

Configure TLS Ciphers

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
1.1	Cipher Filter String Format	1
2	Procedure	2
2.1	Configure TLS Ciphers	2





1 Description

This instruction describes how to configure a system-wide Transport Layer Security (TLS) cipher setting for all TLS-based protocols.

1.1 Cipher Filter String Format

The value of attribute `cipherFilter` consists of one or more cipher filters separated by colons, each cipher filter can be any value of the members contained by a `Cipher` struct, as follows:

- Any cipher name in `supportedCiphers` list, for example PSK-AES256-CB C-SHA.
- Any cipher authentication method in `supportedCiphers` list, for example aPSK.
- Any cipher encryption method in `supportedCiphers` list, for example AES.
- Any cipher key exchange method in `supportedCiphers` list, for example kPSK.
- Any MAC in `supportedCiphers` list, for example SHA1.
- Any protocol version in `supportedCiphers` list, for example SSLv3.

The filter string can be prefixed by one of following marks:

- `!`, the ciphers are permanently deleted from the list. The ciphers deleted can never reappear in the list even if they are explicitly stated, for example `!AES` deletes all cipher suites using AES encryption method.
- `+`, the ciphers are combined in logical order “and” operation, for example `kRSA+AES` is for cipher suites using RSA key exchange method and AES encryption algorithm.
- `-`, the ciphers are deleted from the list, but any of the cipher suites can be added by later options.

The cipher filters must contain at least one positive expression, that is, without character `!` or `-` in the cipher string, otherwise the filter results in an empty cipher suite list.

The filter can also be configured as following two special strings:

- `ALL`, all cipher suites except for the NULL encryption ciphers, which must be explicitly enabled. NULL authentication ciphers are included.
- `DEFAULT`, all cipher suites except the NULL authentication and NULL encryption ciphers.



2 Procedure

2.1 Configure TLS Ciphers

- 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.
 - The user has basic knowledge of cryptography.

Steps

1. Navigate to `Tls` managed object, for example:

```
>dn ManagedElement=NODE06ST,SystemFunctions=1,SecM=1,Tls=1
```

2. Enter Config mode:

```
(Tls=1)>configure
```

3. Set the `cipherFilter` to configure proper cipher suites, for example:

```
(config-Tls=1)>cipherFilter="PSK-AES256-CBC-SHA:DES-CBC3-SHA"
```

The cipher filter string must follow the constraints stated in datatype `CipherList` under `Tls`.

4. Commit the settings:

```
(config-Tls=1)>commit
```

5. Verify the `cipherFilter`:

```
(Tls=1)>show cipherFilter
```

The following is an example output:

```
cipherFilter="PSK-AES256-CBC-SHA:DES-CBC3-SHA"
```

6. Verify that the `enabledCiphers` has been updated accordingly. The value of attribute `enabledCiphers` is automatically sorted by strength of cipher suites, strongest first:

```
(Tls=1)>show enabledCiphers
```



The following is an example output:

```
enabledCiphers="PSK-AES256-CBC-SHA"  
  authentication="aPSK"  
  encryption="AES"  
  export=""  
  keyExchange="kPSK"  
  mac="SHA1"  
  protocolVersion="SSLv3"  
enabledCiphers="DES-CBC3-SHA"  
  authentication="aRSA"  
  encryption="3DES"  
  export=""  
  keyExchange="kRSA"  
  mac="SHA1"  
  protocolVersion="SSLv3"
```