ASM Adaptations

Adaptations are Case Sensitive

fromto The From and To headers are only modified by adaptation if the fromto module parameter is present and has the value of true. See Adaptation Module Administration below.

adaptForeignURI In Session Manager, Request-URI and To headers are not adapted on ingress if the host part of the URI is an IP address that is different from the IP address of the Session Manager. If required, the new adaptation module parameter adaptForeignURI can be added to provide the earlier adaptation behavior prior to that of Session Manager 6.2 release.

keepPortTransport All adaptations strip the port and transport from the Request-URI if the host-part is adapted on egress. This behavior can be overridden with the keepPortTransport parameter.

multipartMIMEsupported This option can be abbreviated to MIME. This option is applicable to egress processing only. If the parameter is set to no , the multipart MIME message bodies are stripped on egress from Session Manager. If the multipart MIME message contains an SDP message body, the message body will be inserted as the only message body in the outgoing message. If omitted or set to any other value, the message bodies will not be modified.

adaptForeignURI If the value is set to true, the INGRESS adaptation is applied to the Request-URI and to the header if the fromto parameter is set, even if the host part is an IP address that is different from the IP address of the Session Manager.

noidtmf: If the value is set to true, no DTMF message body conversion is performed on ingress.

dtmf The value of this parameter determines the DTMF message body format that is desired on egress from the Session Manager . If omitted, no conversion is done. Supported values are nortel, relay, and dtmf.

keepPortTransport If this parameter is present and set to any value, Session Manager does not strip the port and transport when the domain of the Request-URI is modified on egress.

noar This parameter requires a comma-separated list of SIP response codes. This parameter is applicable to the egress adaptation only. You can use this parameter to override the default alternate routing behavior of Session Manager. Session Manager does not alternate route a request to the next SIP Entity if it receives one of the responses listed in the parameter value. An example of a comma-separated list is noar = 404,486.

sessionTimeout Use this parameter for SIP entities that do not support the session timer, as per RFC 4028, or to send periodic SIP messages to keep the session active for more than one hour. If both entities use the session timer in a call, Session Manager keeps the session active for the negotiated interval. If the entities do not use the session timer in a call, then Session Manager keeps the session active for one hour after the last SIP transaction. In such cases, you can set this parameter (in seconds) to extend the one hour interval. For example, if the session timer is not used, the parameter value of sessionTimeout=7200 makes the session stay in memory for 7200 seconds (120 minutes) after the last SIP message exchange.

noallow This parameter requires a comma-separated list of SIP methods. The system strips the methods from the Allow header on egress. Method names are case-insensitive. For example,

noallow=UPDATE and noallow=UPDATE,OPTIONS.

iRHdrs Remove the specified header or headers during adaptation process from messages in the ingress direction. Separate multiple headers with a comma. For example, P-Charging-Vector,P-Location. Header names are case-insensitive. The administrator can remove the headers that Session Manager may add during post adaptation module invocation, for example, P-Location.

eRHdrs Remove the specified header or headers during adaptation process from messages in the egress direction. Separate multiple headers with a comma. For example, P-Charging-Vector,P-Location. The administrator can remove the headers that Session Manager may add during post adaptation module invocation, for example, P-Location.

reduceRtHdrs The intermediate element adds routing headers when the SIP messages move from one element to other. To reduce the number of routing headers values from the SIP message, use the reduceRtHdrs parameter. If you set the value of reduceRtHdrs to true, the system reduces the number of routing headers values, such as Via and Record-Route from the SIP message. However, all the outgoing messages from Session Manager will have the Via and Record-Route header with values of Session Manager IP and transport so that all the responses and subsequent requests for that call can be delivered to Session Manager.

reduceRtHdrs The reduceRtHdrs parameter is introduced in Session Manager, to enable the Routing Header Compression feature.

addRouteHdrs This parameter adds the indicated Route headers to outgoing requests to the entity for dual-Route header support required by Assured Services SIP interface to SoftSwitch. The addRouteHdrs parameter is used in DOD networks to route calls between ESC and LSC utilizing SoftSwitch. The addRouteHdrs values must be added within quotation marks. Multiple values must be separated with a comma. For example
“<sip:10.129.177.129:5061;transport=tcp;lr>,<sip:10.133.177.129:5061;transport=tcp;lr>”

EGRESS Domain Modification parameters

The EGRESS Domain Modification parameters are:

overrideDestinationDomain (can be abbreviated to odstd):By default, this is the first parameter. The Adaptation module replaces the domain in Request-URI, To header (if administered), Refer-To header, and Notify/message-summary body with the given value for egress only. If the request is a REFER, the domain in the Refer-To header will only be modified if it is the IP address of the Session Manager or a domain for which the Session Manager is authoritative.

overrideSourceDomain (may be abbreviated to osrcd): The Adaptation module replaces the domain in the From header (if administered), P-Asserted-Identity header and calling part of the History-Info header with the given value for egress only. The Module Parameter:osrcd=dr.avaya.com odstd=ny.avaya.com is the same as the verbose form overrideSourceDomain=dr.avaya.com overrideDestinationDomain=ny.avaya.com.

INGRESS Domain Modification parameters

The INGRESS Domain Modification parameters are:

ingressOverrideDestinationDomain (can be abbreviated to iodstd): Adaptation module replaces the domain in Request-URI, To header (if administered), and Notify/message-summary body with the given value for ingress only. If the request is a REFER, the domain in the Refer-To header will only be

modified if it is the IP address of the Session Manager or a domain for which the Session Manager is authoritative.

ingressOverrideSourceDomain (can be abbreviated to iosrcd): Adaptation module replaces the domain in the From header (if administered), P-Asserted-Identity header and calling part of the History-Info header with the given value for ingress only.

EGRESS Display Name Modification

egressDisplayName : In Session Manager, if this parameter is present, the adaptation module modifies the display name of the Contact, P-Asserted-Identity, and From/To headers (if fromto = true is specified) of the egress messages.

For outgoing calls, the adaptation module applies the adaptation to the P-Asserted-Identity, Contact, and From headers in both the initial dialog-creating request sent from the Session Manager and in all subsequent in-dialog requests.

For incoming calls, the adaptation module applies the adaptation to the P-Asserted-Identity, Contact, and To headers. If the value of the parameter contains spaces, then the value must be enclosed in double quotes. Additionally, any double quotes that are part of the parameter value must be preceded by a backslash character.

Example values for the egressDisplayName parameter are:

egressDisplayName=SomeCallingName

egressDisplayName=“My Business”

egressDisplayName=“The \”Best\“ Business”