Cannot Log In Via External Authentication if the User Exists in the LDAP and Locally on the ESA

Document ID: 118739

Contributed by Mark Vegh and Enrico Werner, Cisco TAC Engineers.

Feb 10, 2015

Contents

Introduction

This document describes the behavior of AsyncOS when external authentication is enabled on the Email Security Appliance (ESA).

Problem

The ESA can be configured to use external authentication via Lightweight Directory Access Protocol (LDAP). Users who also have a local account configured on the ESA cannot log into the GUI and the CLI.

Solution

If external user authentication is enabled, the ESA uses both authentication methods in order to find the user which tries to connect to the ESA. First the appliance tries to authenticate the user via the external LDAP server.

Note: The administrator account is only available locally.

The two possible scenarios are:

- If the user exists in the LDAP database and also is assigned to a group which is allowed to manage the ESA, then the access is granted.
- If the user exists in the LDAP database and is not in any of the ESA managing groups, access is not granted for the user. This also applies in case of a local profile available for that user.

If the user does not exist in the LDAP server the local user list is used for authentication.