Zone - IP Peer - CLI

In this section:

Related articles:

- Surrogate Registration Support.
- Surrogate Registration Profile - CLI
- Crankback Profile - CLI
- Egress IP Attributes - SIP - CLI
- SIP Trunk Group - Signaling - CLI

Use this object to configure an IP Peer for a particular zone.

Note
If an IP Peer is configured to use an FQDN port (other than port 5061), the SBC increments the configured port number by 1 and uses it as the new port number for SIP over TLS signaling. If the IP Peer is configured to use port 5061 and the transport is TLS, no changes are made to the configuration.

IP Peer

Command Syntax

```
% set addressContext <name> zone <name> ipPeer <peer name>
 authentication
  intChallengeResponse <disabled | enabled>
  incInternalCredentials <disabled | enabled>
 defaultForIp <false | true>
 ipAddress <IP address>
 ipPort <0-65535>
 pathCheck (See Patch Check section below for details)
 policy
  description <description>
  ipSignalingProfile <profile name>
  packetServiceProfile <profile name>
  sip
   fqdn <fqdn>
   fqdnPort <0-65535>
 sip cacProfile <profile name>
 sipResponseCodeStats <enabled|disabled>
    surrogateRegistration (See Surrogate Registration section below for details)
```

Command Parameters

Table 1: Zone IP Peer Parameters

Parameter	Length/Range	Description

`<peer name>`	1-23 characters	The name of the IP Peer.

`authentication`	N/A	Use this object to support local authentication autonomously on a per-IP trunk group basis in situations where an IP-PBX does not perform a registration and the service provider does not require/want registrations (see IP Trunk Group Authentication additional feature functionality).
		• `intChallengeResponse` – Enable this flag on the ingress IP Peer to allow the SBC to reply to local authentication challenges autonomously. If this flag is disabled, the SBC will not reply to authentication challenges locally even if credentials are configured on the egress IP Trunk Group (IPTG).
		  • `disabled` (default)
		  • `enabled`
		• `incInternalCredentials`– Enable this flag on the ingress IP Peer to allow egress IPTG authentication to be internally created using the authorization information in mid-dialogue without being challenged.
		  • `disabled` (default)
		  • `enabled`
		NOTE: If intChallengeResponse is disabled, incInternalCredentials is not used.
		NOTE: If IPTG authentication is configured for both ingress IPTG and IP Peer, the IP Peer configuration takes precedence. If you wish to use the flags configured on IPTG, the IP Peer must not be present in the configurations. Otherwise, the IP Peer flags default to 'disabled' state and take precedence over IPTG flags.

`defaultForIp`	N/A	Set flag to “true” to use this peer for the ipAddress and ephemeral port on ingress. • `false` (default) • `true`
`ipAddress`	IPv4/IPv6 format	The IPv4 or IPv6 address of the Peer.
`ipPort`	0-65535	The TCP/UDP port for this peer. (default = 0)
`pathCheck`	N/A	Use this parameter to define Options ping settings. (See Path Check Parameters table below for details)

policy	N/A	Use this parameter to specify policy parameters and profiles associated with this IP peer.
		• description – IP peer policy description.
		• ipSignalingProfile – The IP signaling profile name.
		• packetServiceProfile – Packet service profile name.
		• sip – Use this parameter to specify SIP FQDN and FQDN port for IP peer policy.
		  • fqdn <string> – The FQDN used to send egress calls or requests to this peer. (range: 1-63 characters).
		  • fqdnPort – Specify the FQDN port. (range: 0-65535).

sip	N/A	Use this parameter to specify the SIP endpoint CAC profile for the IP peer using . • cacProfile – SIP endpoint CAC profile for the IP peer.
sipResponseCodeStats	N/A	Option to enable or disable collection of SIP response code statistics for an IP peer. Possible values: • disabled (default) • enabled
surrogateRegistration	N/A	Use this parameter to configure the SBC to act as a surrogate registration entity between a non-registering IP PBX or SIP UA and REGISTRAR (which mandates registration) for this IP Peer. Do not use FQDN format when configuring a Surrogate Peer. When configuring surrogate registration, be sure to set the expires value of ingress trunk group toward IAD to the maximum default value of “3600”. (See Surrogate Registration Parameters table below for details.)

Path Check

Command Syntax

```
% set addressContext <name> zone <name> ipPeer <peer name> pathCheck
 hostName <peer FQDN>
 hostPort <0-65535>
 profile <Path Check Profile name>
 state <disabled | enabled>
 statusUpdateSupport <disabled | enabled>
```

Command Parameters

Table 2: Path Check Parameters

Parameter	Length/Range	Description
`hostName`	1-63 characters	`<FQDN of the peer>` – This is resolved using DNS, and the resulting servers are pinged using SIP OPTIONS requests.
`hostPort`	0-65535	`<TCP/UDP port number of the peer>` (Default = 5060) – The peer's servers are pinged using SIP OPTIONS requests at this port. When the pathCheck profile is attached to an FQDN-based IP peer with `hostPort` set to `0`, the `pathCheck` task performs SRV lookup to resolve the port numbers. The resolved port numbers are used to send OPTIONS ping to the IP peer. If FQDN-based IP peer is configured with a `hostPort` set to a value other than 0. the `pathCheck` task does not perform SRV lookups. It instead uses the configured port to send OPTIONS ping to the IP peer.
`profile`	0-23 characters	`<profile name>` – The Path Check profile name used when pinging this peer (OPTONS ping).
`state`	N/A	Use this flag to enable/disable active pinging. • `disabled` (default)` • `enabled`
`statusUpdateSupport`	N/A	Enable this flag to provide Options-based status update support. • `disabled` (default) • `enabled` **NOTE**: If `ipAddress/ipPort` is configured and `pathCheck` needs to be enabled for that `ipAddress/ipPort`, ensure `hostName/hostPort` is not configured. **NOTE**: Status updates only apply when new calls are sent to a peer. They do not impact messages belonging to existing calls or new calls received from the peer.

Status updates are sent/received under the following conditions:

Table 3: Status Update Conditions

Status Update is sent by:	When:
Peer	Peer restarts
Peer	Peer is manually blocked
Peer	Peer's congestion state changes (this update is ignored by SBC)
SBC	Peer has restarted indicating it is ready to receive calls
SBC	Peer is manually blocked in SBC

Surrogate Registration

Command Syntax

```
% set addressContext <name> zone <name> ipPeer <peer name> surrogateRegistration
 authUserName <user name [string up to 127 characters]>
 hostPart <1-63 characters>
 regAuthPassword <DES3 encrypted string>
 retryTimer <50-10000000 milliseconds>
 sendCredentials <challengeForAnyMessage | challengeForAnyMessageAndInDialogRequests |
challengeForRegister>
 state <disabled | enabled>
 suppressRegRetryAfterAuthFail <disabled | enabled>
 surrRegProfile <profile name>
 useNextSurrRegForCall <disabled | enabled>
 useUserNameAsPAI <disabled | enabled>
 userPart <user part for surrogate registration>
```

Command Parameters

Table 4: Surrogate Registration Parameters

Parameter	Length/Range	Description
`authUserName`	1-127 characters	`<name>` – Authorization User Name for surrogate registration.
`hostPart`	1-63 characters	`<host name>` – This assigned name is used as a hostname of RURI, FROM, TO headers of all outgoing calls.
`regAuthPassword`	1-32 characters	`<password>` – DES3 (triple Digital Encryption Standard) encrypted string authentication password for surrogate registration. All ASCII characters from 33 to 126 (except 34 - double quotes) are allowed. SBC users "Admin" and "Operator" have full access to surrogate registration passwords. **NOTE**: If regAuthPassword contains ASCII characters, enclose the entire password string with " " (double quotes). `% set addressContext default zone ZONE1 ipPeer basu surrogateRegistration userPart 452613 regAuthPassword "123456789012345678901234O\!$$@#$!@#!@#!@#"` **NOTE**: "Field Service" and "Guest" users do not have access to `regAuthPassword` field.
`retryTimer`	50-10000000	`<#>` – The time, in milliseconds, after which the REGISTRATION is retried after a failure. When a Registration or Refresh-Registration for a peer fails (except 403 message – see Surrogate Registration Criteria below), the retry timer is initiated. Upon expiry, a new Registration for the peer is attempted. (Default = 900000 ms, which equates to 15 minutes).

sendCredentials	N/A	Use this parameter to control how credentials are sent on receiving a challenge from AS for methods REGISTER, INVITE,PRACK, REINVITE, UPDATE and BYE. • challengeForAnyMessage – The SBC sends credentials for REGISTER, INVITE, PRACK, UPDATE, REINVITE and BYE when these messages are challenged. • challengeForAnyMessageAndInDialogRequests – The SBC sends credentials for REGISTER, INVITE, PRACK, UPDATE, REINVITE and BYE when these messages are challenged. The SBC also sends credentials by default as per last challenge in the in-dialog requests such as PRACK, UPDATE, REINVITE and BYE when any one of these methods is challenged earlier in the call. • challengeForRegister (default) – The SBC sends credentials only for REGISTER when challenged. Challenges for any other messages are returned to the IP-PBX.
state	N/A	Use this flag to disable/enable surrogate registration on IP peer. • disabled (default) • enabled
suppressRegRetryAfterAuthFail		Use this flag to control the sending of registration retries when a REGISTER with credentials is challenged (with stale true and realm is identical to previous realm received). When stale = true or realm is not identical to previous realm received, the SBC immediately sends REGISTER. • disabled (default) – Send REGISTER when a 401 or 407 in response to REGISTER with credentials is received. • enabled – Do not attempt to send REGISTER after receiving a 401 or 407 response.
surrRegProfile	1-23 characters	<profile name> – Surrogate registration profile name. To establish a Surrogate Registration Profile, refer to Surrogate Registration Profile - CLI page.
useNextSurrRegForCall	N/A	Enable this flag to use the next available pilot number to resend the INVITE. • disabled (default) • enabled **NOTE**: If using this flag, be sure to configure Crankback profile for 4xx (403) response (refer to Crankback Profile - CLI page for details).
useUserNameAsPAI	N/A	Enable this flag to use the configured userName in surrogateRegistraion as userName in the outgoing INVITE. • disabled (default) • enabled **NOTE**: Because this flag sends PAI in outgoing INVITE, the includePrivacy flag must be disabled (refer to Egress IP Attributes - SIP - CLI page to disable flag).

`userPart`	1-127 characters	`<userpart identity>` – User part name for the IP-PBX/SIP UA for which surrogate registration is being enabled. This is a mandatory parameter. Any character in ABNF format is allowed except a semi-colon (;). **NOTE**: Refresh REGISTER and De-REGISTER are always sent without credentials. If such a REGISTER is challenged, then SBC responds with a new REGISTER with credentials. **NOTE**: The SBC mirrors the credentials to the standby of an HA System. If the `sendCredentials` is set to 'challengeForAnyMessageAndInDialogRequests', upon a switchover the SBC can send in-dialog requests such as REINVITE/UPDATE/BYE with credentials.

Surrogate Registration Criteria

1. When configuring surrogate registration, be sure to set the expires value of ingress trunk group toward IAD to the maximum default value of “3600”.
2. If "surrogateRegistration" is enabled, you must first disable it before modifying regAuthPassword, retryTimer, userPart, authUserName, surrRegProfile, sendCredentials or suppressRegRetryAfterAuthFail parameters.
3. The "requireRegistration" flag must be set to ‘supported-group’ for the IP Peer on which surrogate registration functionality is being enabled (refer to SIP Trunk Group - Signaling - CLI).
4. If a "403 Forbidden" error response is received in response to Registration/Re-registration for a surrogate IP peer, the SBC generates the alarm sonusSbxSurrRegRegistrationFailedNotification and halts further registration for this particular IP Peer. The operator must disable/enable the surrogate registration flag to generate surrogate registration for this IP Peer.
5. If Pass-through registration exists for an IP peer on which surrogate registration is being enabled, the surrogate registration fails and the above alarm is generated. Once Pass-through registration expires, the operator must disable/enable the surrogate registration flag to generate surrogate registration for this IP Peer. Likewise, if surrogate registration exists and Pass-through register is received for the same IP peer, then Pass-through register is rejected (no alarm is generated - check 403 response for reason). The operator must disable surrogate registration to allow Pass-through registration to be successful.
6. If RAC limit is set on the trunk group associated with the IP Peer configured for surrogate registration, you must configure the SIP cause map ‘regTGLimit’ to point to 503 error instead of 403.
7. On enabling the surrogateRegistration state of a Peer, a random timer between 1 to 60 seconds is started and a Register request is sent to avoid a Register avalanche.
8. The SIP Signaling Port must allow transport protocol UDP in order to use surrogate registration. The surrogate task communicates on UDP with other internal SBC tasks.
9. Following a switchover in a redundant system, the SBC sends a new surrogate REGISTER for all IP Peers which are reachable and have surrogate registration enabled.
10. A request from a surrogate peer with a short-lived TCP port is not supported.
11. To allow originating calls from non-pilot numbers behind an IP-PBX, set "validateAor" flag to "disabled". If enabled, only calls from the

AOR configured as surrogate registration username are allowed (refer to SIP Trunk Group - Signaling - CLI).

Command Examples

The following examples demonstrate how to configure, enable and disable surrogate registration.

> **Note**
> Be sure to issue the 'commit' command after configuring surrogate peer and before enabling surrogate registration. Otherwise, an error will occur.

Configure Peer for surrogate registration:

```
set addressContext PKT0_ADDR_CONTEXT_1 zone PKT0_TG1 ipPeer SURR_PEER1 ipAddress 10.32.241.2 ipPort
12020 surrogateRegistration userPart SURR_REG_PEER1 retryTimer 5 regAuthPassword
12345678901234567890123456789O
commit
```

Enable surrogate registration:

```
set addressContext PKT0_ADDR_CONTEXT_1 zone PKT0_TG1 ipPeer SURR_PEER1 surrogateRegistration state
enabled
commit
```

Disable surrogate registration:

```
set addressContext PKT0_ADDR_CONTEXT_1 zone PKT0_TG1 ipPeer SURR_PEER1 surrogateRegistration state
disabled
commit
```