

View SSH Algorithms

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2016. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
2	SSH Algorithm Format	3



[View SSH Algorithms](#)



1 Introduction

This document describes how to view supported Secure Shell (SSH) algorithms.

1.1 Prerequisites

This section describes the prerequisites, which must be fulfilled before using the procedure.

1.1.1 Conditions

The following conditions must apply:

- The user has the System Security Administrator role.
- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.



[View SSH Algorithms](#)



2 SSH Algorithm Format

The value of attribute `selectedCiphers` consists of a string list of ciphers that must include at least one string. Each algorithm in the list must be in the `supportedCiphers` list.

The value of attribute `selectedKeyExchanges` consists of a string list of key exchanges that must include at least one string. Each algorithm in the list must be in the `supportedKeyExchanges` list.

The value of attribute `selectedMacs` consists of a string list of message authentication codes that must include at least one string. Each algorithm in the list must be in the `supportedMacs` list.

To view the SSH algorithm format:

1. Verify the SSH algorithm format:

```
(Ssh=1)>show -v
```

The following is an example output:

```
[...]
supportedCiphers <read-only>
  "aes256-ctr"
  "aes192-ctr"
  "aes128-ctr"
  "aes256-cbc"
  "aes192-cbc"
  "aes128-cbc"
  "cast128-cbc"
  "rijndael-cbc@lysator.liu.se"
  "blowfish-cbc"
  "3des-cbc"
  "arcfour"
  "arcfour128"
supportedKeyExchanges <read-only>
  "diffie-hellman-group-exchange-sha1"
  "diffie-hellman-group14-sha1"
  "diffie-hellman-group1-sha1"
supportedMacs <read-only>
  "hmac-ripemd160@openssh.com"
  "hmac-ripemd160"
  "hmac-sha1-96"
  "hmac-sha1"
  "hmac-md5-96"
  "hmac-md5"
```