding with a success or reject.