Environment Dictionary

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

Prime 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 4-38 for additional information about Resource Managers.

This appendix has the following major sections:

- Cisco Prime Access Registrar Environment Dictionary Variables

  This section lists environment variables you can use in scripts to communicate with Prime Access Registrar or to communicate with other scripts.

- Internal Variables

  This section lists environment variables used by the Prime Access Registrar server for internal operations. The environment variables listed in this section must not be modified by scripts.

Cisco Prime 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 Prime Access Registrar 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-Dynamic-DNS

Acquire-Dynamic-DNS is set and read for resource management override. **Acquire-Dynamic-DNS** is set to FALSE to skip DNS updating during resource management processing.

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-Home-Agent

Acquire-Home-Agent is set and read for resource management override. **Acquire-Home-Agent** is set to FALSE to override the allocation of the home agent IP address during resource management processing.

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 Prime Access Registrar 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.

AuthorizationInfo

The MSISDN information is copied to **AuthorizationInfo** that is fetched by M3UA service.

BackingStore-Env-Vars

BackingStore-Env-Vars overrides the BackingStoreEnvironmentVariables property of remote servers of type *odbc-accounting* only when the property BufferAccountingPackets is set to TRUE. The value is a comma separated list of environment variables to be stored along with the packet contents in the local disk.

Blacklisted-IMSI

This variable is configured on a SIGTRAN-M3UA remote server. For any incoming request with an IMSI value, if the variable is set as TRUE, then that IMSI value is blacklisted and will not forwarded to the HLR. For more information, see Blacklisting IMSI Values, page 23-11.

Broadcast-Accounting-Packet

If set to TRUE, **Broadcast-Accounting-Packet** enables broadcasting of Accounting-on or Accounting-off packets to all remote servers of type *radius*.

Cache-Attributes-In-Session

Cache-Attributes-In-Session is set and read for resource management override. **Cache-Attributes-In-Session** is set to FALSE to override the caching of attributes by the *session-cache* type of resource manager.

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.

Cache-Outer-Identity

Cache-Outer-Identity value is set to enable identifying session of an user. If it is set to TRUE, WiMAX session manager will cache the outer identity. If it is set to FALSE, the WiMAX session manager will cache the inner identity. The value is set to FALSE by default.

Destination-IP-Address

Destination-IP-Address is a read only value which is set to the receiver IP address. **Destination-IP-Address** contains the IP address of the request packet receiver.

Destination-Port

Destination-port is a read only value which is set to the receiving port number. **Destination-port** contains the port number of the receiver of the request.

Dest-Translation-Type

Dest-Translation-Type is configured through the GlobalTitleTranslationScript. When the RoutingIndicator is set to **RTE_GT**, Prime Access Registrar server reads the value that is set in Dest-Translation-Type and sets the TranslationType field of the Called Party Address. The value in this environment variable overrides the value that is configured in the DestinationGTAddress/DestTranslationType property of a remote server, SIGTRAN-M3UA.

Dest-Numbering-Plan

Dest-Numbering-Plan is configured through the GlobalTitleTranslationScript. When the RoutingIndicator is set to **RTE_GT**, Prime Access Registrar server reads the value that is set in Dest-Numbering-Plan and sets the NumberingPlan field of the Called Party Address. The value in this environment variable overrides the value that is configured in the DestinationGTAddress/Dest-Numbering-Plan property of a remote server, SIGTRAN-M3UA.

The following are the only values that are used for Dest-Numbering-Plan environment variable:

- DATA
- GENERIC
- ISDN
- ISDNMOB
- LANMOB
- MARMOB
- NWSPEC
- TEL
- TELEX
- UNKN

If you set any variable other than the above ones, Prime Access Registrar server sets the NumberingPlan that is configured in DestinationGTAddress/Dest-Numbering-Plan property of a remote server of type SIGTRAN-M3UA.

Dest-Encoding-Scheme

Dest-Encoding-Scheme is configured through the GlobalTitleTranslationScript. When the RoutingIndicator is set to **RTE_GT**, Prime Access Registrar server reads the value that is set in Dest-Encoding-Scheme environment variable and sets the EncodingScheme field of the Called Party Address. The value in this environment variable overrides the value that is configured in the DestinationGTAddress/ DestEncodingScheme property of a remote server, SIGTRAN-M3UA.

The following are the only values that are used for Dest-Encoding-Scheme environment variable:

- BCDEVEN
- BCDODD

If you set any variable other than the above ones, Prime Access Registrar server sets the EncodingScheme that is configured in the DestinationGTAddress/ DestEncodingScheme property of a remote server of type SIGTRAN-M3UA.

Dest-Nature-Of-Address

Dest-Nature-Of-Address is configured through the GlobalTitleTranslationScript. When the RoutingIndicator is set to **RTE_GT**, Prime Access Registrar server reads the value that is set in Dest-Nature-Of-Address environment variable and sets the NatureOfAddress field of the Called Party Address. The value in this environment variable overrides the value that is configured in the DestinationGTAddress/ DestNatureofAddress property of a remote server, SIGTRAN-M3UA.

The following are the only values that are used for Dest-Nature-Of-Address environment variable:

- ADDR_NOTPRSNT
- INTNUM
- NATSIGNUM
- SUBNUM

If you set any variable other than the above ones, Prime Access Registrar server sets the NatureOfAddress that is configured in the DestinationGTAddress/ DestNatureofAddress property of a remote server of type SIGTRAN-M3UA.

Dest-GT-Format

Dest-GT-Format configured through the GlobalTitleTranslationScript. When the RoutingIndicator is set to **RTE_GT**, Prime Access Registrar server reads the value that is set in Dest-GT-Format environment variable and uses this format specified for the Global Title Digits(Address Information). The value in this environment variable overrides the value that is configured in the DestinationGTAddress/ DestGTFormat property of a remote server, SIGTRAN-M3UA.

The following are the only values that are used for Dest-GT-Format environment variable:

- GTFRMT_0
- GTFRMT_1
- GTFRMT_2
- GTFRMT_3
- GTFRMT_4
- GTFRMT_5

If you set any variable other than the above ones, Prime Access Registrar server sets the GTFormat that is configured in the DestinationGTAddress/ DestGTFormat property of a remote server of type SIGTRAN-M3UA.

Diameter-Application-Id

Diameter-Application-Id is set to get the application ID in the Diameter packet.

Diameter-Command-Code

Diameter-Command-Code is set to get the command codes in the Diameter packet.

Disable-Accounting-On-Off-Broadcast

If set to TRUE, **Disable-Accounting-On-Off-Broadcast** disables broadcasting of Accounting-On and Accounting-Off packets to all remote servers of type 'radius'.

DSA-Response-Cache

DSA-Response-Cache is used while performing DSA(Dynamic Service Authorization) feature in Prime Access Registrar. It is FALSE by default, which will clear the response dictionary before Re-Authentication. If DSA-Response-Cache is set to TRUE, Prime Access Registrar will not clear the response dictionary before Re-Authenticating with next service configured.

Dynamic-DNS-HostName

Dynamic-DNS-HostName is read while constructing the forward hostname during resource management processing to update DNS entries. If set, the name will be used as forward hostname instead of constructing one.

Dynamic-Search-Filter

Dynamic-Search-Filter overrides the Filter property in remote servers of type *ldap*. The format of the value set for **Dynamic-Search-Filter** should be similar to that of the Filter property.

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.

Dynamic-Search-Scope

Dynamic-Search-Scope is used to dynamically set the SearchScope property of an LDAP remote server configuration on a per-packet basis.

Dynamic-Service-Loop-Limit

Dynamic-Service-Loop-Limit variable is used to change loop counts. When using the same service for reauthentication and reauthorization, a loop can occur in these services. The loop count, by default is 10. You can change the loop count using this variable.

Dynamic-User-Password-Attribute

Dynamic-User-Password-Attribute is read for LDAP authentication and overrides the UserPasswordAttribute. If set, the server uses it to retrieve the password field as its LDAP UserPassword attribute instead of the value set in the remote server configuration.

EAP-Actual-Identity

EAP-Actual-Identity is a read-only variable that contains the International Mobile Subscriber Identity (IMSI) of the user after a successful EAP-SIM authentication.

EAP-Authentication-Mode

EAP-Authentication-Mode is a read-only variable, set after a successful EAP-SIM authentication, that indicates whether the EAP-SIM authentication was a reauthentication or a full authentication.

Enforce-Traffic-Throttling

By default, the value is set to FALSE. When set to TRUE, the traffic throttling check for the packet will be executed.

FetchAuthorizationInfo

When set to TRUE, this variable fetches MSISDN value from the HLR.

Do not use **FetchAuthorizationInfo** for authorization. We recommend that you use the authorization service of m3ua instead.

Generate-BEK

Generate-BEK is read when WiMax provisioning service is enabled. If this is set,
Prime Access Registrar will generate the Bootstrap Encryption Key in the WiMax flow.

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.

HLR-GlobalTitle-Address

HLR-GlobalTitle-Address is configured through the GlobalTitleTranslationScript. When the RoutingIndicator is set to **RTE_GT** in SIGTRAN-M3UA remote server, Prime Access Registrar server reads the value that is set in HLR-GlobalTitle-Address and sets the Destination GT Digits(Address Information field) of the Called Party Address.

HLR-GlobalTitle-Cached

HLR-GlobalTitle-Cached is set as TRUE to indicate the HLR GT is cached.

The Home Location Registry (HLR) Global Title address (GT address in calling party address (CgPA)) from the SendAuthenticationInfo (SAI) response is cached and used for subsequent authorization request. This cached HLR GT is added to the environment dictionary of the packet to be available for the authorization flow.

The cached HLR GT overrides both the configured destination GT values and GT script provided GT values. The HLR GT caching works by default for RTE_GT. The cached HLR GT can be overridden by updating the environment variable HLR-GlobalTitle-Cached to FALSE (or anything other than TRUE) in the GT script.

This HLR GT will not be cached for:

- reauthentication flow
- authorize only flow when authentication vectors are already available in cache (as there will not be SAI request.

HLR-Translated-IMSI

HLR-Translated-IMSI is configured through the IMSITranslationScript. Prime Access Registrar server reads the value in HLR-Translated-IMSI and sets the value as IMSI before sending the request to STP/HLR. The value that is configured in the HLR-Translated-IMSI environment variable overrides the IMSI received in EAP-AKA/EAP-SIM request packet.

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, Prime 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.

IMSI

International Mobile System Identifier (IMSI) that is fetched from the response from HLR.

Incoming-Translation-Groups

Incoming-Translation-Groups is read for authentication while processing responses from a remote RADIUS server. If set, **Incoming-Translation-Groups** specifies the translation groups to be used to filter attributes on requests.

Master-URL-Fragment

Used with the Windows Provisioning Service feature, **Master-URL-Fragment** specifies the fragment within the Master URL to be sent back to the provisioning server. **Master-URL-Fragment** can be set to any of the following four values: *signup*, *renewal*, *passwordchange*, and *forceupdate*. If **Master-URL-Fragment** is not set and is required to send the URL, *signup* will be sent by default.

The environmental variable **Send-PEAP-URL-TLV** indicates whether or not to send the URL.

Misc-Log-Message-Info

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

MSISDN

The Mobile Subscriber ISDN Number (MSISDN) that is fetched from the response from HLR.

Outgoing-Translation-Groups

Outgoing-Translation-Groups is read while proxying to a remote radius server. If set, **Outgoing-Translation-Groups** specifies the translation groups to be used to filter attributes.

Pager

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.

Query-Service

The Query-Service variable is set and read for the *radius-query* service selection type. The Query-Service variable must be set before authentication phase begins at the server, vendor, or client incoming scripting point or using the policy engine. If set, the server directs requests to be processed by the specified *radius-query* service. After the Query-Service variable is set, no AAA processing will be done.

Re-Accounting-Service

Re-Accounting-Service is configured, through script, for dynamic service authorization. When the Re-Accounting-Service is set, the server directs the request to the specified reaccounting service for processing.

Re-Authentication-Service

Re-Authentication-Service is configured, through script, for dynamic service authorization. When the Re-Authentication-Service is set, the server directs the request to the specified reauthentication service for processing.

Re-Authorization-Service

Re-Authorization-Service is configured, through script, for dynamic service authorization. When the Re-Authorization-Service is set, the server directs the request to the specified reauthorization service for processing.

Realm

The **Realm** variable is set for *domain-auth* type of service and is used as the domain name for windows authentication.

Reject-Reason

Reject-Reason is set when a request is being rejected and contains the **Reject-Reason**.
Prime 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.

Remove-Session-On-Acct-Stop

When set to TRUE, server removes the session on receiving an accounting stop packet.

Remote-Servers-Tried

Remote-Servers-Tried contains a list of remote servers that were tried before a request was accepted or rejected (in the case of a Failover multiple remoteserver policy). The list of servers is a comma-separated list of remote server names.

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 Prime 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	(12)
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 as a read-only variable 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

If set, **Retrace-Packet**, causes 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.

Send-PEAP-URI-TLV

When set to TRUE, the URI PEAP-TLV is included along with the Result PEAP-TLV in the access-challenge packet. The authenticating user service (of type userlist, LDAP, or WDA) can set this to TRUE using an extension point script or attribute mapping so that the PEAP-v0 service can send the URI PEAP-TLV. The default value for this is FALSE.

Note This variable is used with the Windows Provisioning Service (WPS) feature.

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.

Set-Session-Mgr-And-Key-Upon-Lookup

When **Set-Session-Mgr-And-Key-Upon-Lookup** is set to TRUE, a session-cache resource manager sets the session-manager and session-key environment variable during a query-lookup, and the Prime Access Registrar server does not cache the response dictionary attributes.
Set-Session-Mgr-And-Key-Upon-Lookup is set to TRUE by a query-service IncomingScript.

Skip-Session-Management

When set to TRUE in a request, **Skip-Session-Management** causes session management to be skipped for the request, even if session management might normally occur.

Skip-Overriding-Username-With-LDAP-UID

Skip-Overriding-Username-With-LDAP-UID is used to decide if the username should be replaced with the UID from the LDAP server. When Skip-Overriding-Username-With-LDAP-UID is set to TRUE, the username is not replaced with the UID from the LDAP server.

You can use Skip-Overriding-Username-With-LDAP-UID to retain case sensitivity in usernames when the username given logging into the network is in a different case that the UID in the LDAP server database, such as *User1* and *user1*.

Skip-Overriding-UserName-With-PEAPIdentity

Skip-Overriding-Username-With-PEAPIdentity is used to decide if the username should be replaced with the PEAP Identity. When Skip-Overriding-Username-With-PEAPIdentity is set to TRUE, the username is not replaced with the PEAP Identity.

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 as a read-only variable 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 as a read-only variable 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.

Virtual-Server-Outgoing-Script

Virtual-Server-Outgoing-Script is read when LawfulIntercept script object is enabled to use virtual script object. If this is set, the configured script will be executed after server outgoing script.

Windows-Domain-Groups

The Windows-Domain-Groups variable is a read-only variable that contains a comma separated list of group names to which the user belongs in the Active Directory. The Windows-Domain-Groups variable is set after a successful authentication using a *domain-auth* type of service.

X509- Subject-Name

X509- Subject-Name reads the value of the subject in the SSL certificate. This is read while processing the access request.

Internal Variables

The following environment variables are used by the server for internal operation. The values for these environment variables must not be modified.

- Add-Message-Authenticator
- Calling-Service-Name
- Cleartext-Password
- Current-Service-Name
- Dynamic-Search-UID
- Duplicate-Req
- EAP-Internal-Services
- Group-Service
- Group-Service-State-ID
- Hidden-Attrib
- IMSI
- Local-Port-type
- Message-Authenticator-Present
- MSCHAP-Account-Name
- MS-ChapV2-Message
- NAS-Name-And-IPAddress
- Notify-Service-Session-Key
- Notify-Service-State-ID
- Number-Requested-Quintets
- Number-Requested-Triplets
- Proxied-Dynamic-Auth (named Proxied-POD in earlier releases)
- Provider-Identifier
- Rcd-NT-Password-Hash-Hash (named Rcd-NT-Password-Hash in earlier releases)
- Remote-Session
- Return-Data
- Roaming
- Script-Level
- Session-ID
- Session-Accounting-Counter
- Session-Generation-Tag
- Session-Last-Accessed-Time
- Session-Manager-Key
- Session-NAS-Identifier
- Session-NAS-Port

- Session-Resource-Count
- Session-Resource-%d
- Session-Reuse
- Session-Start-Time
- Session-Survives-NAS-Reboot
- Session-User-Name
- User-Name-Used-For-Lookup
- WiMax-Authentication
- WiMax-SessionManager-Exists