show software authenticity

This chapter describes the output of the **show software authenticity** command.

- show software authenticity file, on page 1
- show software authenticity keys, on page 2
- show software authenticity running, on page 2

show software authenticity file

Table 1: show software authenticity file Command Output Descriptions

Field	Description
Authenticity Information	
Image Type	States the type of image.
Signer Information	
Common Name	CiscoSystems
Organizational Unit	StarOS
Organizational Name	CiscoSystems
Certificate Serial Number	Number assigned to the certificate.
Hash Algorithm	Type of algorithm used for hashing, such as SHA512.
Signature Algorithm	Type of algorithm used to sign this image, such as 2048-bit RSA.
Key Version	The version of the key used to generate the signature.
Validating digital signature, please wait ... done	This image is <not> authenticate.

show software authenticity keys

Table 2: show software authenticity keys Command Output Descriptions

Field	Description
Primary Public Key	#1 or #2
Backup Public Key	#3 or #4
Key Type	States the type of key, such as Released.
Key Algorithm	The algorithm used to generate the signature key, such as RSA.
Modulus (256 bytes)	Displays the encrypted text corresponding to the public key. Messages encrypted with the public key can only be decrypted using the private key.
Exponent (4 bytes)	The exponent used in modular exponentiation of the public key.
Key Version	The version of the algorithm used by Release Engineering to sign the starfile image.
Product Name	StarOS

show software authenticity running

Table 3: show software authenticity running Command Output Descriptions

Field	Description
SYSTEM IMAGE	
Image Type	States the type of image.
Signer Information	
Common Name	CiscoSystems
Organizational Unit	StarOS
Organizational Name	CiscoSystems
Certificate Serial Number	Number assigned to the certificate.
Hash Algorithm	Type of algorithm used for hashing, such as SHA512.
Signature Algorithm	Type of algorithm used to sign this image, such as 2048-bit RSA.

Field	Description
Key Version	The version of the key used to generate the signature.
Verifier Information	
Verifier Name	Firmware = CFE3 ROM
Verifier Version	Firmware release number
CFE3 ROM	
Image Type	States the type of image.
Signer Information	
Common Name	CiscoSystems
Organizational Unit	StarOS
Organizational Name	CiscoSystems
Certificate Serial Number	Number assigned to the certificate.
Hash Algorithm	Type of algorithm used for hashing, such as SHA512.
Signature Algorithm	Type of algorithm used to sign this image, such as 2048-bit RSA.
Key Version	The version of the key used to generate the signature.
Verifier Information	
Verifier Name	Firmware = BIOS/UEFI
Verifier Version	Firmware release number
BIOS3	
Image Type	States the type of image.
Signer Information	
Common Name	CiscoSystems
Organizational Unit	StarOS
Organizational Name	CiscoSystems
Certificate Serial Number	Number assigned to the certificate.
Hash Algorithm	Type of algorithm used for hashing, such as SHA512.
Signature Algorithm	Type of algorithm used to sign this image, such as 2048-bit RSA.
Key Version	The version of the key used to generate the signature.

Field	Description
Verifier Information	
Verifier Name	Microloader
Verifier Version	Release number