

View SSH Algorithms

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2016, 2017. 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	Description	1
2	Procedure	1
2.1	View SSH Algorithms	1



[View SSH Algorithms](#)



1 Description

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

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

2 Procedure

2.1 View SSH Algorithms

Prerequisites

- No documents are required.
- No tools are required.
- 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.

Steps

1. Navigate to `Ssh` Managed Object (MO), for example:

```
>dn ManagedElement=N0DE06ST,SystemFunctions=1,SecM=1,Ssh=1
```
2. 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"
```