Tamper Detection Feature

Teldat-Dm 825-I

Legal Notice

Warranty

This publication is subject to change.

Teldat offers no warranty whatsoever for information contained in this manual.

Teldat is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

I Related Documents. 1

Chapter 1 Introduction 2

Chapter 2 Configuration 3

2.1 Getting the Tamper Detection Feature 3

2.2 Configuration Commands for the Tamper Detec. Feature 4

2.2.1 ENABLE. 4

2.2.2 NO 5

Chapter 3 Monitoring. 6

3.1 Accessing interface monitoring 6

3.2 Interface monitoring. 6

3.2.1 STATUS. 6

I Related Documents

Teldat-Dm 704-I Configuration and Monitoring

Teldat-Dm 772-I Common Configuration Interfaces

Chapter 1 Introduction

The *Tamper Detection* feature allows the device to detect an active attempt to compromise its integrity or that of associated data.

If a threat is detected, the device can then take appropriate defensive action. The main application for tamper detection is its use in utility metering systems (such as energy, gas and water meters, data concentrators, data gateways, etc.).

Tamper Detection identifies unwanted activities that attempt to prevent devices from operating.

Some Teldat devices include the *Tamper Detection* feature, based on physical tampering.

Physical tampering is defined as any physical activity aimed at preventing the measurement mechanism in the device from working.

Physical tampering includes:

1. Opening the front cover of the device.

2. Opening the back cover of the device.

3. Inserting metal objects into the device.

The device automatically sends a tamper alert if someone tries to open the cover. Hence, any tampering that involves opening the cover is detected. Metal objects cannot be inserted without first opening the cover.

The device can send an SNMP Trap or generate an event whenever it detects tampering.

Please contact Teldat's Technical Service for more information on devices that support *Tamper Detection*.

Chapter 2 Configuration

2.1 Getting the Tamper Detection Feature

You can set the configuration options for the *Tamper Detection* feature in the *TAMPER-Det* configuration menu.

To access the *TAMPER-Det* configuration menu, first access the general configuration menu and (from there) access the *TAMPER-Det* feature.

```
onfig>feature ?
  aaa                     AAA configuration environment
  acat                    Advanced Choice-based Action Taker configuration
                          environment
  access-lists            Access generic access lists configuration
                          environment
  act                     Alsa custom trap configuration environment
  afs                     Advanced stateful firewall and routing
  autoset-cfg             Autoset-Config configuration environment
  bandwidth-reservation   Bandwidth-Reservation configuration environment
  class-map               Class Map configuration environment
  dns                     DNS configuration environment
  dns-updater             DNS Updater configuration environment
  echo-responder          Echo protocol configuration environment
  err-disable             Error disable configuration
  frame-relay-switch      Frame Relay Switch configuration environment
  gps-applications        GPS applications configuration environment
  hotspot                 Hotspot configuration environment
  http                    Access the router http protocol configuration
  ip-discovery            TIDP configuration environment
  ipv6-access-list        IPV6 access list configuration
  istud                   IPSEC Tunnel Server Discovery configuration
                          environment
  key-chain               Key chain management
  ldap                    LDAP configuration environment
  mac-filtering           Mac-filtering configuration environment
  management              Management configuration environment
  management-platform     Management Platform configuration
  netflow                 Netflow client configuration
  nsla                    Network Service Level Advisor configuration
  nsm                     Network Service Monitor configuration environment
  ntp                     NTP configuration environment
  policy-map              Policy Map configuration environment
  power-switch            TeleControl Module control environment
  prefix-lists            Access generic prefix lists configuration
                          environment
  radius                  RADIUS protocol configuration environment
  rmon                    Remote Network Monitoring configuration environment
  route-map               Route-map configuration environment
  scada-forwarder         SCADA Forwarder configuration environment
  sniffer                 Sniffer configuration environment
  spi                     SPI, mobile IP Presence Service,configuration
                          environment
  ssh                     Secure Shell configuration environment
  stun                    Stun facility configuration environment
  syslog                  Syslog configuration environment
  tamper-detection        Tamper Detection configuration environment
  tftp                    TFTP configuration environment
  vlan                    IEEE 802.1Q switch configuration environment
  vli                     Virtual Linux Interface configuration
  vrf                     VRF configuration environment
  wnms                    Wireless Network Management System
  wrr-backup-wan          WRR configuration environment
  wrs-backup-wan          WRS configuration environment
Config>feature
```

Example showing how to access the *Tamper Detection* menu:

```
Config>feature tamper-detection

-- Tamper Detection Configuration --
TAMPER-Det Config>
```

Note

The *Tamper Detection* feature is only available on some devices and you may need a license to enable it. Please contact our Technical Service for more information on the devices that support this feature.

2.2 Configuration Commands for the Tamper Detec. Feature

The *Tamper Detection* configuration commands must be entered in the configuration menu associated with the *TAMPER-Det* feature.

```
Config>feature tamper-detection

-- Tamper Detection Configuration --
TAMPER-Det Config>
```

You can enter the following commands from the *TAMPER-Det* configuration menu:

```
TAMPER-Det Config>?
  enable    Enables Tamper Detection feature
  no        Negate a command or set its defaults
  exit      Exit to parent menu
TAMPER-Det Config>
```

Command	Function
ENABLE	Enables the Tamper Detection feature.
NO	Removes a configuration parameter or restores its default value.
EXIT	Exits the TAMPER-Det configuration menu.

Command history:

Release	Modification
11.00.06	The "*enable*" and "*no*" commands were added as of version 11.00.06.
11.01.02	The "*enable*" and "*no*" commands were added as of version 11.01.02.

2.2.1 ENABLE

This parameter enables the *Tamper Detection* feature.

If *Tamper Detection* is enabled, the device will continuously monitor the detection mechanisms in order to report any attempts to tamper with the device.

Syntax:

```
TAMPER-Det Config>enable ?
  <cr>
```

Example:

```
TAMPER-Det Config>enable
TAMPER-Det Config>
```

Command history:

Release	Modification
11.00.06	The "*enable*" command was introduced as of version 11.00.06.
11.01.02	The "*enable*" command was introduced as of version 11.01.02.

2.2.2 NO

Removes a configuration parameter or restores its default value.

Syntax:

```
TAMPER-Det Config>no <command>
```

Example:

```
TAMPER-Det Config>no ?
  enable    Enables Tamper Detection feature
TAMPER-Det Config>no enable
```

Command history:

Release	Modification
11.00.06	The "*no*" command was introduced as of version 11.00.06.
11.01.02	The "*no*" command was introduced as of version 11.01.02.

Chapter 3 Monitoring

3.1 Accessing interface monitoring

The *Tamper Detection* feature monitoring menu is accessed from the general monitoring menu and allows you to access the *Tamper Det* feature.

The *Tamper Detection* feature appears as a *Tamper Det* menu.

Example:

```
+feature tamper-detection

-- Tamper Detection user console --

Tamper Det+
```

3.2 Interface monitoring

This section describes the *Tamper Detection* menu monitoring commands.

The monitoring commands are as follows:

```
Tamper Det+?
  status    Displays tamper detector status
  exit      EXIT
Tamper Det+
```

You can enter the following commands from the *Tamper Det* monitoring menu:

Command	Function
STATUS	Displays Tamper Detection status and statistics.
EXIT	Returns to the previous menu.

Command history:

Release	Modification
11.00.06	The "*status*" command was introduced as of version 11.00.06.
11.01.02	The "*status*" command was introduced as of version 11.01.02.

3.2.1 STATUS

This command displays status information linked to the *Tamper Detection* feature.

It shows whether the feature is enabled and the current state of the device's cover.

You can view statistics on how many times the cover has been opened or removed.

Syntax:

```
Tamper Det+status ?
  <cr>
```

Example:

```
Tamper Det+status

 Tamper detection feature.............: ENABLED
 Housing cover........................: REMOVED
 Number of times the cover was removed.: 17
 Number of times the cover was put.....: 16

Tamper Det+
```

Command history:

Release	Modification
11.00.06	The "*status*" command was introduced as of version 11.00.06.
11.01.02	The "*status*" command was introduced as of version 11.01.02.