

Product Notice #0329



Windows Server 2012 R2 Hardening for CloudBond™ 365

This Product Notice explains how to harden the Windows Server 2012 R2 operating system used in CloudBond 365, based on public security recommendations, and how to use the AudioCodes Hardening Automation utility.

Detailed Notice

The hardening will be done by running the *ServerHardeningTool.exe* on all CloudBond 365 Operating Systems (Host and Virtual Machines). This will ease the following vulnerabilities:

- Disabled SMBv1
- Disabled Digest authentication
- Disabled SSLV2/V3
- Increased Diffie-Hellman Key size greater than '2048'
- Disabled the following Ciphers:
 - DES 56/56
 - RC2 128/128
 - RC2 40/128
 - RC2 56/128
 - RC2 56/56
 - RC4 128/128
 - RC4 40/128
 - RC4 56/128
 - RC4 64/128
 - Triple DES 168

ServerHardeningTool.exe will also enable TLS 1.0, TLS 1.1, TLS 1.2 and the AES 128/128 and AES 256/256 ciphers.

Performing the Hardening

Before performing the hardening, which disables some SSL and Cipher protocols, you must validate the following to use SSL/TLS and Ciphers which will be supported after the hardening:

SBC/Gateway TLS Context

This validates that the SBC/Gateway TLS Context, used with the CloudBond 365, are set to work with the supported TLS versions and Cipher types towards the CloudBond 365.

SNMPv3

If the SNMPv3 is used to monitor CloudBond 365, you need to ensure that it is set to use one of the supported Ciphers.

Downloading ServerHardeningTool.exe

The Server Hardening Tool zip file can be download from <https://downloads-audiocodes.s3.amazonaws.com/CB365%207.6/ServerHardeningTool.zip>

1. Unzip the file and copy the files to all CloudBond 365 Operating Systems - both Host and Virtual.
2. Run *ServerHardeningTool.exe*.
3. At the 'Do you wish to continue' message, enter "Y" to confirm the change.

```
C:\Users\Administrator\Documents\ServerHardeningTool\ServerHardeningTool...
This script will disable:
- SMBv1
- Digest Authentication
- PCT 1.0
- SSL 2.0
- SSL 3.0

The following weak ciphers:
- DES 56/56
- RC2 128/128
- RC2 40/128
- RC2 56/128
- RC2 56/56
- RC4 128/128
- RC4 40/128
- RC4 56/128
- RC4 64/128
- Triple DES 168

It will also set Set Diffie-Hellman to use 2048 bit and specifically enable TLS
1.0,
TLS 1.1, TLS 1.2 and the ciphers AES 128/128 and AES 256/256

Do you wish to continue? <y/n>
-
```

Note: This Product Notice only affects the CloudBond 365 product (and not CloudBond CCE).



If you have any questions, contact us at <https://www.audiocodes.com/corporate/offices-worldwide>

AudioCodes Ltd. | 1 Hayarden Street | Airport City | Lod | Israel | +972-3-976-4000

Join our mailing list for news and updates