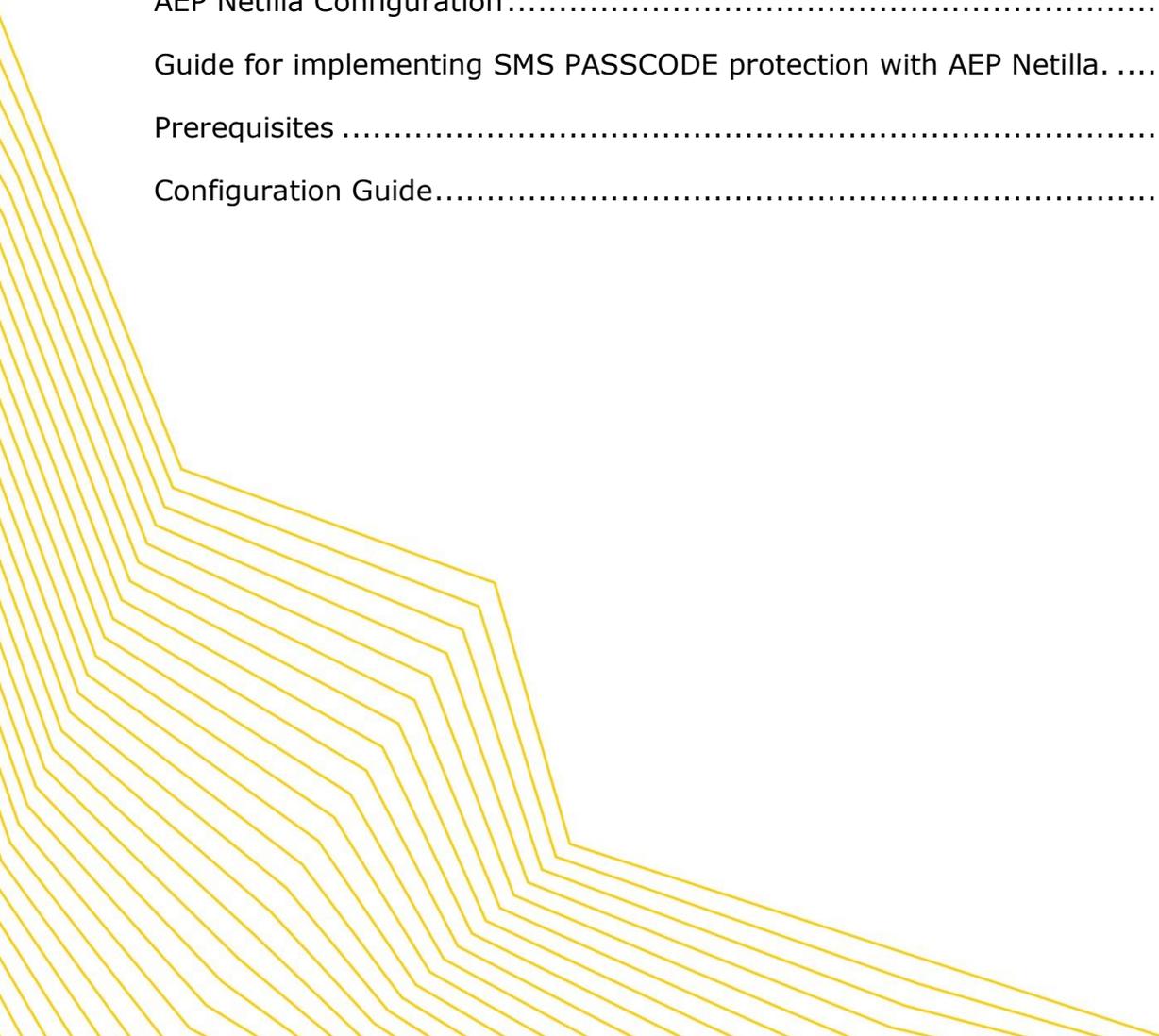




AEP Netilla Configuration

Contents

AEP Netilla Configuration	0
Guide for implementing SMS PASSCODE protection with AEP Netilla.	1
Prerequisites	1
Configuration Guide.....	1





Guide for implementing SMS PASSCODE protection with AEP Netilla.

This document outlines the process of configuring AEP Netilla with SMS PASSCODE protection.

Prerequisites

AEP Netilla
Microsoft radius server (NPS)
SMS PASSCODE

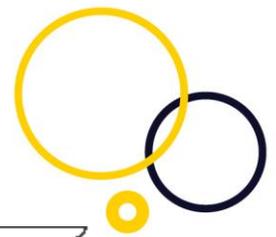
Configuration Guide

When setting up the AEP Netilla to use Radius authentication, you need to set up two stages.

The first stage should be LDAP, for username and password authentication.
The second stage should be Radius, for the SMS authentication.



In the Radius stage (Stage 2) set a false password in the field "Initial password". Then set SMS PASSCODE to skip password check in the SMS PASSCODE configuration tool.



aep™ Series A
NETWORKS
Administrator Site - Version 7.2.0.9

V-realm: local
eth0 IP Address: 10.0.0.1
eth1 IP Address: 0.0.0.0

User: admin
Role: admin

[Return to Webtop](#) [Help](#)

Authentication Stage 2 (SMS)

Type: **RADIUS**

Authentication Scope:

Domain:

Use same username as previous stage?

Username Template:

Reauthentication Interval:

Reauthentication Retries:

Primary RADIUS

RADIUS Server IP: RADIUS Port (Usually 1812 or 1645):

RADIUS Secret: RADIUS Timeout:

Initial password: Empty First Password:

Group Attribute ID: Attributes Encoding:

Secondary RADIUS

select to include backup server.

RADIUS Server IP: RADIUS Port (Usually 1812 or 1645):

RADIUS Secret: RADIUS Timeout:

Initial password: Empty First Password:

Group Attribute ID: Attributes Encoding:

[Edit Authentication Stage 2 \(SMS\) Policy](#)

If you have a Single Sign on solution, the username and password from Stage1 will be passed on. To configure and set up the radius server, please refer to the SMS PASSCODE administration guide. Radius server configuration is included in the SMS PASSCODE administration guide.