

SSH and TLS Protocol Management

DESCRIPTION

Copyright

© Ericsson AB 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	Introduction	1
2	Functions and Concepts	3
2.1	SSH	3
2.2	TLS	3
2.3	Method of selecting algorithms or cipher suites	3
2.4	Types of Operations	4
3	Managed Object Model	5
4	Configuration Management	7





1 Introduction

This document provides an overview of the SSH and TLS protocol management.





2 Functions and Concepts

The operator can use *SecM* to configure Transport Layer Security (TLS) and Secure Shell (SSH) authentication and encryption methods.

2.1 SSH

The Secure Shell (SSH) is a protocol for secure remote logon and other secure network services over an insecure network. The SSH transport layer is a secure, low-level transport protocol. It provides strong encryption, cryptographic host authentication, and integrity protection.

The SSH protocol uses certain algorithms for authentication and encryption. This document describes how algorithms for ciphering, key exchange, and message authentication can be configured; refer to [RFC 4253](#).

2.2 TLS

The Transport Layer Security (TLS) protocol provides communications security over the Internet. The protocol allows client-server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

The TLS security algorithms are expressed by cipher suites. A cipher suite defines a collection of key exchange, encryption, and authentication algorithms supported in TLS; refer to [RFC 5246](#).

2.3 Method of selecting algorithms or cipher suites

At first deployment, the system initializes a set of default SSH algorithms and TLS cipher suites. The default algorithms are chosen by Ericsson design, based current security design rules. Algorithms and cipher suites can be added to, or removed from the default list.

The supported algorithms and cipher suites specifies the full set of selectable items. The supported lists are constructed from the underlying SSH and TLS software, and may contain additional algorithms or remove ones that were deemed obsolete at software upgrade. If an algorithm is removed, make sure that the removed algorithm is not used exclusively by any peer of the Managed Element (ME), otherwise the connections of that peer will fail.

In the SSH case, if the default algorithms are not adequate, then the names of the preferred algorithms need to be added to the attribute that list the selected algorithms. Non-preferred algorithms can be removed by updating the same list.



In the TLS case, cipher suites are added by choosing types or names of the preferred ones. The selected types or names must be specified in the cipher suites filter according to the syntax of the filter. The filter also allows removal of cipher suites types and names.

2.4 Types of Operations

SSH and TLS protocol management supports the following operations:

- View enabled SSH algorithms:

Currently enabled SSH algorithms are accessible through attributes `selectedCiphers`, `selectedKeyExchanges`, and `selectedMacs` in the *Ssh* Managed Object (MO). For more details on how to perform this operation, refer to *View SSH Algorithms*.

- Change enabled SSH algorithms:

The SSH algorithms enabled may need to be changed because of security requirements or compatibility with SSH peers. The SSH algorithms must be selected from the supported algorithm set, accessible through the *Ssh* MO attributes `supportedCiphers`, `supportedKeyExchanges`, and `supportedMacs`. The enabled SSH algorithms can be configured through attributes `selectedCiphers`, `selectedKeyExchanges`, and `selectedMacs` in the *Ssh* MO. For more details on how to perform this operation, refer to *View SSH Algorithms* and *Configure SSH Algorithms*.

- View enabled TLS cipher suites:

Currently enabled TLS cipher suites in the system are accessible through the attribute `enabledCiphers`. The `enabledCiphers` attribute is the result of cipher filter applied on `supportedCiphers`. For more details on how to perform this operation, refer to *Show Supported and Enabled TLS Ciphers*.

- Change enabled TLS cipher suites:

The enabled TLS cipher suites may need to be changed because of security requirements, or for compatibility with TLS peers. The TLS cipher suites must be selected from the supported cipher suite set accessible through the `supportedCiphers` attribute of the *Tls* MO. The enabled TLS cipher suites can be configured through the attribute `cipherFilter`. For more details on how to perform this operation, refer to *Show Supported and Enabled TLS Ciphers* and *Configure TLS Ciphers*.

3 Managed Object Model

The Security Management managed area is represented in the *Managed Object Model (MOM)* as follows:

```
ManagedElement
+-SystemFunctions
  +-SecM
    +-Ssh
    +-Tls
```

For general information about the MOM, Managed Object Classes (MOCs), MOs, cardinality, and related concepts, refer to *Managed Object Model User Guide*.

The System Management MOCs are described in Table 1.

Table 1 Security Management Managed Object Class (MOC) Descriptions

Managed Object Class	Description
<i>SecM</i>	The root of the System Management model
<i>Ssh</i>	Configures system-wide properties of SSH
<i>Tls</i>	Configures system-wide properties of TLS





4 Configuration Management

SSH and TLS protocol management is accessed using NETCONF or the ECLI to manipulate the MIB.

The following operations, described in Operating Instructions using the ECLI, can be performed by an administrator with the System Security Administrator role:

SSH

- *View SSH Algorithms*
- *Configure SSH Algorithms*

TLS

- *Show Supported and Enabled TLS Ciphers*
- *Configure TLS Ciphers*