APPENDIX B

# Environment Dictionary

This appendix describes the environment variables the scripts use to communicate with Cisco Access Registrar or to communicate with other scripts.

Cisco Access Registrar sets the **arguments** variable in the Environment dictionary, before calling the **InitEntryPoint** of each script. The **arguments** variable is set to the value of the **InitEntryPointArgs** property corresponding to that script, and it allows the administrator to pass (possibly unique) information to each script initialization function.

Environment variables that are set and read for resource management override provide scripts further control over session management. These environment variables, including the following **Acquire-User-Session-Limit**, **Acquire-Group-Session-Limit**, **Acquire-IP-Dynamic**, **Acquire-IP-Per-NAS-Port**, **Acquire-IPX-Dynamic**, and **Acquire-USR-VPN**, can be set at any point before session management is invoked. These environment variables are read as the packet flows through each Resource Manager that the chosen Session Manager calls. The default setting for these environment variables is TRUE. See the "Resource Managers" section on page 3-14 for additional information about Resource Managers.

# Cisco Access Registrar Environment Dictionary Variables

The following variables are text strings stored in the Environment dictionary passed to each scripting point.

## Accepted-Profiles

**Accepted-Profiles** is read during authorization after calling server and client incoming scripts (not set by CAR code). If set, the authorization done by local user lists checks to see if the given user's profile as specified in the user record is one of those in the separated list of profiles. If it is not in the separated list of profiles, the request is rejected.

## Accounting-Service

**Accounting-Service** is set after calling server and client incoming scripts and is used to determine which accounting service is used for this request. If set, the server directs the request to be processed by the specified accounting service.

When **Accounting-Service** is not set, the **DefaultAccountingService** (as defined in the server configuration) is used instead.

## Acquire-Group-Session-Limit

**Acquire-Group-Session-Limit** is set and read for resource management override.
**Acquire-Group-Session-Limit** is set to FALSE to override the use of group session limit resource management.

## Acquire-IP-Dynamic

**Acquire-IP-Dynamic** is set and read for resource management override. **Acquire-IP-Dynamic** is set to FALSE to override the use of a managed pool of IP addresses resource management.

## Acquire-IPX-Dynamic

**Acquire-IPX-Dynamic** is set and read for resource management override. **Acquire-IPX-Dynamic** is set to FALSE to override the use of a managed pool of IPX addresses resource management.

## Acquire-IP-Per-NAS-Port

**Acquire-IP-Per-NAS-Port** is set and read for resource management override.
**Acquire-IP-Per-NAS-Port** is set to FALSE to override the use of ports associated with specific IP addresses resource management.

## Acquire-Subnet-Dynamic

**Acquire-Subnet-Dynamic** is not always used. If set to FALSE, subnet-dynamic resource managers are skipped.

## Acquire-User-Session-Limit

**Acquire-User-Session-Limit** set and read for resource management override.
**Acquire-User-Session-Limit** is set to FALSE to override the use of user session limit resource management.

## Acquire-USR-VPN

**Acquire-USR-VPN** is set and read for resource management override. **Acquire-USR-VPN** is set to FALSE to override the use of Virtual Private Networks (VPNs) that use USR NAS Clients resource management.

## Allow-Null-Password

**Allow-Null-Password** is read during password matching and set in local userlist password matching if not set prior. If **Allow-Null-Password** is set to TRUE, the CAR server accepts requests with null passwords.

## Authentication-Service

**Authentication-Service** is set and read for authentication service selection and is used to determine which service is used to authenticate the user. If set, the server directs the request to be processed by the specified authentication service. When **Authentication-Service** is not set, the **DefaultAuthenticationService** is used instead.

## Authorization-Service

**Authorization-Service** is set and read for authorization service selection and is used to determine which service to use to authorize the user. If set, the server directs the request to be processed by the specified authorization service. When **Authorization-Service** is not set, the **DefaultAuthorizationService** is used instead.

## Current-Group-Count

**Current-Group-Count** is set and read for group session management. If set, the group-session-limit resource manager sets **Current-Group-Count** to be the new value of the group-session-limit counter.

## Dynamic-Search-Path

**Dynamic-Search-Path** is read for LDAP searching. If set, the server uses it as its LDAP search path rather than the value set in the remote server configuration.

## Group-Session-Limit

**Group-Session-Limit** is set and read for group session management. The group-session-limit resource manager sets this environment variable to be the limit of the group-session-limit counter as set by the configuration.

## Ignore-Accounting-Signature

**Ignore-Accounting-Signature** is set after calling server and client incoming scripts and is used to ignore missing or incorrect accounting signatures from NASs. If set, Cisco Access Registrar does not check whether the account request packet has been signed with the same shared secret as the NAS.

**Ignore-Accounting-Signature** is used to work with RADIUS implementations that did not sign Accounting-Requests. A script was provided in the distribution (for USR NASs) that could be set in the IncomingScript extension point for the USR Vendor that simply set this environment variable.

## Incoming-Translation-Groups

**Incoming-Translation-Groups** is read for authentication. If set, **Incoming-Translation-Groups** specifies the translation groups to be used to filter attributes on requests.

# Misc-Log-Msg-Info

**Misc-Log-Msg-Info** is read for packet event logging. If a log message is generated, the value of **Misc-Log-Msg-Info** is inserted into the middle of the log message.

# PAGER Environment Variable

The **aregcmd** command supports the **PAGER** environment variable. When the **aregcmd** command **stats** is used and the **PAGER** environment variable is set, the output of the **stats** command is displayed using the program specified by the **PAGER** environment variable.

# Reject-Reason

**Reject-Reason** is set when a request is being rejected and contains the **Reject-Reason**. Cisco Access Registrar uses the value of **Reject-Reason** to look up the reject reason in the reply message table.

If **Reject-Reason** is set to one of: UnknownUser, UserNotEnabled, UserPasswordInvalid, UnableToAcquireResource, ServiceUnavailable, InternalError, MalformedRequest, ConfigurationError, IncomingScriptFailed, OutgoingScriptFailed, IncomingScriptRejectedRequest, OutgoingScriptRejectedRequest, or TerminationAction, then the value set in the configuration under **/Radius/Advanced/ReplyMessages** will be returned.

# Remote-Server

**Remote-Server** is set and read for logging a rejected packet from a remote server. **Remote-Server** records the name and IP address of the remote server to which the request has been forwarded.

# Request-Authenticator

**Request-Authenticator** is set for every packet upon reception. Getting the **Request-Authenticator** from a script returns the value of the request authenticator.

# Request-Type

**Request-Type** is set when a request is first received to the type of request, such as one of Access-Request, Access-Accept, Access-Reject, Accounting-Request, Accounting-Response, or Access-Challenge before calling any extension points.

The request contains a string representation of the RADIUS packet type (code). When Cisco Access Registrar does not recognize the packet type, it is represented as “Unknown-Packet-Type-<*N*>, where <*N*> is the numeric value of the packet type (for example “Unknown-Packet-Type-9). The known packet types are listed in Table B-1.

*Table B-1 Request-Type Packets*

| String | Packet Code |
|---|---|
| Access-Request | (1) |
| Access-Accept | (2) |
| Access-Reject | (3) |
| Accounting-Request | (4) |
| Accounting-Response | (5) |
| Access-Challenge | (11) |
| Status-Server | (12) |
| Status-Client | (13) |
| USR-Resource-Free-Request | (21) |
| USR-Resource-Free-Response | (22) |
| USR-Resource-Query-Request | (23) |
| USR-Resource-Query-Response | (24) |
| USR-NAS-Reboot-Request | (26) |
| USR-NAS-Reboot-Response | (27) |
| Ascend-IPA-Allocate | (50) |
| Ascend-IPA-Release | (51) |
| USR-Enhanced-Radius | (254) |

**Note** **Request-Type** is to be used only by scripts.

# Require-User-To-Be-In-Authorization-List

**Require-User-To-Be-In-Authorization-List** is read for authorization. If we are authorizing with a different service than we authenticated with (not usually done) and the user is not known by the authorization service, the default is to continue on unless this environment variable is set, in which case we reject the request with a cause of Unknown-user.

# Response-Type

**Response-Type** is set and read throughout processing and used to determine whether the request should be accepted, rejected, or challenged. When **Response-Type** is set to“Access-Reject at any time during the processing of a request, no more processing of the request is done, and an Access-Reject response is sent. For other valid values for **Response-Type**, see Table B-1.

## Retrace-Packet

**Retrace-Packet** Read and if set, will cause a trace the packet to be displayed during the incoming and outgoing scripts. If set, will cause a second trace of the request packet's contents after running all the incoming scripts and/or a second trace of the response packet's contents before running the outgoing scripts.

## Session-Key

**Session-Key** is read for session management. If set, the server uses it as the key to look up the session associated with the current request, if any. If not set, the server uses the NAS IP Address and NAS Port to create a session key.

## Session-Manager

**Session-Manager** is read after user authorization and determines which dynamic resources to allocate for this user, when one is needed. If set, the server directs the request to be processed by the specified session manager. When not set, the SessionManager (as defined in **DefaultSessionManager**) is used when needed.

## Session-Notes

**Session-Notes** is a comma-separated list set to make session information available to scripts. **Session-Notes** contains the names of other environment variables. If set, these variables are stored on a Session as notes.

## Session-Service

**Session-Service** is set and read during session management. If set, the server will direct the request to be processed by the specified session service.

## Source-IP-Address

**Source-IP-Address** is set when a request is first received to the IP address from which the IP request was received before calling any extension points. **Source-IP-Address** contains the IP address of the NAS or proxy server that sent the request to this server.

**Note** **Source-IP-Address** is to be used only by scripts.

## Source-Port

**Source-Port** is set when a request is first received to the port from which the request was received. Source-Port is set for each request before calling any extension points and contains the port on the NAS or proxy server that was used to send the request to this server.

**Note** **Source-Port** is to be used only by scripts.

## Subnet-Size-If-No-Match

**Subnet-Size-If-No-Match** is set to one of BIGGER, SMALLER or EXACT, determines the behavior of the subnet-dynamic resource manager if a pool of the requested size is not available.

## Trace-Level

**Trace-Level** is set for each request before calling any extension points. **Trace-Level** is set to the current trace level as specified through **aregcmd**. If set by a script, Trace-Level changes the trace level used to determine what level of information is traced.

## Unavailable-Resource

**Unavailable-Resource** is set during session management. If the request is being rejected because one of the resource managers failed to allocate a resource, **Unavailable-Resource** is set to the name of the resource manager that failed.

## Unavailable-Resource-Type

**Unavailable-Resource-Type** is set during session management. If the request is being rejected because one of the resource managers failed to allocate a resource, **Unavailable-Resource-Type** is set to the type of the resource manager that failed.

## UserDefined1

**UserDefined1** is set to the value of the UserDefined1 property of the user from a local user list during password matching of local users.

## User-Authorization-Script

**User-Authorization-Script** is read in local services during authorization. If set, the server calls the specified script to do additional user authorization after authentication succeeds.

## User-Group

**User-Group** is read in local services during authorization. If set, species the UserGroup to which the current user belongs.

## User-Group-Session-Limit

**User-Group-Session-Limit** is read during session management. If set, **User-Group-Session-Limit** overrides the limit specified for the group-session-limit resource manager.

## User-Name

**User-Name** is read by a local service during authentication. When **User-Name** is set, it is the name used to authenticate or authorize the request and overrides the **User-Name** in the Request dictionary.

## User-Profile

**User-Profile** is read in local services during authorization. If set, **User-Profile** specifies the Profile from which the current user should receive attributes.

## User-Session-Limit

**User-Session-Limit** is read during session management. If set, **User-Session-Limit** overrides the limit specified for the user-session-limit resource manager.