



Cisco Intercompany Media Engine Alert Descriptions and Default Configurations

The following list comprises the Cisco Intercompany Media Engine alerts, their definitions, and default settings:

- [BannedFromNetwork](#), page H-1
- [IMEDistributedCacheCertificateExpiring](#), page H-2
- [IMEDistributedCacheFailure](#), page H-3
- [IMESdlLinkOutOfService](#), page H-3
- [InvalidCertificate](#), page H-4
- [InvalidCredentials](#), page H-5
- [MessageOfTheDay](#), page H-5
- [SWUpdateRequired](#), page H-6
- [TicketPasswordChanged](#), page H-6
- [ValidationsPendingExceeded](#), page H-7

BannedFromNetwork

This alert indicates that network administrators have banned this Cisco IME server from the network (IME distributed cache ring), making this Cisco IME service fully or partly inoperative. Network administrators rarely ban servers but do so if they detect that the server is being used to launch malicious attacks into the network. If you receive this alert in error, contact TAC immediately.

Default Configuration

Table H-1 *Default Configuration for the BannedFromNetwork Alert*

| Value | Default Configuration |
|--|---------------------------|
| Enable Alert | Selected |
| Severity | Alert |
| Enable/Disable this alert on the following servers | Enabled on listed servers |

Table H-1 *Default Configuration for the BannedFromNetwork Alert (continued)*

| Value | Default Configuration |
|----------------------|--|
| Threshold | Trigger alert when following condition met: Cisco IME service banned from network |
| Duration | Trigger alert immediately |
| Frequency | Trigger alert on every poll |
| Schedule | 24 hours daily |
| Enable Email | Selected |
| Trigger Alert Action | Default |

IMEDistributedCacheCertificateExpiring

This alert indicates the number of days that remain until the certificate that is used for the IME distributed cache expires. You must replace the certificate prior to expiration.

Default Configuration

Table H-2 *Default Configuration for the IMEDistributedCacheCertificateExpiring Alert*

| Value | Default Configuration |
|--|--|
| Enable Alert | Selected |
| Severity | Warning |
| Enable/Disable this alert on the following servers | Enabled on listed servers |
| Threshold | Trigger alert when following condition met: Cisco IME distributed cache certificate about to expire. 14 days. |
| Duration | Trigger alert immediately |
| Frequency | Trigger up to 1 alerts within 1440 minutes |
| Schedule | 24 hours daily |
| Enable Email | Selected |
| Trigger Alert Action | Default |

IMEDistributedCacheFailure

This alert indicates the health of the IME distributed cache. A value of zero (red) means that the IME distributed cache is suffering from a significant problem such as one of the following conditions:

- The Cisco IME cannot resolve issues after the network was partitioned. In this case, validation attempts may fail.
- The Cisco IME service is not connected to the network at all and is unable to reach the bootstrap servers.

A value of one (yellow) indicates that the Cisco IME network is experiencing minor issues, such as connectivity between bootstrap servers or other Cisco IME network issues. Check for any alarms that may indicate why this counter is 1. A value of two indicates that IME distributed cache is functioning normally and the system is considered healthy.

Default Configuration

Table H-3 *Default Configuration for the IMEDistributedCacheFailure Alert*

| Value | Default Configuration |
|--|---|
| Enable Alert | Selected |
| Severity | Alert |
| Enable/Disable this alert on the following servers | Enabled on listed servers |
| Threshold | Trigger alert when following condition met: IME distributed cache failure in states 1: network experience minor issues 0: network in trouble |
| Duration | Trigger alert immediately |
| Frequency | Trigger 1 alert within 60 minutes |
| Schedule | 24 hours daily |
| Enable Email | Selected |
| Trigger Alert Action | Default |

IMESdILinkOutOfService

This alert indicates that the Cisco IME service has lost communication with Cisco IME Config Manager services, such as Cisco AMC service or Cisco CallManager service.

This alert usually indicates that one of these services has gone down (either intentionally, for maintenance; or unintentionally, due to a service failure or connectivity failure).

Default Configuration**Table H-4** *Default Configuration for the IMESdLinkOutOfService Alert*

| Value | Default Configuration |
|--|---|
| Enable Alert | Selected |
| Severity | Critical |
| Enable/Disable this alert on the following servers | Enabled on listed servers |
| Threshold | Trigger alert when following condition met: SDLLinkOOS event generated |
| Duration | Trigger alert immediately |
| Frequency | Trigger alert on every poll |
| Schedule | 24 hours daily |
| Enable Email | Selected |
| Trigger Alert Action | Default |

InvalidCertificate

This alert indicates that the administrator enabled the IME distributed cache on the Cisco IME server but omitted the configuration of a valid certificate or configured an incorrect certificate.

Default Configuration**Table H-5** *Default Configuration for the InvalidCertificate Alert*

| Value | Default Configuration |
|--|---|
| Enable Alert | Selected |
| Severity | Alert |
| Enable/Disable this alert on the following servers | Enabled on listed servers |
| Threshold | Trigger alert when following condition met: Invalid certificate configured |
| Duration | Trigger alert immediately |
| Frequency | Trigger alert on every poll |
| Schedule | 24 hours daily |
| Enable Email | Selected |
| Trigger Alert Action | Default |

InvalidCredentials

The alert indicates that the Cisco Unified Communications Manager cannot connect to the Cisco IME server, because the username and password that are configured on Cisco Unified Communications Manager do not match those configured on the Cisco IME server.

The alert includes the username and password that were used to connect to the Cisco IME server as well as the IP address and name of the target Cisco IME server. To resolve this alert, log into the Cisco IME server and check that the username and password that are configured match those configured in Cisco Unified Communications Manager.

Default Configuration

Table H-6 Default Configuration for the InvalidCredentials Alert

| Value | Default Configuration |
|--|---|
| Enable Alert | Selected |
| Severity | Error |
| Enable/Disable this alert on the following servers | Enabled on listed servers |
| Threshold | Trigger alert when following condition met: Invalid or mismatched credentials. |
| Duration | Trigger alert immediately |
| Frequency | Trigger alert on every poll |
| Schedule | 24 hours daily |
| Enable Email | Selected |
| Trigger Alert Action | Default |

MessageOfTheDay

The Cisco IME service generates this alert when the administrators of the Cisco IME network have a message for you.

Default Configuration

Table H-7 Default Configuration for the MessageOfTheDay Alert

| Value | Default Configuration |
|--|--|
| Enable Alert | Selected |
| Severity | Notice |
| Enable/Disable this alert on the following servers | Enabled on listed servers |
| Threshold | Trigger alert when following condition met: Message from network administrators |

Table H-7 Default Configuration for the MessageOfTheDay Alert (continued)

| Value | Default Configuration |
|----------------------|---|
| Duration | Trigger alert immediately |
| Frequency | Trigger up to 1 alert within 1440 minutes |
| Schedule | 24 hours daily |
| Enable Email | Selected |
| Trigger Alert Action | Default |

SWUpdateRequired

The Cisco IME server generates this alert when a new version of the Cisco IME server software is required. This alert repeats until you perform the upgrade. To obtain more information about the software update, go to the Cisco website. You should install critical updates within days of receiving this alert.

These upgrades address security vulnerabilities or key functional outages. In some cases, if you do not apply a critical upgrade immediately, the Cisco IME server may become unable to connect to the network.

Default Configuration

Table H-8 Default Configuration for the SWUpdateRequired Alert

| Value | Default Configuration |
|--|---|
| Enable Alert | Selected |
| Severity | Warning |
| Enable/Disable this alert on the following servers | Enabled on listed servers |
| Threshold | Trigger alert when following condition met: Software update required |
| Duration | Trigger alert immediately |
| Frequency | Trigger up to 1 alerts within 60 minutes |
| Schedule | 24 hours daily |
| Enable Email | Selected |
| Trigger Alert Action | Default |

TicketPasswordChanged

The Cisco IME server generates this alert when the administrator changes the password that is used to generate the validation tickets.

Verify that an authorized administrator changed the password. Unauthorized changes may indicate compromise to the administrative interfaces on the Cisco IME service. If you determine that unauthorized changes have been made, change the administrative passwords on the Cisco IME server immediately to prevent further unauthorized access. To change the administrative password, type **set password admin** in the Cisco IME server CLI.

Default Configuration

Table H-9 Default Configuration for the TicketPasswordChanged Alert

| Value | Default Configuration |
|--|--|
| Enable Alert | Selected |
| Severity | Notice |
| Enable/Disable this alert on the following servers | Enabled on listed servers |
| Threshold | Trigger alert when following condition met: Ticket password changed |
| Duration | Trigger alert immediately |
| Frequency | Trigger on every poll |
| Schedule | 24 hours daily |
| Enable Email | Selected |
| Trigger Alert Action | Default |

ValidationsPendingExceeded

This alert indicates the number of pending validations on the Cisco IME server. This number provides an indicator of the backlog of work on the Cisco IME server.

Default Configuration

Table H-10 Default Configuration for the ValidationsPendingExceeded Alert

| Value | Default Configuration |
|--|---|
| Enable Alert | Selected |
| Severity | Critical |
| Enable/Disable this alert on the following servers | Enabled on listed servers |
| Threshold | Trigger alert when following condition met: Cisco IME pending validations exceeded 100 |
| Duration | Trigger alert immediately |
| Frequency | Trigger up to 1 alerts within 60 minutes |
| Schedule | 24 hours daily |

Table H-10 *Default Configuration for the ValidationsPendingExceeded Alert (continued)*

| Value | Default Configuration |
|----------------------|------------------------------|
| Enable Email | Selected |
| Trigger Alert Action | Default |