Obtain a BIOS Password for an SSL Appliance

Document ID: 118662

Contributed by Nazmul Rajib, William Koester, and Jose Escobar, Cisco TAC Engineers.
Nov 17, 2014

Contents

Introduction

The SSL Appliance 1500, 2000 and 8200 contains crypto materials that must be kept secure. For security reasons, an access to the CLI of an SSL Appliance is limited. For example, you cannot boot an appliance up into single user mode and access it via CLI. In addition, if you attempt to reimage an SSL Appliance, or attempt to access a boot menu or BIOS option, you may be prompted for a password, which is not created during initial bootstrap process. This document describes the processes to obtain a BIOS password.

Steps to Follow

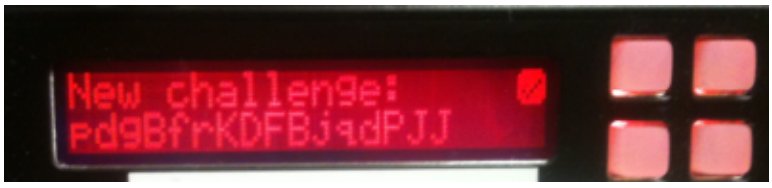
In order to obtain a password, please follow the steps below:

1. Obtain the Serial Number of your SSL Appliance. This is printed on the chassis.

2. Generate a Challenge Key on your SSL Appliance. Press the following sequences on the keypad:

UL, LL, UR, LR, UL, LL, UR, LR (Upper Left, Lower Left, Upper Right, Lower Right)

This triggers a back−end challenge generator, and the challenge is displayed on the LCD:



3. Write down the challenge key.
Caution: A challenge key is case sensitive.

4. Send the challenge key and serial number of the chassis to the Cisco Technical Support in order to obtain a password.