ORBEM Force Configuration Mode Commands

Attention

- With Release 21.16 onwards, the **force** keyword has to be appended to the **orbem** CLI command to enter the ORBEM mode and enable the feature. The **orbem** keyword is now hidden.
- Support for the end-of-life ORBEM/WEM feature will be fully discontinued in future releases.

The ORBEM Configuration Mode is used to manage the Object Request Broker Element Manager (ORBEM) server options for the current context.

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem force

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Important

The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Important

For information on common commands available in this configuration mode, refer to the Common Commands chapter.

- activate client id, on page 2
- client id, on page 2
- event-notif-iiop-port, on page 3
- event-notif-service, on page 4
- event-notif-siop-port, on page 16
- iiop-port, on page 17
- iiop-transport, on page 17
- iop-address, on page 18
- max-attempt, on page 19
- session-timeout, on page 19

- siop-port, on page 20
- ssl-auth-policy, on page 21
- ssl-certificate, on page 22
- ssl-private-key, on page 23

activate client id

Activates/deactivates a Common Object Request Broker Architecture (CORBA) client for the ORBEM interface.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

`[ no ] activate client id` *`name`*

no

Deactivates the specified client

id *name*

Specifies the client to be activated. *name* must refer to a previously configured CORBA client expressed as an alphanumeric string of 1 through 10 characters.

Usage Guidelines

Activates CORBA clients after they have been configured or deactivated by the system or by configuration.

Example

The following command activates the CORBA *ems* client.

```
activate client id ems
```

client id

Configures or removes a CORBA client from the ORBEM interface.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

```
client id name { encrypted password | password } pwd
no client id name
```

no

Removes the specified client from the configuration.

id *name*

Specifies the client to be configured. *name* must be an alphanumeric string of 1 through 10 characters.

encrypted password

Specifies the use of an encrypted password for use by the chassis while saving configuration scripts. Signifies that ORBEM messages are transported using SSL encryption techniques. StarOS displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

password

Specifies the plain text password for the CORBA client. *pwd* must be an alphanumeric string of 1 through 35 characters.

pwd

Specifies the password for the CORBA client.

For an encrypted password, *pwd* must be an alphanumeric string of 1 through 212 characters.

For an unencrypted password, *pwd* must be an alphanumeric string of 1 through 35 characters.

Usage Guidelines

Use this command to configure or remove a CORBA client from the ORBEM interface.

CORBA clients must be configured prior to being activated.

Example

The following command sets a plain text password for CORBA client *ems*:

```
client id ems password ems1001
```

event-notif-iiop-port

Configures the port number for Internet inter-ORB event notifications.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

event-notif-iiop-port *number*
default event-notif-iiop-port

default

Restores the port number for the inter-ORB event notifications to the system default: 7778.

number

Specifies the port number to use as an integer from 1 through 65535. Default: 7778

Usage Guidelines

Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for standardized inter-ORB communications.

Event notification port configured is only used if the Internet inter-ORB transport is enabled via the **iiop-transport** command with the event notification service being enabled as well.

Example

The following command sets the IIOP port number to 5466:

```
event-notif-iiop-port 5466
```

event-notif-service

Enables or disables the ORB Notification Service and allows the configuration of filters dictating which event notifications are sent.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

[no] event-notif-service [filter { event-id *event_id* **[to** *final_event_id* **] | facility** *event_facility* **level** *event_level* **}]**
default event-notif-service filter

default

Restores the ORB Notification Service filter to its default behavior of sending all "error" level and higher events, and "info" level events for the orbs facility, CLI command logs, and license change logs.

no

Disables the event notification service.

filter

Specifies a filter that determines for which events the system sends notifications.

event-id *event_id* [to *final_event_id*]

Specifies an event filter based on event identification (event ID) number.

event_id is a specific event ID to filter or is the initial event ID in range if the **to** keyword is used.

In 14.1 and earlier releases, *event_id* is an integer from 1 through 202699.

In 15.0 and later releases, *event_id* is an integer from 1 through 204999.

to allows the specification of a range of event IDs to filter. When used, *final_event_id* specifies the last event ID in the range to be filtered. It can be configured to an integer from 1 through 204999, but must be a value greater than the initial event ID.

facility *event_facility* level *event_level*

Specifies an event filter based on facility type and notification severity level.

event_facility specifies the facility type and can be any one of the following:

- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: Authentication, Authorization and Accounting (AAA) client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **aal2**: ATM Adaptation Layer 2 (AAL2) protocol logging facility
- **acl-log**: Access Control List (ACL) logging facility
- **acsctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: ACS Manager facility
- **afctrl**: Fabric Controller facility [ASR 5500 only]
- **afmgr**: Fabric Manager logging facility [ASR 5500 only]
- **alarmctrl**: Alarm Controller facility
- **alcap**: Access Link Control Application Part (ALCAP) protocol logging facility

- **alcapmgr**: ALCAP manager logging facility
- **all**: All facilities
- **asngwmgr**: Access Service Network (ASN) Gateway Manager facility
- **asnpcmgr**: ASN Paging Controller Manager facility
- **bfd**: Bidirectional Forwarding Detection (BFD) protocol logging facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bindmux**: IPCF BindMux-Demux Manager logging facility
- **bngmgr**: Broadband Network Gateway (BNG) Demux Manager logging facility
- **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
- **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
- **callhome**: Call Home application logging facility
- **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
- **cbsmgr**: Cell Broadcasting Service (CBS) logging facility [HNBGW]

Important In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

- **cdf**: Charging Data Function (CDF) logging facility
- **cgw**: Converged Access Gateway (CGW) logging facility
- **cli**: Command Line Interface (CLI) logging facility
- **cmp**: Certificate Management Protocol (IPSec) logging facility
- **connectedapps**: SecGW ASR 9000 oneP communication procotol
- **connproxy**: Controller Proxy logging facility
- **credit-control**: Credit Control (CC) facility
- **csp**: Card/Slot/Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: CSS RADIUS Signaling facility
- **cx-diameter**: Cx Diameter Messages facility [CSCF <--> HSS]
- **data-mgr**: Data Manager Framework logging facility
- **dcardctrl**: IPSec Daughter Card Controller logging facility

- **dcardmgr**: IPSec Daughter Card Manager logging facility
- **demuxmgr**: Demux Manager API facility
- **dgmbmgr**: Diameter Gmb Application Manager logging facility
- **dhcp**: Dynamic Host Configuration Protocol (DHCP) logging facility
- **dhcpv6**: DHCPv6
- **dhost**: Distributed Host logging facility
- **diabase**: Diabase messages facility
- **diactrl**: Diameter Controller proclet logging facility
- **diameter**: Diameter endpoint logging facility
- **diameter-acct**: Diameter Accounting
- **diameter-auth**: Diameter Authentication
- **diameter-dns**: Diameter DNS subsystem
- **diameter-ecs**: ACS Diameter signaling facility
- **diameter-engine**: Diameter version2 engine logging facility
- **diameter-hdd**: Diameter Horizontal Directional Drilling (HDD) Interface facility
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSec Data Path facility
- **drvctrl**: Driver Controller facility
- **dpath**: IPSec Data Path logging facility
- **drvctrl**: Driver Controller logging facility
- **doulosuemgr**: Doulos (IMS-IPSec-Tool) user equipment manager
- **eap-diameter**: Extensible Authentication Protocol (EAP) IP Sec urity facility
- **eap-ipsec**: Extensible Authentication Protocol (EAP) IPSec facility
- **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
- **ecs-css**: ACSMGR <-> Session Manager Signalling Interface facility
- **egtpc**: eGTP-C logging facility
- **egtpmgr**: enhanced GPRS Tunneling Protocol (eGTP) manager logging facility
- **egtpu**: eGTP-U logging facility
- **embms**: evolved Multimedia Broadcast Multicast Service facility
- **embms**: eMBMS Gateway Demux facility
- **epdg**: evolved Packet Data (ePDG) gateway logging facility

- **event-notif**: Event Notification Interface logging facility
- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility
- **fng**: Femto Network Gateway (FNG) logging facility
- **gbmgr**: SGSN Gb Interface Manager facility
- **gmm**:
  - For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)
  - For 3G: Logs the access application layer (above the RANAP layer)
- **gprs-app**: GPRS Application logging facility
- **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
- **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
- **gss-gcdr**: GTPP Storage Server GCDR facility
- **gtpc**: GTP-C protocol logging facility
- **gtpcmgr**: GTP-C protocol manager logging facility
- **gtpp**: GTP-prime protocol logging facility
- **gtpu**: GTP-U protocol logging facility
- **gtpumgr**: GTP-U Demux manager
- **gx-ty-diameter**: Gx/Ty Diameter messages facility
- **gy-diameter**: Gy Diameter messages facility
- **h248prt**: H.248 port manager facility
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task (HAT) process facility
- **hdctrl**: HD Controller logging facility
- **henbapp**: Home Evolved NodeB (HENB) App facility

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

- **henbgw**: HENB-GW facility

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

- **henbgw-pws**: HENB-GW Public Warning System logging facility

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

- **henbgw-sctp-acs**: HENB-GW access Stream Control Transmission Protocol (SCTP) facility

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

- **henbgw-sctp-nw**: HENBGW network SCTP facility

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

- **henbgwdemux**: HENB-GW Demux facility

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

- **henbgwmgr**: HENB-GW Manager facility

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

- **hnb-gw**: HNB-GW (3G Femto GW) logging facility

Important In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

- **hnbmgr**: HNB-GW Demux Manager logging facility

Important In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

- **hss-peer-service**: Home Subscriber Server (HSS) Peer Service facility
- **igmp**: Internet Group Management Protocol (IGMP)
- **ikev2**: Internet Key Exchange version 2 (IKEv2)
- **ims-authorizatn**: IP Multimedia Subsystem (IMS) Authorization Service facility
- **ims-sh**: HSS Diameter Sh Interface Service facility
- **imsimgr**: SGSN IMSI Manager facility
- **imsue**: IMS User Equipment (IMSUE) facility
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipms**: Intelligent Packet Monitoring System (IPMS) logging facility
- **ipne**: IP Network Enabler (IPNE) facility
- **ipsec**: IP Security logging facility
- **ipsecdemux**: IPSec demux logging facility
- **ipsg**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Services Gateway facility
- **ipsp**: IP Pool Sharing Protocol logging facility
- **kvstore**: Key/Value Store (KVSTORE) Store facility
- **l2tp-control**: Layer 2 Tunneling Protocol (L2TP) control logging facility
- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **lagmgr**: Link Aggregation Group (LAG) manager logging facility

- **lcs**: Location Services (LCS) logging facility
- **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
- **li**: Refer to the *Lawful Intercept Configuration Guide* for a description of this command.
- **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
- **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
- **local-policy**: Local Policy Service facility
- **location-service**: Location Services facility
- **m3ap**: M3 Application Part facility
- **m3ua**: M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway manager logging facility
- **map**: Mobile Application Part (MAP) protocol logging facility
- **megadiammgr**: MegaDiameter Manager (SLF Service) logging facility
- **mme-app**: Mobility Management Entity (MME) Application logging facility
- **mme-embms**: MME evolved Multimedia Broadcast Multicast Service facility
- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: MME Demux Manager logging facility
- **mmemgr**: MME Manager facility
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes
- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 logging facility
- **mpls**: Multiprotocol Label Switching (MPLS) protocol logging facility
- **mrme**: Multi Radio Mobility Entity (MRME) logging facility
- **mseg-app**: Mobile Services Edge Gateway (MSEG) application logging facility (This option is not supported in this release.)
- **mseg-gtpc**: MSEG GTP-C application logging facility (This option is not supported in this release.)
- **mseg-gtpu**: MSEG GTP-U application logging facility (This option is not supported in this release.)
- **msegmgr**: MSEG Demux Manager logging facility (This option is not supported in this release.)
- **mtp2**: Message Transfer Part 2 (MTP2) Service logging facility
- **mtp3**: Message Transfer Part 3 (MTP3) Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility

- **nas**: Non-Access Stratum (NAS) protocol logging facility [MME 4G]
- **netwstrg**: Network Storage facility
- **npuctrl**: Network Processor Unit Control facility
- **npudrv**: Network Processor Unit Driver facility [ASR 5500 only]
- **npumgr**: Network Processor Unit Manager facility
- **npumgr-acl**: NPUMGR ACL logging facility
- **npumgr-drv**: NPUMGR DRV logging facility
- **npumgr-flow**: NPUMGR FLOW logging facility
- **npumgr-fwd**: NPUMGR FWD logging facility
- **npumgr-init**: NPUMGR INIT logging facility
- **npumgr-lc**: NPUMGR LC logging facility
- **npumgr-port**: NPUMGR PORT logging facility
- **npumgr-recovery**: NPUMGR RECOVERY logging facility
- **npumgr-rri**: NPUMGR RRI (Reverse Route Injection) logging facility
- **npumgr-vpn**: NPUMGR VPN logging facility
- **npusim**: NPUSIM logging facility [ASR 5500 only]
- **ntfy-intf**: Notification Interface logging facility [Release 12.0 and earlier versions only]
- **ocsp**: Online Certificate Status Protocol logging facility.
- **orbs**: Object Request Broker System logging facility
- **ospf**: OSPF protocol logging facility
- **ospfv3**: OSPFv3 protocol logging facility
- **p2p**: Peer-to-Peer Detection logging facility
- **pagingmgr**: PAGINGMGR logging facility
- **pccmgr**: Intelligent Policy Control Function (IPCF) Policy Charging and Control (PCC) Manager library
- **pdg**: Packet Data Gateway (PDG) logging facility
- **pdgdmgr**: PDG Demux Manager logging facility
- **pdif**: Packet Data Interworking Function (PDIF) logging facility
- **pgw**: Packet Data Network Gateway (PGW) logging facility
- **pmm-app**: Packet Mobility Management (PMM) application logging facility
- **ppp**: Point-To-Point Protocol (PPP) link and packet facilities
- **pppoe**: PPP over Ethernet logging facility
- **proclet-map-frwk**: Proclet mapping framework logging facility
- **push**: VPNMGR CDR push logging facility

- **radius-acct**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Diameter Rf interface messages facility
- **rip**: Routing Information Protocol (RIP) logging facility [RIP is not supported at this time.]
- **rlf**: Rate Limiting Function (RLF) logging facility
- **rohc**: Robust Header Compression (RoHC) facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RANAP User Adaptation (RUA) [3G Femto GW - RUA messages] logging facility
- **s102**: S102 protocol logging facility
- **s102mgr**: S102Mgr logging facility
- **s1ap**: S1 Application Protocol (S1AP) Protocol logging facility
- **sabp**: Service Area Broadcast Protocol (SABP) logging facility
- **saegw**: System Architecture Evolution (SAE) Gateway facility
- **sbc**: SBc protocol logging facility
- **sccp:** Signalling Connection Control Part (SCCP) Protocol logging (connection-oriented messages between RANAP and TCAP layers).
- **sct**: Shared Configuration Task logging facility
- **sctp**: Stream Control Transmission Protocol (SCTP) Protocol logging facility
- **sef_ecs**: Severely Errored Frames (SEF) APIs printing facility
- **sess-gr**: SM GR facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs interface protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN "glue" interfaces (for example, between PMM, MAP, GPRS-FSM, SMS).

- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
- **sgsn-mbms-bearer**: SGSN Multimedia Broadcast/Multicast Service (MBMS) Bearer app (SMGR) logging facility
- **sgsn-misc**: Used by stack manager to log binding and removing between layers
- **sgsn-system**: SGSN System Components logging facility (used infrequently)
- **sgsn-test**: SGSN Tests logging facility; used infrequently
- **sgtpcmgr**: SGSN GTP-C Manager logging information exchange through SGTPC and the GGSN
- **sgw**: Serving Gateway facility
- **sh-diameter**: Sh Diameter messages facility
- **sitmain**: System Initialization Task main logging facility
- **sls**: Service Level Specification (SLS) protocol logging facility
- **sm-app**: SM Protocol logging facility
- **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
- **sndcp**: Sub Network Dependent Convergence Protocol (SNDCP) logging facility
- **snmp**: SNMP logging facility
- **sprmgr**: IPCF Subscriber Policy Register (SPR) manager logging facility
- **srdb**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
- **sscfnni**: Service-Specific Coordination Function for Signaling at the Network Node Interface (SSCF-NNI) logging facility
- **sscop**: Service-Specific Connection-Oriented Protocol (SSCOP) logging facility
- **ssh-ipsec**: Secure Shell (SSH) IP Security logging facility
- **ssl**: Secure Socket Layer (SSL) message logging facility
- **stat**: Statistics logging facility
- **supserv**: Supplementary Services logging facility [H.323]
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **tcap**: TCAP Protocol logging facility
- **testctrl**: Test Controller logging facility
- **testmgr**: Test Manager logging facility

- **threshold**: threshold logging facility
- **ttg**: Tunnel Termination Gateway (TTG) logging facility
- **tucl**: TCP/UDP Convergence Layer (TUCL) logging facility
- **udr**: User Data Record (UDR) facility (used with the Charging Service)
- **user-data**: User data logging facility
- **user-l3tunnel**: User Layer 3 tunnel logging facility
- **usertcp-stack**: User TCP Stack
- **vim**: Voice Instant Messaging (VIM) logging facility
- **vinfo**: VINFO logging facility
- **vmgctrl**: Virtual Media Gateway (VMG) controller facility
- **vmgctrl**: VMG Content Manager facility
- **vpn**: Virtual Private Network logging facility
- **wimax-data**: WiMAX DATA
- **wimax-r6**: WiMAX R6
- **wsg**: Wireless Security Gateway (ASR 9000 Security Gateway)
- **x2gw-app**: X2GW (X2 proxy Gateway, eNodeB) application logging facility
- **x2gw-demux**: X2GW demux task logging facility

event_level

specifies the severity level of the event notification to filter and can be configured to one of the following:

- critical: display critical events
- error: display error events and all events with a higher severity level
- warning: display warning events and all events with a higher severity level
- unusual: display unusual events and all events with a higher severity level
- info: display info events and all events with a higher severity level
- trace: display trace events and all events with a higher severity level
- debug: display all events

Usage Guidelines

This command is used to enable or disable the ORB Notification Service. Additionally, it can be used to configure filters dictating which events are sent. This service is disabled by default.

Filters can be configured for a specific event identification number (event ID), a range of event IDs, or specific severity levels for events for particular facilities.

When no filters are configured and the service is enabled, the ORB Notification Service sends all "error" level and higher events, and "info" level events for the orbs facility, CLI command logs, and license change logs.

Multiple instance of this command can be executed to configure multiple filters.

Example

The following command enables the ORB Notification service:

```
event-notif-service
```

The following command disables the ORB Notification service:

```
no event-notif-service
```

The following command configures a filter for the ORB Notification Service allowing only event IDs *800* through *805* to be sent:

```
event-notif-service filter event-id 800 to 805
```

The following command configures a filter for the ORB Notification Service allowing only *critical* level notifications for all facilities:

```
event-notif-service filter facility all level critical
```

event-notif-siop-port

Configures the port to use for secure socket layer (SSL) inter-ORB event communication.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

```
event-notif-siop-port number
default event-notif-siop-port
```

default

Restores the port to use for secure socket layer inter-ORB event communication to the system default: 7777.

number

Specifies the port number to use as an integer from 1 through 65535. Default: 7777

Usage Guidelines

Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for inter-ORB communications using SSL.

Example

```
event-notif-siop-port 25466
```

iiop-port

Configures the port number for Internet Inter-ORB Protocol (IIOP) communications.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

`[local]host_name(config-orbem)#`

Syntax Description **`[ no ] iiop-port`** *number*

default

Restores the port number for inter-ORB communications to the system default: 14132.

no

Disables the IIOP port.

number

Specifies the port number to use as an integer from 1 through 65535. Default: 14132

Usage Guidelines Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for standardized inter-ORB communications.

Internet inter-ORB port is only used if IIOP transport is enabled via the **iiop-transport** command.

Example

The following commands sets the IIOP port number to 2546:

```
iiop-port 2546
```

iiop-transport

Enables/disables use of the Internet Inter-ORB Protocol (IIOP) for management across the network.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

`[ no ] iiop-transport`

no

Disables internet inter-ORB protocol communication across the network.

Usage Guidelines

Enables the transport of IIOP messages to support remote management across the network.

The default is IIOP transport disabled.

Example

The following command enables ORB-based management across the network:

`iiop-transport`

iop-address

Sets the IP address used by the ORBEM Server to advertise service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

`[ default ] iop-address` *`ip_address`*

default

Restores the IP address for inter-ORB communications to the system default: IP address of the current context.

ip_address

Specifies the IP address to use for inter-ORB communications using IPv4 dotted-decimal notation.

Usage Guidelines

Change the inter-ORB IP address when the IP address of the current context should not be used. The IP address of the local context may not be appropriate when the ORB configuration across nodes would cause conflicts with the IP addresses.

The default inter-ORB IP address is the IP address of the current context.

Example

The following command sets the inter-ORB IPv4 address to 10.2.3.4:

```
iop-address 10.2.3.4
```

max-attempt

Configures the maximum number of failed login attempts after which the client is deactivated.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

max-attempt *count*
default max-attempt

default

Restores the maximum number of failed login attempts before which the client is deactivated to the system default: 3 attempts.

count

Specifies the number of failed login attempts prior to deactivating a client. The value must be an integer from 1 through 10. Default: 3 attempts

Usage Guidelines

Adjust the maximum number of attempts to a smaller value to increase the security level of the system.

Example

The following command sets the maximum number of attempts to 5:

```
max-attempt 5
```

session-timeout

Configures the amount of idle time (no activity) before a client session is terminated.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

session-timeout *seconds*
default session-timeout

default

Restores the amount of idle time (no activity) before a session is terminated to the system default: 300 seconds.

seconds

Specifies the number of seconds of idle time before a client session is terminated. The value must be must be an integer from 1 through 86400. Default: 300 seconds

Usage Guidelines

Reduce the session timeout when the maximum number of sessions allowed is frequently being reached. Setting this to a lower value will help release idle sessions faster to allow use by other clients.

Example

The following sets the session timeout value to 150 seconds:

```
session-timeout 150
```

siop-port

Configures the SSL I/O port for inter-ORB events.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

siop-port *number*
[default | no] siop-port

default

Restores the secure socket layer I/O port for inter-ORB events to the system default: 14131.

default

Restores the secure socket layer I/O port for inter-ORB events to the system default: 14131.

number

Specifies the port number to use as an integer from 1 through 65535. Default: 14131

Usage Guidelines

Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for inter-ORB communications.

Example

The following command sets the SIOP port number to 2466:

```
siop-port 2466
```

ssl-auth-policy

Configures the SSL peer authentication policy used by the ORBEM server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

`ssl-auth-policy { auth-none | auth-once | auth-once-fail | auth-peer | auth-peer-fail }`

auth-none

Specifies that the ORBEM server does not authenticate the peer. This is the default setting.

auth-once

Specifies that the ORBEM server authenticates the peer once (no fail).

auth-once-fail

Specifies that the ORBEM server authenticates the peer once (fail if no certificate).

auth-peer

Specifies that the ORBEM server authenticates the peer every time (no fail).

auth-peer-fail

Specifies that the ORBEM server authenticates the peer every time (fail if no certificate).

Usage Guidelines Use to configure the peer authentication policy used by the SSL transport of ORBEM.

Example

The following command sets the policy to authenticate the peer once without failure.

```
ssl-auth-policy auth-once
```

ssl-certificate

Defines the certificate to be used by the SSL transport of ORBEM.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description **ssl-certificate { string** *certificate* **| file** *url* **}**

string *certificate*

Specifies an ORBEM SSL certificate. *certificate* is an alphanumeric string of up to 4096 characters.

file *url*

Default: /usr/ssl/certs/orbscert.pem

Specifies an ORBEM SSL certificate file and location. *url* is an alphanumeric string of up to 1024 characters.

Usage Guidelines Use to configure the certificate to be used by the SSL transport of ORBEM. Note that if the **file** option is used, the certificate content is read from the *url* and converted into a quoted string.

Example

The following command defines the certificate *cert3.pem* file as being located in the **/usr/ssl/certs** directory:

```
ssl-certificate file /usr/ssl/certs/cert3.pem
```

The following command defines the certificate string (the string shown is abbreviated):

```
ssl-certificate string
```

"-----BEGIN CERTIFICATE-----\n\
MIIELDCCA5WgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBsTELMAkGA1UEBhMCVVMx\n\
FjAUBgNVBAgTDU1hc3NhY2h1c2V0dHMxEjAQBgNVBAcTCVRld2tzYnVyeTEeMBwG\n\
A1UEChMVU3RhcmVudCBOZXR3b3JrcyBJbmMuMSIwIAYDVQQLExlFbGVtZW50IE1h\n\
bmFnZW1lbnQgU3lzdGVtMQ4wDAYDVQQDEwVPUkJFTTEiMCAGCSqGSIb3DQEJARYT\n\
b3JiZW1AbnVsaW5raW5jLmNvbTAeFw0wMjA5MDYxMjE5MTNaFw0yMjA5MDExMjE5\n\
MTNaMIGxMQswCQYDVQQGEwJVUzEWMBQGA1UECBMNTWFzc2FjaHVzZXR0czESMBAG\n\
A1UdDgQWBBSpuGGMTwgaq8H+e70ZPIFHVZjiWDCB3gYDVR0jBIHWMIHTgBRkVBzy\n\
4zW5Gv0pXcwT07PtzCm53qGBt6SBtDCBsTELMAkGA1UEBhMCVVMxFjAUBgNVBAgT\n\
DU1hc3NhY2h1c2V0dHMxEjAQBgNVBAcTCVRld2tzYnVyeTEeMBwGA1UEChMVU3Rh\n\
cmVudCBOZXR3b3JrcyBJbmMuMSIwIAYDVQQLExlFbGVtZW50IE1hbmFnZW1lbnQg\n\
U3lzdGVtMQ4wDAYDVQQDEwVPUkJFTTEiMCAGCSqGSIb3DQEJARYTb3JiZW1AbnVs\n\
aW5raW5jLmNvbYIBADANBgkqhkiG9w0BAQQFAAOBgQATOdeDWikcoUIU8Gth9wr4\n\
Z5Fi8akXHhKhN7UMKyiW/Nn5NyfqPIA+9JwYMqwVOG8ybtfBQIGRCQodbXUm6Z9Z\n\
cM3XxWKVKHVolGS83f/JfpSLnuGkBIW8m3p/snHBH2BtgNT8OLItlTdBHedTKL72\n\
ZIxGF9/ok9hUqU4ikzQcEQ==\n\
-----END CERTIFICATE-----\n"

ssl-private-key

Configures the SSL private key used by the ORBEM server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

ssl-private-key { string *key* **| file** *url* **}**

string *key*

Specifies an ORBEM SSL private key. *key* is an alphanumeric string of up to 4096 characters.

file *url*

Default: /usr/ssl/certs/orbscert.pem

Specifies the ORBEM SSL private key file location. *url* is an alphanumeric string of up to 1024 characters.

Usage Guidelines

Use to configure the private key for the SSL transport of ORBEM. Note that if **file** option is used, the private key is read from the *url* and converted into a quoted string.

Example

The following command defines the private-key *cert3.pem* file as being located in the **/usr/ssl/certs** directory:

```
ssl-private-key file /usr/ssl/certs/cert3.pem
```

The following command defines the private-key string (the string shown is abbreviated):

```
ssl-private-key string
```

"-----BEGIN RSA PRIVATE KEY-----\n\

MIICXQIBAAKBgQC6Dh79iaK/zZG/Kwme2XS6G8/n3/+sac6huxI1WNyammyYZKZp\n\

XTjHUlS92fvn0UUM4tFjN4XoqveSiqy3IqUhnVKS3+0L7s9beanQUJuR9MdLy9Ho\n\

7qh720wpN4isqN7YfGLoqGslLQjhS8z6ZT0ZUhyusY0rE6yHTV23nHKNtQIDAQAB\n\

9br1iVWvy/N23WXwZIiH+e1tBfHqlSd/0wJBANEEOgH/vJse/YdHeYjlT76IcGRp\n\

Tq6ldBXdoLRDGUF2AqdboJ7wWCOJQO34XbBtmWFfTkqz48Mi6uh3/5kDfH8CQGAl\n\

XObwPFRztvkXprZfh7IekxAIuoHiT1JsEKSIGPzEqDY2rmoWDghOvPETO+5zWEQk\n\

TXzLaRHgbIy9MKnXSt8CQQCcBfT7VndEfG9VWyPzeL4vx4ZhUMZQ6FIJdXo7Xq9x\n\

mzX8hgIcfdg3tahlNt35gL/DjUY7d14+MgLrRf3Udbk9\n\

-----END RSA PRIVATE KEY-----\n"