



CHAPTER 9

Security Troubleshooting

Revised: July 22, 2009, OL-8723-19

Introduction

This chapter provides the information needed to monitor and troubleshoot security events and alarms. This chapter is divided into the following sections:

- [Security Events and Alarms](#)—Provides a brief overview of each security event and alarm.
- [Monitoring Security Events](#)—Provides the information needed to monitor and correct the security events.
- [Troubleshooting Security Alarms](#)—Provides the information needed to troubleshoot and correct the security alarms.

Security Events and Alarms

This section provides a brief overview of the security events and alarms for the Cisco BTS 10200 Softswitch in numerical order. [Table 9-1](#) lists all of the security events and alarms by severity.



Note

Click the Security message number in [Table 9-1](#) to display information about the event or alarm.

Table 9-1 Security Events and Alarms by Severity

Critical	Major	Minor	Warning	Info	Not Used
	SECURITY (3)		SECURITY (2)	SECURITY (1)	
			SECURITY (4)		
			SECURITY (5)		
			SECURITY (6)		

SECURITY (1)

For additional information, refer to the [“Test Report—Security \(1\)”](#) section on page 9-5.

DESCRIPTION	Test Report
SEVERITY	Information (INFO)
THRESHOLD	100
THROTTLE	0

SECURITY (2)

To monitor and correct the cause of the event, refer to the [“Invalid Credentials Presented by a Session Initiation Protocol Phone—Security \(2\)”](#) section on page 9-5.

DESCRIPTION	Invalid Credentials Presented by a Session Initiation Protocol Phone (Invalid Credentials Presented by a SIP Phone)
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Authentication User Name–STRING [33] From AOR–STRING [65] SIP Request Type–STRING [15] Sender IP–STRING [20]
PRIMARY CAUSE	There are invalid credentials in Session Initiation Protocol (SIP) request.
PRIMARY ACTION	Ensure that the password on the SIP phone matches the value provisioned in the BTS 10200.

SECURITY (3)

To troubleshoot and correct the cause of the alarm, refer to the [“Internet Protocol Security Connection Down—Security \(3\)”](#) section on page 9-7.

DESCRIPTION	Internet Protocol Security Connection Down (IPSEC Connection Down)
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	The kerberized management server (KMS) fails to establish the pf_key socket with the Internet Protocol security (IPSEC) engine. This implies that the IPSEC engine is not running and that it may not be installed.
PRIMARY ACTION	<ol style="list-style-type: none"> 1. Verify that the IPSEC is installed and running in the kernel. 2. Reboot. 3. If problem persists, call the Technical Assistance Center (TAC). (Contact Cisco TAC.)



Note

Refer to the [“Obtaining Documentation and Submitting a Service Request”](#) section on page lvi for detailed instructions on contacting Cisco TAC and opening a service request.

SECURITY (4)

To monitor and correct the cause of the event, refer to the [“Internet Protocol Security Media Terminal Adapter Key Establish Error—Security \(4\)”](#) section on page 9-5.

DESCRIPTION	Internet Protocol Security Media Terminal Adapter Key Establish Error (IPSEC MTA Key Establish Error)
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	A failure to establish the IPSEC keys to a given media terminal adapter (MTA) using Kerberized key management protocol has occurred.
PRIMARY ACTION	Validate the kerberos and the MTA device provisioning.

SECURITY (5)

To monitor and correct the cause of the event, refer to the [“Internet Protocol Security Outgoing Security Association Not Found—Security \(5\)”](#) section on page 9-6.

DESCRIPTION	Internet Protocol Security Outgoing Security Association Not Found (IPSEC Outgoing SA Not Found)
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	The KMS receives SA-missing messages from the IPSEC engine and is unable to find a provisioned device to establish the needed security association (SA).
PRIMARY ACTION	Remove or modify the security policy which caused the SA not found error. This action assumes that security is provisioned.

SECURITY (6)

To monitor and correct the cause of the event, refer to the [“Secure Session Initiation Protocol Endpoint Validation Failure—Security \(6\)”](#) section on page 9-6.

DESCRIPTION	Secure Session Initiation Protocol Endpoint Validation Failure (Secure SIP Endpoint Validation Failure)
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	AOR-STRING [65] Secure Fqdn-STRING [65] Source IP Address-STRING [16] Violation Description-STRING [80]
PRIMARY CAUSE	There is erroneous provisioning in the BTS 10200.
PRIMARY ACTION	Check if correct value of Secure-FQDN is provisioned in the BTS 10200.
SECONDARY CAUSE	There is erroneous provisioning in the domain name system (DNS).
SECONDARY ACTION	Verify the resolution of the Secure-FQDN in the DNS.
TERNARY CAUSE	There is erroneous provisioning in the customer premises equipment (CPE).
TERNARY ACTION	Verify the CPE provisioning to ensure that the correct source Internet Protocol (IP)/contact is used.

Monitoring Security Events

This section provides the information needed to monitor and correct security events. [Table 9-2](#) lists all of the security events in numerical order and provides cross reference to each subsection in this section.

Table 9-2 *BTS 10200 Security Events*

Event Type	Event Name	Event Severity
SECURITY(1)	Test Report—Security (1)	INFO
SECURITY(2)	Invalid Credentials Presented by a Session Initiation Protocol Phone—Security (2)	WARNING
SECURITY(3)	Internet Protocol Security Connection Down—Security (3)	MAJOR
SECURITY(4)	Internet Protocol Security Media Terminal Adapter Key Establish Error—Security (4)	WARNING
SECURITY(5)	Internet Protocol Security Outgoing Security Association Not Found—Security (5)	WARNING
SECURITY(6)	Secure Session Initiation Protocol Endpoint Validation Failure—Security (6)	WARNING

Test Report—Security (1)

The Test Report event is for testing the security event category. The event is informational and no further action is required.

Invalid Credentials Presented by a Session Initiation Protocol Phone—Security (2)

The Invalid Credentials Presented by a Session Initiation Protocol Phone event serves as a warning that credentials in a SIP request are not valid. To correct the cause of the event, ensure that password provisioned on the SIP phone matches the value provisioned in the BTS 10200.

Internet Protocol Security Connection Down—Security (3)

The Internet Protocol Security Connection Down alarm (major) indicates that the IP security engine is not running. To troubleshoot and correct the cause of the Internet Protocol Security Connection Down alarm, refer to the [“Internet Protocol Security Connection Down—Security \(3\)”](#) section on page 9-7.

Internet Protocol Security Media Terminal Adapter Key Establish Error—Security (4)

The Internet Protocol Security Media Terminal Adapter Key Establish Error event serves as a warning that the IPSEC MTA key establishment failed. The primary cause of the event is that a failure to establish the IPSEC keys to a given MTA using Kerberized key management protocol occurred. To correct the primary cause of the event, validate Kerberos provisioning and MTA device provisioning.

Internet Protocol Security Outgoing Security Association Not Found—Security (5)

The Internet Protocol Security Outgoing Security Association Not Found event serves as a warning that the KMS is unable to find a provisioned device to establish the needed SA. To correct the primary cause of the event, remove or modify the security policy which caused the ‘SA not found’ error.

Secure Session Initiation Protocol Endpoint Validation Failure—Security (6)

The Secure Session Initiation Protocol Endpoint Validation Failure event serves as a warning that a secure SIP endpoint validation failed. The primary cause of the event is that the BTS 10200 is incorrectly provisioned. To correct the primary cause of the event, check if correct value of **secure-fqdn** is provisioned in the BTS 10200 system. The secondary cause of the event is that the DNS is incorrectly provisioned. To correct the secondary cause of the event, verify resolution of **secure-fqdn** in the DNS. The tertiary cause of the event is that the CPE is incorrectly provisioned. To correct the tertiary cause of the event, verify the CPE provisioning to ensure that the correct source IP/contact being used.

Troubleshooting Security Alarms

This section provides the information needed to monitor and correct security alarms. [Table 9-3](#) lists all of the security alarms in numerical order and provides cross reference to each subsection in this section.

Table 9-3 *BTS 10200 Security Alarms*

Alarm Type	Alarm Name	Alarm Severity
SECURITY(3)	Internet Protocol Security Connection Down—Security (3)	MAJOR

Internet Protocol Security Connection Down—Security (3)

The Internet Protocol Security Connection Down alarm (major) indicates that the IP security engine is not running. The primary cause of the alarm is that the KMS has failed to establish the pf_key socket with the IPSEC engine. The alarm implies that the IPSEC engine is not running and that it may not be installed. To primary cause of the alarm, verify that IPSEC is installed and running in the kernel and reboot the platform. If problem persists or is recurrent, contact Cisco TAC.

**Note**

Refer to the [“Obtaining Documentation and Submitting a Service Request”](#) section on [page lvi](#) for detailed instructions on contacting Cisco TAC and opening a service request.

