Validate the Integrity of a Downloaded Software File

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Validation

Related Information

Introduction

This document describes how to verify the checksum of a software file downloaded from Cisco to a computer and onto any MDS or NX-OS switch.

Prerequisites

Requirements

There are no specific requirements for this document.

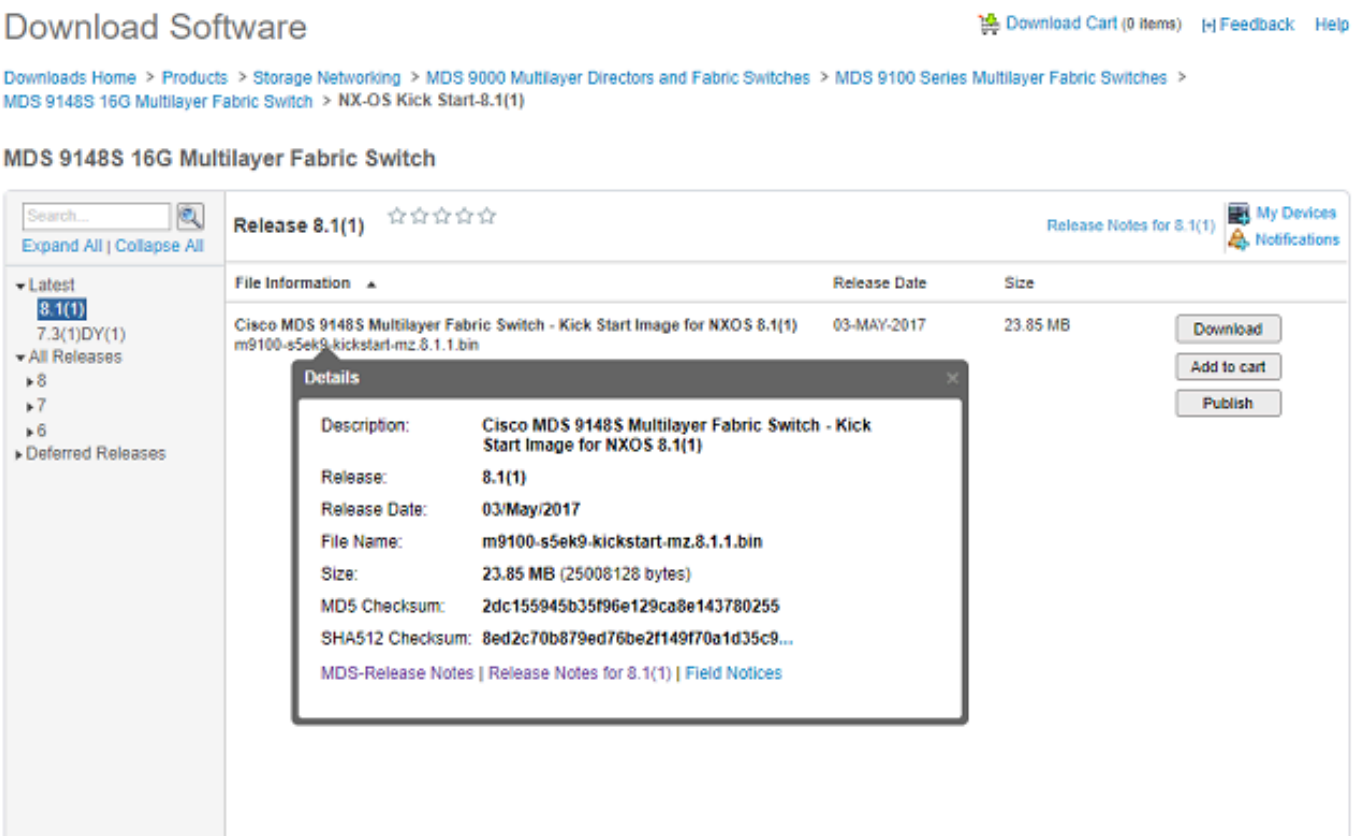
Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Validation

From the Cisco Software Download page, place the cursor over the file you want to download. This gives additional file details, which includes the MD5 and SHA512 checksum, as shown in the image:



On a Windows PC, there is an inbuilt tool, certutil, which you can use with the MD5 or SHA512 hash algorithms (amongst others) to establish the unique checksum of any file.

certutil -hashfile <filename> MD5|SHA512

Use the previous m9100-s5ek9-kickstart-mz.8.1.1.bin file as an example:

<#root>

```
c:\Temp>
certutil -hashfile m9100-s5ek9-kickstart-mz.8.1.1.bin MD5
MD5 hash of file m9100-s5ek9-kickstart-mz.8.1.1.bin:
2d c1 55 94 5b 35 f9 6e 12 9c a8 e1 43 78 02 55
CertUtil: -hashfile command completed successfully.
c:\Temp>
certutil -hashfile m9100-s5ek9-kickstart-mz.8.1.1.bin SHA512
SHA512 hash of file m9100-s5ek9-kickstart-mz.8.1.1.bin:
8e d2 c7 0b 87 9e d7 6b e2 f1 49 f7 0a 1d 35 c9 2e 75 75 bc 2f 88 1b 49 73 b6 a4 a8 db 44 98 78 2d 14 5c
CertUtil: -hashfile command completed successfully.
c:\Temp>
```

On a Mac, you can use **md5** or **shasum -a 512 <filename>** to achieve this:

```
<#root>
$
md5 m9100-s5ek9-kickstart-mz.8.1.1.bin

MD5 (m9100-s5ek9-kickstart-mz.8.1.1.bin) =
2dc155945b35f96e129ca8e143780255

$
shasum -a 512 m9100-s5ek9-kickstart-mz.8.1.1.bin

8ed2c70b879ed76be2f149f70a1d35c92e7575bc2f881b4973b6a4a8db4498782d145d6da6f4e50871ce9821862a76a726722be3
 m9100-s5ek9-kickstart-mz.8.1.1.bin
```

On a Linux or Unix machine, use **md5sum** or **sha512sum** typically located in /usr/bin, that is:

```
<#root>
$
md5sum m9100-s5ek9-kickstart-mz.8.1.1.bin
2dc155945b35f96e129ca8e143780255
 m9100-s5ek9-kickstart-mz.8.1.1.bin
$
sha512sum m9100-s5ek9-kickstart-mz.8.1.1.bin
8ed2c70b879ed76be2f149f70a1d35c92e7575bc2f881b4973b6a4a8db4498782d145d6da6f4e50871ce9821862a76a726722be3
 m9100-s5ek9-kickstart-mz.8.1.1.bin
```

Once the file is transferred to the MDS or Nexus bootflash, you can check the md5sum or sha512sum with:

```
<#root>
MDSswitch#
show file bootflash:m9100-s5ek9-kickstart-mz.8.1.1.bin ?

 <CR>
 > Redirect it to a file
 >> Redirect it to a file in append mode
 cksum Displays CRC checksum for a file

md5sum
```

```
 Displays MD5 checksum for a file
 sha256sum Displays SHA256 checksum for a file

sha512sum

 Displays SHA512 checksum for a file
 | Pipe command output to filter


MDSswitch#

show file bootflash:m9100-s5ek9-kickstart-mz.8.1.1.bin md5sum


2dc155945b35f96e129ca8e143780255


MDSswitch#

show file bootflash:m9100-s5ek9-kickstart-mz.8.1.1.bin sha512sum


8ed2c70b879ed76be2f149f70a1d35c92e7575bc2f881b4973b6a4a8db4498782d145d6da6f4e50871ce9821862a76a726722be3
```

From the previous example, you can see that the m9100-s5ek9-kickstart-mz.8.1.1.bin file off the Cisco Download Software site, the Windows, Mac or Linux PC, and the MDS switch has the same md5sum and sha512sum characters.

This confirms the validity of the file transferred to the switch.

Note: Some earlier NX-OS versions do not have the sha512sum option but md5sum must be present on all versions.

Related Information

- Cisco Technical Support & Downloads