

# RESTful API

## Interface Description

UPDATED: 27 July 2023

**© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.**

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# Table of Contents

**1 Introduction** ..... **19**

1.1 Document Purpose ..... 19

1.2 Intended Audience ..... 19

**2 The RESTful API Interface** ..... **20**

2.1 How the LoadMaster RESTful API Works ..... 20

2.2 JSON-based Input and Output ..... 21

2.3 Security ..... 23

2.3.1 Configure Certificate-Based Authentication ..... 23

2.3.1.1 Enable Session Management ..... 23

2.3.1.2 Create a User (If Needed) ..... 24

2.3.1.3 Enable Client Certificate Authentication on the LoadMaster ..... 25

2.3.1.4 Generate and Download the Client Certificate ..... 26

2.3.1.5 Specify the Certificate Details in the API ..... 27

2.3.1.6 Create a PFX File (If Running Commands using a Web Browser) ..... 28

2.3.2 How to Use API Keys ..... 28

2.3.2.1 Delete an API Key ..... 29

2.4 Enabling the LoadMaster RESTful API Interface ..... 29

2.5 Using get and set commands ..... 30

2.6 Error Reports ..... 30

2.7 Notation ..... 30

**3 RESTful API Commands** ..... **32**



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.1 Command Syntax ..... 32
3.2 List All API Commands and get/set Parameters ..... 32
3.3 Home Screen Information ..... 32
3.3.1 Retrieve the LoadMaster Firmware Version ..... 33
3.3.2 Retrieve the Boot Time and Active Time ..... 33
3.3.3 Retrieve the Serial Number ..... 33
3.3.4 Retrieve the Virtual Service and Real Service Statuses ..... 33
3.3.5 Retrieve Licensing Information ..... 33
3.4 Initial Configuration ..... 33
3.4.1 Read the EULA ..... 34
3.4.2 Accept the EULA and Set the License Type ..... 34
3.4.3 Retrieve the Available License Types ..... 35
3.4.4 License the LoadMaster ..... 35
3.4.5 Set the Initial Password ..... 35
3.5 Licensing using the Activation Server Functionality ..... 36
3.6 Virtual Services ..... 37
3.6.1 Virtual Service Control ..... 37
3.6.1.1 Properties ..... 39
3.6.1.2 Basic Properties ..... 41
3.6.1.3 Standard Options ..... 41
3.6.1.4 SSL Properties ..... 47
3.6.1.4.1 TLSType Parameter ..... 52


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.6.1.5 Advanced Properties ..... 56
3.6.1.5.1 Upload Error File ..... 64
3.6.1.5.2 Verify Parameter ..... 64
3.6.1.6 WAF Settings ..... 65
3.6.1.6.1 WAF InterceptOpts Parameter ..... 66
3.6.1.6.2 Assign a WAF Rule to a Virtual Service ..... 69
3.6.1.6.3 Unassign an WAF Rule from a Virtual Service ..... 70
3.6.1.7 ESP Options ..... 71
3.6.1.8 Real Servers ..... 93
3.6.1.9 Miscellaneous ..... 98
3.6.2 Adding a Virtual Service Using a Template ..... 99
3.6.3 Manage Templates ..... 99
3.6.3.1 Export a Virtual Service as a Template ..... 99
3.6.3.2 Upload a Template ..... 99
3.6.3.3 Display a List of Installed Templates ..... 99
3.6.3.4 Delete a Template ..... 99
3.6.4 Manage SSO ..... 100
3.6.4.1 SSO Domains ..... 100
3.6.4.1.1 Upload RSA Files ..... 111
3.6.4.1.2 Upload an Identity Provider (IdP) Metadata File (if using SAML) ..... 112
3.6.4.1.3 Download the Service Provider Certificate (if using SAML) ..... 112
3.6.4.1.4 Sessions ..... 112


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.6.4.2 SSO Image Sets ..... 113
3.6.5 Cache Configuration ..... 114
3.6.6 Compression Options ..... 114
3.6.7 Kubernetes Settings ..... 114
3.6.7.1 Upload a Kube Config File ..... 114
3.6.7.2 Delete the Kube Config File ..... 115
3.6.7.3 List the Contexts in the Kube Config File ..... 115
3.6.7.4 Check the Operations Mode ..... 115
3.6.7.5 Set the Operations Mode ..... 115
3.6.7.6 Check the Namespace being Watched ..... 115
3.6.7.7 Set the Namespace to Watch ..... 115
3.6.7.8 Check the Watch Timeout ..... 115
3.6.7.9 Set the Watch Timeout ..... 115
3.6.7.10 Restart the Ingress Controller ..... 116
3.6.8 Legacy WAF Settings ..... 116
3.6.8.1 Commands Relating to Commercial Rule Files ..... 116
3.6.8.1.1 Display the Commercial WAF Rule Settings ..... 116
3.6.8.1.2 Enable Automatic Commercial Rule File Updates ..... 116
3.6.8.1.3 Enable/Disable Automatic Installation of Commercial Rule File Updates ..... 117
3.6.8.1.4 Set the Time of the Automatic Commercial Rule File Installation ..... 117
3.6.8.1.5 Download WAF Commercial Rule File Updates Now ..... 117
3.6.8.1.6 Display the WAF Rule Change Log ..... 118


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.6.8.1.7 Manually Install Commercial Rule Files ..... 118
3.6.8.2 Commands Relating to Custom Rule Files ..... 118
3.6.8.2.1 Upload a Custom Rule File or Rule Set ..... 118
3.6.8.2.2 Delete a Custom Rule File ..... 119
3.6.8.2.3 Download a Custom Rule File ..... 119
3.6.8.2.4 Upload a Custom Rule Data File ..... 119
3.6.8.2.5 Delete a Custom Rule Data File ..... 120
3.6.8.2.6 Download a Custom Rule Data File ..... 120
3.6.8.3 Command Relating to Custom and Commercial Rules ..... 120
3.6.8.3.1 List WAF Rules ..... 120
3.6.8.4 Commands Relating to Remote Logging ..... 120
3.6.8.4.1 Set the WAF Logging Format ..... 121
3.6.8.4.2 Disable Remote Logging ..... 121
3.6.8.4.3 Enable Remote Logging ..... 121
3.6.8.4.4 Save Temporary WAF Remote Log Data ..... 121
3.6.8.4.5 Clear Temporary WAF Remote Log Data ..... 121
3.6.9 WAF Settings ..... 121
3.6.9.0.1 WAF OwaspOpts Parameter ..... 125
3.6.9.1 OWASP Custom Rulesets ..... 128
3.6.9.2 OWASP Custom Data File ..... 128
3.6.9.3 OWASP Rules ..... 128
3.7 Global Balancing ..... 129


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.7.1 Manage Fully Qualified Domain Names (FQDNs) ..... 129
3.7.1.1 Add FQDN ..... 129
3.7.1.2 Delete FQDN ..... 130
3.7.1.3 List FQDNs ..... 130
3.7.1.4 Show FQDN ..... 131
3.7.1.5 Modify FQDN ..... 132
3.7.1.6 Add Map ..... 136
3.7.1.7 Modify a Map ..... 136
3.7.1.8 Delete a Map ..... 139
3.7.1.9 Change the Location of a Map ..... 139
3.7.1.10 Add a Location ..... 140
3.7.1.11 Remove a Location ..... 140
3.7.1.12 Change Checker Address ..... 141
3.7.1.13 Additional Records ..... 142
3.7.2 Manage Clusters ..... 142
3.7.2.1 List Clusters ..... 142
3.7.2.2 Show Cluster ..... 143
3.7.2.3 Add Cluster ..... 143
3.7.2.4 Delete Cluster ..... 143
3.7.2.5 Modify Cluster ..... 143
3.7.2.6 Change Cluster Location ..... 144
3.7.3 Miscellaneous Params ..... 144


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.7.3.1 List the Miscellaneous Parameters ..... 144
3.7.3.2 Modify Miscellaneous Parameters ..... 145
3.7.3.3 Upload a Location Data Patch File ..... 148
3.7.4 IP Range Selection Criteria ..... 148
3.7.4.1 List the IP Addresses ..... 148
3.7.4.2 Show IP Address Details ..... 148
3.7.4.3 Add IP Address ..... 148
3.7.4.4 Delete IP Address ..... 148
3.7.4.5 Change the Location for an IP Address ..... 148
3.7.4.6 Delete IP Location ..... 149
3.7.4.7 Add IP Country ..... 149
3.7.4.8 Remove IP Country ..... 149
3.7.4.9 List the Custom Locations ..... 149
3.7.4.10 Add a Custom Location ..... 149
3.7.4.11 Edit a Custom Location ..... 150
3.7.4.12 Delete a Custom Location ..... 150
3.7.5 IP Access List Settings ..... 150
3.7.5.1 Retrieve the IP Access List Settings ..... 150
3.7.5.2 Enable/Disable Automatic IP Access List Updates ..... 150
3.7.5.3 Enable/Disable Automatic Installation of the IP Access List Updates ..... 150
3.7.5.4 Set the Time of the Automatic Installation ..... 150
3.7.5.5 Download the Updates Now ..... 151


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.7.5.6 Install the Updates Now ..... 151
3.7.5.7 View the Access List ..... 151
3.7.5.8 View Changes to the Access List ..... 151
3.7.5.9 View the User-Defined Allow List ..... 151
3.7.5.10 Add an Address to the Allow List ..... 151
3.7.5.11 Remove an IP Address or Network from the Allow List ..... 151
3.7.6 Configure DNSSEC ..... 151
3.7.6.1 Generate the Key Signing Keys (KSKs) ..... 151
3.7.6.2 Import the KSKs ..... 152
3.7.6.3 Delete the KSK Files ..... 152
3.7.6.4 Enable/Disable DNSSEC ..... 152
3.7.6.5 Retrieve the DNSSEC Configuration Settings ..... 152
3.7.7 GSLB Statistics ..... 152
3.7.8 Enable/Disable GEO ..... 152
3.7.8.1 Check if GEO is Enabled ..... 152
3.7.8.2 Enable GEO ..... 153
3.7.8.3 Disable GEO ..... 153
3.8 Statistics ..... 153
3.9 SDN Statistics ..... 165
3.10 Real Servers ..... 173
3.10.1 Enabling/Disabling Real Servers ..... 176
3.10.1.1 Globally Enable/Disable a Real Server ..... 176


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.10.1.2 Locally Enable/Disable a Real Server ..... 176
3.11 Rules & Checking ..... 177
3.11.1 Show Rules ..... 177
3.11.2 Delete a Rule from the System ..... 177
3.11.3 Add/Modify a Rule on the System ..... 177
3.11.4 Add/Delete Real Server Rule ..... 183
3.11.5 Add/Delete SubVS Rule ..... 184
3.11.6 Add Virtual Service Rules ..... 184
3.11.7 Delete Virtual Service Rules ..... 185
3.11.8 Check Parameters ..... 185
3.12 Certificates & Security ..... 187
3.12.1 Certificate Management ..... 187
3.12.2 ACME Certificates ..... 189
3.12.2.1 Get an existing Let's Encrypt account ..... 190
3.12.2.2 Register a Let's Encrypt Account ..... 190
3.12.2.3 DigiCert Certificate Account Parameters ..... 190
3.12.2.4 ACME Certificate Commands ..... 191
3.12.2.4.1 ACME Global Parameters ..... 191
3.12.2.4.2 Delete the ACME Configuration Parameters ..... 191
3.12.2.4.3 Request a New ACME Certificate ..... 191
3.12.2.4.4 Renew an ACME Certificate ..... 192
3.12.2.4.5 Delete an ACME Certificate ..... 192


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.12.2.4.6 List the ACME Certificates ..... 192
3.12.2.4.7 Get the ACME Account Information ..... 193
3.12.2.4.8 Get Details about a Specific ACME Certificate ..... 193
3.12.3 Cipher Sets ..... 193
3.12.3.1 Modify a Custom Cipher Set/Create a New Custom Cipher Set ..... 193
3.12.3.2 Retrieve the Details of an Existing Cipher Set ..... 193
3.12.3.3 Delete a Custom Cipher Set ..... 194
3.12.4 Remote Access ..... 194
3.12.4.1 Set Admin Access ..... 199
3.12.4.2 Get GEO Partner Status ..... 200
3.12.4.3 WUI Authentication and Authorization Options ..... 200
3.12.5 Admin WUI Access ..... 203
3.12.6 OCSP Configuration ..... 208
3.12.7 LDAP Configuration ..... 209
3.12.7.1 Add an LDAP Endpoint ..... 209
3.12.7.2 Modify an LDAP Endpoint ..... 210
3.12.7.3 Delete an LDAP Endpoint ..... 211
3.12.7.4 Retrieve Details of All LDAP Endpoints ..... 212
3.12.7.5 Retrieve Details of a Specific LDAP Endpoint ..... 212
3.12.8 Intrusion Detection Options (IPS/IDS) ..... 212
3.13 Interfaces ..... 212
3.13.1 Get Interface Details ..... 212


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.13.2 Modify Interface Details ..... 213
3.13.3 Additional Addresses ..... 215
3.13.4 Bonded Interfaces ..... 215
3.13.5 VLANs ..... 215
3.13.6 VXLANs ..... 216
3.14 Host & DNS Configuration ..... 216
3.14.1 Resolve DNS Names Now ..... 217
3.14.2 Hosts for Local Resolution ..... 218
3.15 Route Management ..... 218
3.15.1 Default Gateway ..... 218
3.15.2 Additional Routes ..... 219
3.15.3 Packet Routing Filter ..... 219
3.15.4 VPN Management ..... 220
3.15.4.1 Create a New VPN Connection ..... 220
3.15.4.2 Delete an Existing IPsec Connection ..... 220
3.15.4.3 Set the VPN Addresses ..... 221
3.15.4.4 Set the Perfect Forward Secrecy Option ..... 222
3.15.4.5 Set the Connection Secret ..... 222
3.15.4.6 Start the Connection ..... 222
3.15.4.7 Stop the Connection ..... 222
3.15.4.8 Get the Connection Status ..... 223
3.15.4.9 List All Existing Connections ..... 223


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.15.4.10 Stop the IKE Daemon ..... 223
3.15.4.11 Start the IKE Daemon ..... 223
3.15.4.12 Get the IKE Daemon Status ..... 223
3.16 Access Lists ..... 223
3.17 Cluster Control ..... 225
3.17.1 Clustering API Commands ..... 225
3.17.1.1 Get the Status of the Cluster ..... 225
3.17.1.2 Create a Cluster ..... 226
3.17.1.3 Initiate a Node Joining a Cluster ..... 227
3.17.1.4 Add a Node to the Cluster ..... 227
3.17.1.5 Enable a Node ..... 227
3.17.1.6 Disable a Node ..... 227
3.17.1.7 Delete a Node ..... 228
3.17.2 RESTful API Clustering Example ..... 228
3.18 QoS/Limiting ..... 229
3.18.1 Maximum Client Concurrent Connection Limit ..... 230
3.18.2 Client CPS Limit ..... 230
3.18.3 Legacy Client CPS Limit Commands ..... 230
3.18.4 Client RPS Limit ..... 231
3.18.5 Client Bandwidth Limit ..... 231
3.18.6 Per-Virtual Service Limits ..... 232
3.18.7 URL-Based Limiting Rules ..... 232


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.19 System Administration ..... 233
3.19.1 User Management ..... 233
3.19.1.1 Change the System Password ..... 233
3.19.1.2 Set the Minimum Password Length ..... 233
3.19.1.3 List All Local Users ..... 233
3.19.1.4 Display Permissions for a Particular Local User ..... 234
3.19.1.5 Add a New Local User ..... 234
3.19.1.6 Delete a Local User ..... 234
3.19.1.7 Change the Password of a Local User ..... 234
3.19.1.8 Set Permissions for a Local User ..... 235
3.19.1.9 Local Certificate Management ..... 236
3.19.1.10 Remote User Group Management ..... 236
3.19.1.11 Extended Permissions Management ..... 237
3.19.2 Licensing ..... 237
3.19.2.1 License ..... 238
3.19.2.2 AlsiLicense ..... 239
3.19.2.3 Accesskey ..... 239
3.19.2.4 KillASLInstance ..... 240
3.19.2.5 Deactivate a non-SPLA License ..... 240
3.19.3 System Reboot ..... 240
3.19.4 Update Software ..... 240
3.19.4.1 Upgrade to a Newer Version of Software ..... 240


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.19.4.2 Check the Previously Installed Firmware Version ....241
3.19.4.3 Restore to a Previously Installed Version of Software ....241
3.19.4.4 List the Installed Add-On Packs ....241
3.19.4.5 Upload or Update an Add-On Pack ....241
3.19.4.6 Delete Add-On Pack ....241
3.19.5 Backup/Restore ....241
3.19.5.1 Automated Backups ....242
3.19.6 Date/Time Settings ....244
3.20 Logging Options ....245
3.20.1 Manage System Logs ....245
3.20.2 Ping Host ....246
3.20.3 Run a Traceroute ....246
3.20.4 Debug Options ....247
3.20.4.1 Get/Set Debug Options ....247
3.20.4.2 Retrieve RAID Information ....248
3.20.4.3 Retrieve RAID Disk Information ....248
3.20.4.4 Reset Statistics ....248
3.20.4.5 Flush SSO Authentication Cache ....248
3.20.5 Extended Log Files ....248
3.20.5.1 List the Extended Log Files ....248
3.20.5.2 Clear Extended Log Files ....249
3.20.5.3 Save Extended Log Files ....249


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.20.5.4 Enable/Disable Extended ESP Logging ..... 249
3.20.6 Syslog Options ..... 250
3.20.7 SNMP Options ..... 251
3.20.8 Email Options ..... 253
3.20.9 SDN Log Files ..... 254
3.20.9.1 Debug Options ..... 254
3.21 Troubleshooting ..... 254
3.21.1 Get/Set Debug Options ..... 254
3.21.2 Run a Top ..... 255
3.21.3 Run the Other Debug Options ..... 256
3.21.4 Run a TCP Dump ..... 256
3.22 Miscellaneous Options ..... 257
3.22.1 WUI Settings ..... 257
3.22.2 L7 Configuration ..... 258
3.22.3 Network Options ..... 262
3.22.4 HA Management ..... 265
3.22.5 Cloud HA Parameters ..... 269
3.22.5.1 Azure HA Parameters ..... 270
3.22.5.2 AWS HA Parameters ..... 270
3.22.6 SDN Configuration ..... 271
3.22.6.1 Add an SDN Controller ..... 271
3.22.6.2 Modify an SDN Controller ..... 272


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.22.6.3 Delete an SDN Controller ..... 275
3.22.6.4 Show the Existing SDN Controllers ..... 275
3.23 Network Telemetry ..... 277
3.24 Setting Up HA using the RESTful API ..... 280
3.24.1 Set up HA on a Regular LoadMaster using RESTful API ..... 280
3.24.2 Set up HA on a LoadMaster for Azure using RESTful API ..... 281
**4 Scripting Examples with the LoadMaster RESTful API ..... 282**
**5 List All API Commands and get/set Parameters ..... 283**
**References ..... 284**
**Last Updated Date ..... 285**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# 1 Introduction

Kemp leads the industry in driving the price/performance value proposition for application delivery and load balancing to levels that our customers can afford. Our products' versatile and powerful architecture provide the highest value, while enabling our customers to optimize their businesses that rely on Internet-based infrastructure to conduct business with their customers, employees and partners.

Kemp products optimize web and application infrastructure as defined by High Availability (HA), high-performance, flexible scalability, security and ease of management. They maximize the total cost-of-ownership for web infrastructure, while enabling flexible and comprehensive deployment options.

## 1.1 Document Purpose

This document describes the RESTful API Interface to the Kemp LoadMaster. It describes in detail how to configure the various features of the Kemp LoadMaster using the RESTful API.

This document does not explain each of the features or options in detail. For further information, please refer to the relevant Feature Description document on www.kemptechnologies.com/documentation.

## 1.2 Intended Audience

This document is intended to help anyone who wishes to configure the Kemp LoadMaster using the RESTful API.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# 2 The RESTful API Interface

This document describes an interface designed to allow remote applications access to the LoadMaster in a simple and consistent manner. The interface is a REST-like interface. REST (Representational State Transfer) is a style of software architecture for distributed systems and is one of the predominant web service design models.

## 2.1 How the LoadMaster RESTful API Works

The LoadMaster RESTful API works in a RESTful manner, by allowing a user or application to pass HTTPS requests to the LoadMaster. The LoadMaster answers the request with an XML formatted response. The HTTPS request is in the format:

```
https://<LoadMaster IP
Address>/access/<command>?<parameter1>=value&<parameter2>=value
```

You can also run the commands using cURL. If you are using cURL, you may need to surround the URL in double quotes for it to work, for example:

```
curl -k
"https://bal:<Password>@<LoadMasterIPAddress>/access/set?param=backupmethod&v
alue=sftp"
```

When you run commands using cURL, you may also need to include **-k** or **--insecure** if you are using the self-signed LoadMaster certificate.

The basic interface is a simple HTTPS GET operation where the command is specified by the URL. If any parameters are required by the operation, they are passed as QUERY parameters.

> When using the API there is a maximum URL length of 1K. If you want to set a value which is longer than this, use a POST operation instead.

The following points should be noted regarding the formatting of the HTTPS request:

- Only one command can be given at a time.
- The '?' character signifies the end of a command.
- The '&' character signifies the end of a parameter/value pair.
- If there are any unnecessary parameter/value pairs, they will be ignored.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- The order in which the parameter/value pairs appear does not matter.
- There cannot be any spaces within the query. Although some applications, like browsers, would convert spaces to HTML code prior to sending the string to the LoadMaster.
- Multiple parameters can be modified within the same command.

For example, the following query will return the maximum cache size from a LoadMaster with the IP address of 10.11.0.20.

**https://10.11.0.20/access/get?param=cachesize**

The response to the query, from the LoadMaster, is returned in an easily decoded XML format, for example:

```
-----------------------------------------------------
<?xml version="1.0" encoding="ISO-8859-1"?>
<Response stat="200" code="ok">
    <Success>
        <Data>
            <cachesize>
            100
            </cachesize>
        </Data>
    </Success>
</Response>

-----------------------------------------------------
```

> Not all commands in this document are allowed on all LoadMasters. Some functions are only available for certain LoadMaster licenses.

> The connection drops if more than 30 calls are performed in less than 3 seconds over all API interfaces.

## 2.2 JSON-based Input and Output

In LoadMaster firmware version 7.2.50, beta functionality was added which allows you to specify API requests as a POST of a JSON object and receive a JSON-based API payload response. As of firmware version 7.2.52, this functionality is no longer in beta and is officially part of the LoadMaster product.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> When using JSON-based input and output, the supported authentication method is token-based, API keys. Certificate-based authentication is not supported. For further details, refer to the **How to Use API Keys** section of the RESTful API Interface Description document.

To use JSON-based input and output, all requests must be a POST of a JSON object. For authorization purposes, an API key (**apikey**) or a username/password pair (**apiuser**, **apipass**) can also be given. Once the machine has been licensed, one or the other must be provided for access to be allowed. If an **apikey** is provided, this has precedence over any username/passwords provided.

Each request is a JSON object. The only mandatory field is **cmd** which is the name of the command to execute.

Some commands have sub-commands, for example **logging**, **ssodomain**, **aclcontrol**, **geoacl**, and **cluster**. In the old format, most of these sub-commands are run like this: **<LoadMasterIPAddress>/access/logging/df**. In the new format, here is an example of how a sub-command is run: **logging.df**.

Here is an example of a simple request (**-d** tells cURL to send the following string as a POST request):

**curl -k -d '{ "apikey" : "<APIKey>", "cmd" : "listapi" } '
https://<LoadMasterIPAddress>/accessv2**

Here is another example that sets a parameter value:

**curl -k -d '{ "apikey" : "<APIKey>", "cmd" : "set", "param" : "enableapi", "val" : true } '
https://<LoadMasterIPAddress>/accessv2**

For reference, here is how these requests would look if you ran these API v1 commands using the old format:

**https://<LoadMasterIPAddress>/access/listapi**

**https://<LoadMasterIPAddress>/access/set?param=enable&value=1**

Any parameters given to the **accessv2** request are ignored. For example, **<LoadMasterIPAddress>/accessv2/example** is the same as **<LoadMasterIPAddress>/accessv2**.

If a command requires binary data, for example a certificate, this data must be passed in the "data" string and be base64-encoded.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

If a command returns binary data, this is returned as a base64-encoded string. This field normally has the name "data".

## 2.3 Security

An application can only access the LoadMaster using the standard WUI IP address. Security is provided in exactly the same way as over the standard WUI, that is, valid credentials must be passed on every access when using Basic Authentication.

The user **bal** naturally has access to all functionality; other users have access to the subsystems that have been assigned to them using the LoadMaster permissions.

Currently there is no way to modify user permissions using this interface.

Depending on security settings and whether the browser has ever connected to the WUI before adding login information may be required. In this case instead of a standard command format such as:

**https://<LoadMasterIPAddress>/access/<command>?params**

the login information would need to be included, for example:

**https://<UserName>:<UserPassword>@<LoadMasterIPaddress>/access/<command>?params**

You can also use certificate-based authentication or API keys.

For instructions on how to use certificate based authentication, refer to the **Configure Certificate-Based Authentication** section.

For instructions on how to use API keys, refer to the **How to Use API Keys** section.

### 2.3.1 Configure Certificate-Based Authentication

Follow the steps in the sections below to configure certificate-based authentication.

Certificate-based authentication is not supported in version 2 of the API (which is currently in beta).

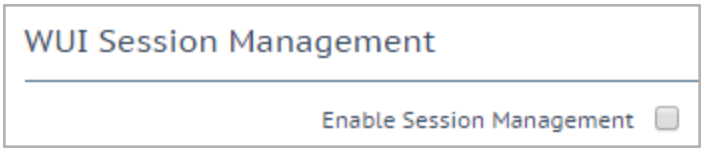
Certificate-based authentication will be deprecated for version 1 at some point in the future. Instead, use API keys. For further details, refer to the **How to Use API Keys** section.

#### 2.3.1.1 Enable Session Management

You must enable **Session Management** before you can enable client certificate authentication. To enable Session Management, follow the steps below:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

1. In the main menu of the LoadMaster WUI, navigate to **Certificates & Security > Admin WUI Access**.




2. Select the **Enable Session Management** check box.

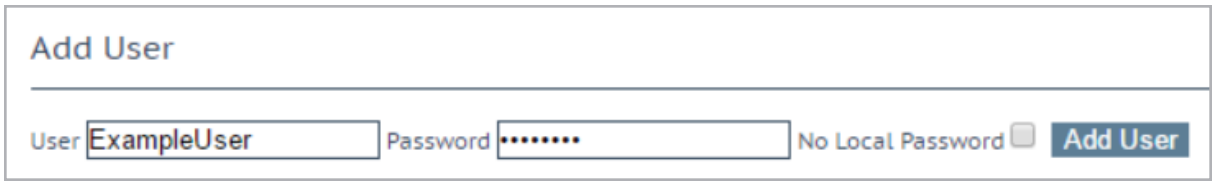
> After this check box is selected, you must log in to continue using the LoadMaster.

3. Configure any other settings as needed.

#### 2.3.1.2 Create a User (If Needed)

It is not possible to use certificate-based authentication with the **bal** user. However, you can create a non-**bal** user and grant it **All Permissions**, or whatever permissions you want. If you do not already have another user created, you can add one by following these steps:

1. In the main menu of the LoadMaster WUI, expand **System Configuration > System Administration** and click **User Management**.




2. At the bottom of the screen, enter a username in the **User** text box.

3. At this point, you can either set a **Password** for the new user, or select the **No Local Password** check box.

> For further information on the **No Local Password** option and on certificate authentication in general, refer to the User Management, Feature Description.

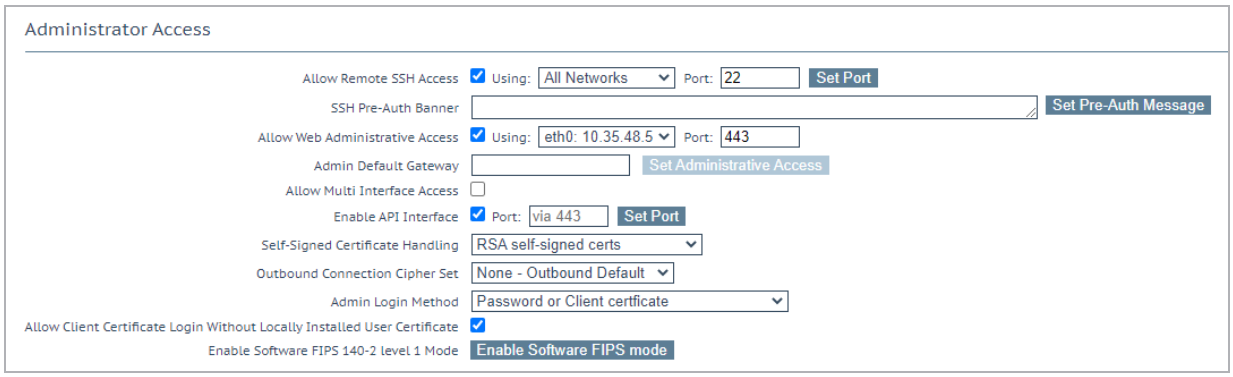
4. Click **Add User**.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 2.3.1.3 Enable Client Certificate Authentication on the LoadMaster

A number of different login methods are available to enable. For steps on how to set the **Admin Login Method**, along with a description of each of the available methods, refer to the steps below:

1. In the main menu of the LoadMaster WUI, expand **Certificates & Security** and click **Remote Access**.




2. Select the relevant **Admin Login Method**.

> The **Pre-Auth Click Through Banner** in the **Admin WUI Access** screen must be set for all **Admin Login Method** options to be made available.

> Using local certificates only works with API authentication. Because of this, it might be best to select the **Password or Client certificate** option. This enables API access using the client certificate and WUI access using the username/password.

The following login methods are available:

- **Password Only Access (default):** This option provides access using the username and password only – there is no access using client certificates.
- **Password or Client certificate: You** can log in either using the username/password or using a valid client certificate. If a valid client certificate is in place, the username and password is not required.
  The LoadMaster asks the client for a certificate. If a client certificate is available, the LoadMaster checks for a match. The LoadMaster checks if the certificate matchesone of the local certificates, or checks if the Subject Alternative Name (SAN) or Common Name (CN) of the certificate is a match. The SAN is used in preference to the CN when performing a match. If


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- there is a match, you are granted access to the LoadMaster. This works both using the API and user interface.
  An invalid certificate will not allow access.
  If no client certificate is supplied, the LoadMaster expects that a username and password is supplied (for the API) or will request a password using the standard WUI login page.
- **Client certificate required:** Access is only allowed with the use of a client certificate. It is not possible to log in using the username and password. SSH access is not affected by this (only the **bal** user can log in using SSH).
- **Client certificate required (Verify via OCSP):** This is the same as the **Client certificate required** option, but the client certificate is verified using an OCSP service. You must configure the OCSP Server Settings for this to work. For further information on the OCSP Server Settings, refer to the SSL Accelerated Services, Feature Description.

Some points to note regarding the client certificate methods are below:

- The **bal** user does not have a client certificate. Therefore, it is not possible to log into the LoadMaster as **bal** using the **Client certificate required** methods. However, a non-**bal** user can be created and granted **All Permissions**. This will allow the same functionality as the **bal** user.
- There is no log out option for users that are logged in to the WUI using client certificates, as it is not possible to log out (if the user did log out the next access would automatically log them back in again). The session terminates when the page is closed, or when the browser is restarted.

#### 2.3.1.4 Generate and Download the Client Certificate

To generate a local certificate, follow the steps below:

> Users with **User Administration** permissions are able to manage local certificates for themselves and other users.

1. In the main menu of the LoadMaster WUI, navigate to **System Configuration > System Administration > User Management**.



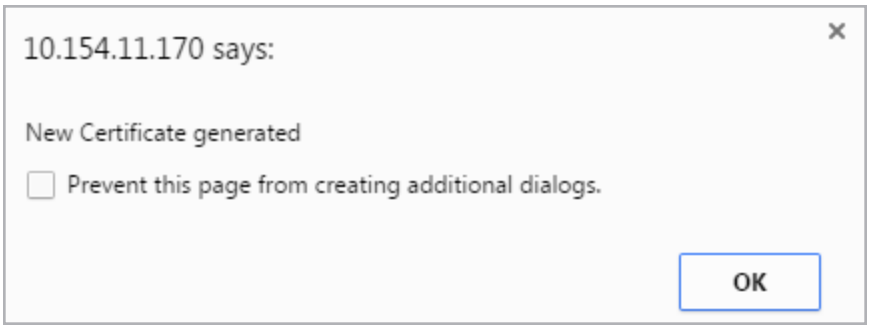

2. Click **Modify** on the relevant user.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

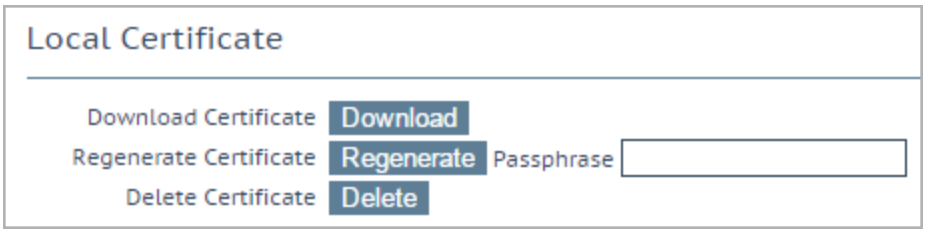



3. Enter a **Passphrase** and click **Generate**.

> Entering a passphrase is optional. If a passphrase is entered, it is used to encrypt the private key.




4. Click **OK** to the pop-up message that appears.




5. Click **Download**.

You can also regenerate from this screen.

#### 2.3.1.5 Specify the Certificate Details in the API

After configuring all of the options as outlined in the above sections, you must specify the details of the certificate to run the API commands successfully. You must also run the command as a cURL command, for example:

```
curl -k -E <PathToCertificateFile>/<CertificateFilename>.pem
https://172.21.59.100/access/get?param=version
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 2.3.1.6 Create a PFX File (If Running Commands using a Web Browser)

If you are running the RESTful APIs from the command line – you can use the PEM file, as indicated in the **Specify the Certificate Details in the API** section. If you want to run RESTful API commands using a web browser, you need to create a PFX file and import that into the browser.

You can convert the .pem file to .pfx any way you like. For the purposes of this document, we have provided steps on how to do it using OpenSSL. If you are using Windows, you may need to install OpenSSL to run these steps.

To create a .pfx file using, follow the steps below:

1. Open the .pem certificate.
2. Copy from the start of the **-----BEGIN CERTIFICATE-----** section to the end of the **-----END CERTIFICATE-----** section.
3. Paste this text into a new file.
4. Save the file as **<CerFileName>.cer**.
5. Go to the .pem certificate file again.
6. Copy from the start of the -----BEGIN RSA PRIVATE KEY----- section to the end of the -----END RSA PRIVATE KEY----- section.
7. Paste this text into a new file.
8. Save the file as **<KeyFileName>.key**.
9. Use the **openssl** command to create the .pfx file:

```
openssl pkcs12 -export -out <NewFileName>.pfx -inkey <KeyFilename>.key -in <CerFileName>.cer
```

10. Import the certificate to the web browser.

### 2.3.2 How to Use API Keys

When running API commands, you can authenticate using an API key. An API key is a unique identifier used to authenticate a user.

To generate an API key, run the following command:

```
https://<LoadMasterIPAddress>/access/addapikey
```

A list of API keys is returned. You can have up to 16 API keys per user - if you try to create more, the oldest is deleted.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

When you have an API key, you can perform any command as normal, but you no longer need the username or password. For example:

```
https://<LoadMasterIPAddress>/access/listvs?&apikey=<APIKey>
```

You can list the API keys by running the following command:

```
https://<LoadMasterIPAddress>/access/listapikeys?&apikey=<APIKey>
```

#### 2.3.2.1 Delete an API Key

You can delete an API key by running the following command:

```
https://<LoadMasterIPAddress>/access/delapikey?&key=<APIKeyToDelete>
```

You must specify an API key or a username and password to validate the request. The various options for running this command are detailed below.

```
curl -k
"https://<LoadMasterIPAddress>/access/delapikey?apikey=<ValidAPIKey>&key=<API
KeyToDelete>"
```

The above example assumes that the access **apikey** and the **key** to delete belong to the same user.

```
curl -k -u <Username>:<Password>
"https://<LoadMasterIPAddress>/access/delapikey?key=<APIKeyToDelete>"
```

The above example assumes the user whose username is specified owns the API key to delete.

```
curl -k -u <Username>:<Password>
"https://<LoadMasterIPAddress>/access/delapikey?key=<APIKeyToDelete>&user=<Ow
nerOfKey>"
```

The above example is usually performed by the **bal** user. For example:

```
curl -k -u bal:<Password>
"https://<LoadMasterIPAddress>/access/delapikey?key=<APIKeyToDelete>&user=<Ow
nerOfKey>"
```

The following example using an API key to authenticate is also valid:

```
curl -k
"https://<LoadMasterIPAddress>/access/delapikey?apikey=<ValidAPIKey>&key=<API
KeyToDelete>&user=<OwnerOfKey>"
```

> The user performing the delete command must have the **User Administration** permission.

## 2.4 Enabling the LoadMaster RESTful API Interface

The RESTful API interface is enabled or disabled using the LoadMaster WUI. By default the interface is disabled.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

To enable the RESTful API interface complete the following steps:

1. Select the **Certificates & Security > Remote Access** menu option.
2. Select the **Enable API Interface** checkbox.

## 2.5 Using get and set commands

Several parameters can be managed using the **set** and **get** commands. These parameters are described throughout the document. A list of parameters is also provided in **List All API Commands and get/set Parameters**.

Values of parameters can be obtained using the **get** command using the format

**https://<LoadMasterIPAddress>/access/get?param=<ParameterName>**

Values of parameters can be set using the **set** command using the format

**https://<LoadMasterIPAddress>/access/set?param=<ParameterName>&value=<ParameterValue>**

## 2.6 Error Reports

If an error occurs, for example where a request is missing the **param** value, an error report is generated as follows:

```
------------------------------------------------------------
<?xml version="1.0" encoding="ISO-8859-1"?>
<Response stat="400" code="fail">
    <Error>
    param: String Value missing
    </Error>
</Response>

------------------------------------------------------------
```

The HTTP status of the request also reflects the response code.

## 2.7 Notation

Throughout the document the parameter types are defined as follows:

| Type | Abbreviation | Typical Values |
|---|---|---|


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| Boolean | B | Y or N; y or n; 1 or 0; |
| Integer | I | <minint>-<maxint> |
| String | S | "value" |
| Address | A | IP-address |
| File | F | Some type of file |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# 3 RESTful API Commands

## 3.1 Command Syntax

A request is made up of two parts: the command and the parameters.

**https://<LoadMaster IP address>/access/<command>?params**

When there is more than one parameter in a request, individual parameters are separated using an ampersand (**&**) symbol.

All commands are consistent. For example in all places where a Virtual Service is required, the IP address of a Virtual Service is specified by using **vs=<ipaddr>**, for example, to show a Virtual Service, the command could be:

**https://<LoadMasterIPAddress>/access/showvs?vs=10.0.0.10&port=80&prot=tcp**

To show a Real Server on a Virtual Service:

**https://<LoadMasterIPAddress>/access/showrs?vs=10.0.0.10&port=80&prot=tcp&rs=99.1.1.1&rsport=80**

## 3.2 List All API Commands and get/set Parameters

To list all available API commands and the currently installed LoadMaster version, run the following command:

**https://<LoadMasterIPAddress>/access/listapi**

Several parameters can be retrieved and configured using the get and set commands. For further information on the get and set commands, refer to the following section: **Using get and set commands**.

The **getall** command returns a list of all parameters that are available (and that are not null):

**https://<LoadMasterIPAddress>/access/getall**

## 3.3 Home Screen Information

Some information which is available in the LoadMaster WUI is also available using the API. Refer to the sub-sections below for further details.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

### 3.3.1 Retrieve the LoadMaster Firmware Version

The LoadMaster firmware version can be obtained using the **get** command and the **version** parameter:

**https://<LoadMasterIPAddress>/access/get?param=version**

### 3.3.2 Retrieve the Boot Time and Active Time

The boot time is the time at which the LoadMaster last booted. The boot time and active time are the same when a LoadMaster is not running in HA mode. When in HA mode, the active time is the time at which the LoadMaster last became the active unit. The active time will be zero if the LoadMaster is in standby mode. To retrieve these values, run the following commands:

**https://<LoadMasterIPAddress>/access/get?param=boottime**
**https://<LoadMasterIPAddress>/access/get?param=activetime**

### 3.3.3 Retrieve the Serial Number

To retrieve the LoadMaster serial number, run the **get** command for the **serialnumber** parameter:

**https://<LoadMasterIPAddress>/access/get?param=serialnumber**

### 3.3.4 Retrieve the Virtual Service and Real Service Statuses

To retrieve the total numbers of Virtual Services, SubVSs and Real Servers that are up, down and administratively disabled, run the **vstotals** command:

**https://<LoadMasterIPAddress>/access/vstotals**

### 3.3.5 Retrieve Licensing Information

To retrieve details about the LoadMaster license and subscription, run the **licenseinfo** command:

**https://<LoadMasterIPAddress>/access/licenseinfo**

## 3.4 Initial Configuration

> The initial configuration API commands are not valid for pay-per-use cloud LoadMasters. They are valid for Bring Your Own License (BYOL) cloud LoadMasters.

A number of steps are involved in initially deploying a LoadMaster, such as accepting the End User License Agreement (EULA) and licensing the unit. Before the LoadMaster can be fully deployed the user must display and accept the EULA. These initial configuration steps can either be performed using the WUI or the API. The API commands relating to initial configuration are listed in the sections below.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These commands should be run in sequential order

### 3.4.1 Read the EULA

The ReadEula command displays the EULA and a magic cookie.

The magic cookie is used for security reasons - it limits the possibility of remote attacks. If a command requires the magic cookie (like some of the other ones in the sections below) and does not get the correct magic cookie from the previous command, the command will fail.

```
https://<LoadMasterIPAddress>/access/readeula
```

The magic string is an automatically generated random string. Copy this string because it will be needed in the next command to set the license type.

### 3.4.2 Accept the EULA and Set the License Type

Currently there are three license types available from Kemp. These are:

- Trial (Unrestricted)
- Perpetual
- Free (Restricted)

When running the **AcceptEULA** command, you enter the magic cookie key returned by the readEula command. The **AcceptEULA** command accepts the EULA and sets the type of license used, for example **Trial**, **Perm** or **Free**.

The **type** parameter must be set when running the **accepteula** command. The **type** set depends on the type of LoadMaster you are deploying.

```
https://<LoadMasterIPAddress>/access/accepteula?magic=<CorrectMagicString>&type=free
```

| Value | Description |
|---|---|
| Trial | Temporary license for users evaluating the Kemp LoadMaster |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | |
|---|---|
| Perm | Purchased permanent LoadMaster |
| Free | Free LoadMaster |

If running this command on a Virtual LoadMaster (VLM) which has been created in the Multi-Tenant LoadMaster product, the license type set here is irrelevant because the license type will be inherited from the Multi-Tenant LoadMaster. However, this command still needs to be run to get another magic string which is needed to run the next command (**AcceptEula2**).

### 3.4.3 Retrieve the Available License Types

To retrieve a list of available license types for a particular Kemp ID, run the **alsilicensetypes** command:

```
https://<LoadMasterIPAddress>/access/alsilicensetypes?kempid=<KempID>&password=<PasswordForKempID>&orderid=<OrderID>
```

The **orderid** parameter is only needed for Virtual LoadMasters.

If successful, the output provides a list of license types and associated IDs. The ID number is used when licensing using the **alsilicense** command.

### 3.4.4 License the LoadMaster

The LoadMaster can be licensed using the **license** or **alsilicense** commands. For further information, please refer to the **Licensing** section.

### 3.4.5 Set the Initial Password

The **Set_Initial_Passwd** command is used to set the password of the default LoadMaster user (**bal**).

```
https://<LoadMasterIPAddress>/access/set_initial_passwd?passwd=<password1>
```

| Parameter | Parameter Type | Description | Mandatory |
|---|---|---|---|
| Passwd | String | This is the password for the default administrator user (**bal**). The password should contain at least 8 alphanumeric characters. | Yes |

If you are licensing using Kemp 360 Central, you may need to use the **usersetsyspassword** command instead:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

**https://<LoadMasterIPAddress>/access/usersetsyspassword?currpassword=<Initial Password>&password=<NewPassword>**

Refer to the following table to determine what command you should use:

| LoadMaster Version | Kemp 360 Central version >= V2.3 | Kemp 360 Central version < V2.3 |
|---|---|---|
| LoadMaster >= V7.2.47 | Use **usersetsyspassword** | Use **set_initial_password** |
| LoadMaster < V7.2.47 | Use **set_initial_password** | Use **set_initial_password** |

To future-proof any existing LoadMaster deployment scripts you may have, modify the scripts to first use **set_initial_password** to attempt setting the bal password. If that fails, use **usersetsyspassword**.

If you are trying to license LoadMaster version 7.2.46 against a version of Kemp 360 Central that is above V2.3, you will not be able to log into the WUI after setting the password using the API. To work around this, you must run the following command after running the **set_initial_password** command:

**https://<LoadMasterIPAddress>/access/set?param=motd&value=**

## 3.5 Licensing using the Activation Server Functionality

You can license locally if using Kemp 360 Central with Activation Server functionality.

To retrieve a list of available license types, use the **aslgetlicensetypes** command:

**https://<LoadMasterIPAddress>/access/aslgetlicensetypes?aslhost=<Kemp360CentralHostOrIPAddress>&aslport=<Kemp360CentralPort>**

> The **aslhost** parameter was introduced in LoadMaster firmware version 7.2.43. The parameters previously used were called **aslipaddr** and **aslname**. If you have scripts using these old parameters, you will need to update them to use the new **aslhost** parameter if upgrading.

For example:

**https://10.35.47.20/access/aslgetlicensetypes?aslhost=10.35.44.19&aslport=443**

After running the **aslgetlicensetypes** command, a list of available license types with license IDs is displayed:

```
<Response stat="200" code="ok">
<Success>{"categories": [{"description": "Licenses from Kemp 360 ASL Server",
"licenseTypes": [
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

{"id": "2", "name": "VLM-MAX", "description": "VLM-MAX", "available": 1}
]}]}</Success>
</Response>

To activate the license, use the **aslactivate** command and specify the license type ID:

**https://<LoadMasterIPAddress>/access/aslactivate?lic_type_id=<LicenseTypeID>**

For example:

**https://10.35.47.20/access/aslactivate?lic_type_id=2**

For compatibility across releases, the **lic_id_type** and the **licensetypeid** can be used interchangeably in any command where a license type ID is required. Therefore, the above command synopsis could also be shown as:

**https://<LoadMasterIPAddress>/access/aslactivate?licensetypeid=<LicenseTypeID>**

For example:

**https://10.35.47.20/access/aslactivate?licensetypeid=2**

## 3.6 Virtual Services

### 3.6.1 Virtual Service Control

The basic forms of the Virtual Services commands are below. Virtual Services can be addressed either by using the IP address or the index (ID). The index is a numerical value that tracks the Virtual Service internally.




The index can be displayed by using the **showvs** or **listvs** command or, alternatively by checking the Virtual Service properties screen in the WUI, which displays the Virtual Service ID.

**https://<LoadMasterIPAddress>/access/listvs**
**https://<LoadMasterIPAddress>/access/showvs?vs=<IPaddr>&port=<Port>&prot=<tcp/udp>**
**https://<LoadMasterIPAddress>/access/showvs?vs=<index>**
**https://<LoadMasterIPAddress>/access/addvs?vs=<IPaddr>&port=<Port>&prot=<tcp/udp>[&...]**
**https://<LoadMasterIPAddress>/access/delvs?vs=<IPaddr>&port=<Port>&prot=<tcp/udp>**
**https://<LoadMasterIPAddress>/access/delvs?vs=<index>**
**https://<LoadMasterIPAddress>/access/modvs?vs=<IPaddr>&port=<Port>&prot=<tcp/udp>[&...]**
**https://<LoadMasterIPAddress>/access/modvs?vs=<index>[&...]**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

The **delvs** command returns an OK status on success; otherwise the commands return the current settings of the Virtual Service.

The **addvs** and **modvs** command both allow the user to modify all the settings of a Virtual Service. The **addvs** command will first create the Virtual Service - while **modvs** will modify an existing Virtual Service.

> Frequently adding or deleting Virtual Services at a high velocity is not the recommended best practice. If you need to modify parameters, use the **modvs** command. If you need to constantly modify Virtual Service IP addresses, moving to FQDNs (rather than IP addresses) is the recommended best practice.

The **listvs** command lists all Virtual Services on the LoadMaster.

(When creating a new Virtual Service, the default values set are non-transparent and subnet originating - except for UDP services, which are transparent (force L4).)

When the status of the Virtual Service is returned, the Real Servers associated with the Virtual Service are also returned.

> Some commands depend on other commands as a prerequisite. If the prerequisites are not met, the command will do nothing.

> Not all parameters are applicable on all setups. The parameters available for use depends on the configured environment

The **dupvs** command duplicates the Virtual Service. For example:

**https://<LoadMasterIPAddress>/dupvs?vs=<VSIP>&port=<Port>&prot=<tcp/udp>&newport=<Port>&newvs=<NewVSIP>**

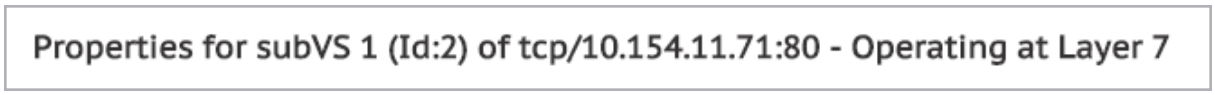
You can also specify the Virtual Service **Index** number in the **vs** parameter for the Virtual Service to be copied:

**https://<LoadMasterIPAddress>/access/dupvs?vs=<VSIndex>&newport=<Port>&newvs=<NewVSIP>**

**Sub-Virtual Services (SubVSs)**

The Virtual Service commands can be used on SubVSs also. However, as SubVSs do not have IP addresses, the SubVS index must be used. The SubVS index can be found using the **listvs** command.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.




Alternatively, check the ID SubVS properties screen in the WUI by clicking modify on a SubVS. In the example above, the SubVS ID is **2**.

To display details about a particular SubVS, run the following command:

**https://<LoadMasterIPAddress>/access/showvs?vs=<SubVSindex>**

A new SubVS can be added by running one of the following commands:

**https://<LoadMasterIPAddress>/access/modvs?vs=<VSIP>&port=<Port>&prot=<tcp/udp>&createsubvs=**
**https://<LoadMasterIPAddress>/access/modvs?vs=<index>&createsubvs=**

A SubVS can be deleted from a Virtual Service by running the following command:

**https://<LoadMasterIPAddress>/access/delvs?vs=<VSindex>**

A Real Server can be deleted from a SubVS by running the following command:

**https://<LoadMasterIPAddress>/access/delrs?vs=<SubVSindex>&rs=%21<RSindex>**

A SubVS can be duplicated within the same Virtual Service by running the following command:

**https://<LoadMasterIPAddress>/access/dupvs?vs=<SubVSindex>**

To modify SubVS settings, run the following command:

**https://<LoadMasterIPAddress>/access/modvs?vs=<SubVSindex> [&...]**

SubVS index is an integer value.

Frequently adding or deleting Real Servers or SubVSs at a high velocity is not the recommended best practice. If you need to modify parameters, use the **modrs** command. If you need to constantly modify Real Server IP addresses, moving to FQDNs (rather than IP addresses) is the recommended best practice.

The parameters that can be set in the **addvs** and **modvs** commands are described in the sections below. For ease of use, the parameters have been broken into sections based on where the corresponding field appears in the WUI.

#### 3.6.1.1 Properties

| Name | Type | Default | Range | Description |
|---|---|---|---|---|


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| Port | I | <unset> | 3-65530, * | The port for the Virtual Service. A wildcard port can also be specified by using an asterisk (*).<br><br>The **port** parameter is used to assign a port when initially creating a Virtual Service. If modifying the port of an existing Virtual Service, specify the existing port as the **port** parameter and use the **vsport** parameter to assign the new port.<br><br>The reason why these must be separate parameters is because you need to specify what the port of the existing Virtual Service is (because there may be another Virtual Service with the same IP address but a different port) and if you want to change the port, a second port parameter (VSPort) is needed to specify the new port value. |
| VSPort | I | <unset> | 3-65530, * | The port for the Virtual Service.<br><br>The **port** parameter is used to assign a port when initially creating a Virtual Service. If modifying the port of an existing Virtual Service, specify the existing port as the **port** parameter and use the **vsport** parameter to assign the new port.<br><br>The reason why these must be separate parameters is because you need to specify what the port of the existing Virtual Service is (because there may be another Virtual Service with the same IP address but a different port) and if you want to change the port, a second port parameter (VSPort) is needed to specify the new port value. |
| Protocol | S | <unset> | udp, tcp | The protocol to be used for the Virtual Service. |
| VSAddress | A | Address | | The IP address of the Virtual Service. |
| MasterVS | I (Read Only) | <unset> | 0 – Not a parent Virtual Service | Signifies whether or not the Virtual Service is a parent Virtual Service (that is, if it has one or more SubVSs). |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | 1 – Is a parent Virtual Service | |

### 3.6.1.2 Basic Properties

| Name | Type | Default | Range | Description |
|---|---|---|---|---|
| Enable | B | Y | | Activate or deactivate the Virtual Service |
| VStype | S | <port dependent> | gen - Generic<br>http - HTTP/HTTPS<br>http2 - HTTP/2<br>ts - Remote Terminal<br>tls – STARTTLS protocols<br>log – Log Insight | Specifies the type of service being load balanced. |
| NickName | S | <unset> | | Specifies the "friendly" name of the service.<br>In addition to the usual alphanumeric characters, the following ‘special’ characters can be used as part of the Service Name:<br>**. @ - _**<br>You cannot use a special character as the first character of the Service Name. |

### 3.6.1.3 Standard Options

| Name | Type | Default | Range | Description |
|---|---|---|---|---|


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| Cookie | S | <unset> | | This parameter is only relevant when the persistence mode is set to **cookie**, **active-cookie**, **cookie-src** or **active-cook-src**. Enter the name of the cookie to be checked. |
| ForceL7 | B | Y (if not UDP) | 0 - Disabled<br>1 - Enabled | Enabling **ForceL7** means the Virtual Service runs at Layer 7 and not Layer 4. This may be needed for various reasons, including that only Layer 7 services can be non-transparent. |
| Idletime | I | 660 | 0-86400 | Specifies the length of time (in seconds) that a connection may remain idle before it is closed. The range for this parameter is 0 to 86400.<br>Setting the **Idletime** to 0 ensures the default L7 connection timeout is used. You can modify the default timeout value by setting the **ConnTimeout** parameter. |
| Persist | S | none | The list of relevant persist values are:<br>• ssl<br>• cookie<br>• active-cookie<br>• cookie-src<br>• active-cook-src<br>• cookie-hash | Specify the type of persistence (stickiness) to be used for this Virtual Service.<br>**Note:** If setting the persistence mode to an option that requires a cookie (or query-hash), the **cookie** parameter must also be set. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | • cookie-hash-src<br>• url<br>• query-hash<br>• host<br>• header<br>• super<br>• super-src<br>• src<br>• rdp<br>• rdp-src<br>• rdp-sb<br>rdp-sb-src<br>none<br>udpsip | |
| SubnetOriginating | B | 0 | 0 – Disabled<br>1 – Enabled | When transparency is not enabled, the source IP address of connections to the Real Servers is that of the Virtual Service. When transparency is enabled, the source IP address will be the IP address that is initiating connection to the Virtual Service. If the Real Server is on a subnet, and the Subnet Originating Requests option is enabled, then the subnet address of the LoadMaster will be used as the source IP address. |
| PersistTimeout | I | 0 | 0-2419200 | The length of time (in seconds) after the last connection that the LoadMaster will remember the persistence information. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | Timeout values are rounded down to an even number of minutes. Setting a value that is not a number of whole minutes results in the excess being ignored. Setting a value to less than 60 seconds results in a value of 0 being set, which disables persistency. |
| Refreshpersist | B | | 0 – Disabled<br>1 – Enabled | When this parameter is enabled, it keeps auto-refreshing persist entries for long lived connections. |
| QueryTag | S | <unset> | | This is the query tag to be matched if the **Persist type** is set to **query-hash**. |
| Schedule | S | rr | rr<br>wrr<br>lc<br>wlc<br>fixed<br>adaptive<br>sh<br>dl<br>sdn-adaptive<br>uhash | Specify the type of scheduling of new connections to Real Servers that is to be performed. The valid values are spelled out below:<br>rr = round robin<br>wrr = weighted round robin<br>lc = least connection<br>wlc = weighted least connection<br>fixed = fixed weighting<br>adaptive = resource based (adaptive)<br>sh = source IP hash<br>dl = weighted response time<br>sdn-adaptive = resource based (SDN adaptive)<br>uhash = URL hash |
| ServerInit | I | 0 | 0-6 | By default, the LoadMaster will not initiate a connection with a Real Server until it has received some data from a client. This prohibits certain protocols from working |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | as they need to communicate with the Real Server before transmitting data.<br><br>If the Virtual Service uses one of these protocols, specify the protocol using the ServerInit parameter to enable it to work correctly.<br><br>0 = Normal Protocols<br><br>1 = SMTP<br><br>2 = SSH<br><br>3 = Other Server Initiating<br><br>4 = IMAP4<br><br>5 = MySQL<br><br>6 = POP3 |
| Transparent | B | Y | 0 - Disabled<br><br>1 - Enabled | When using Layer 7, when this is enabled - the connection arriving at the Real Server appears to come directly from the client. Alternatively, the connection can be non-transparent which means that the connections at the Real Server appear to come from the LoadMaster.<br><br>If a Virtual Service (with or without a SubVS) has SSL re-encrypt enabled, the transparency flag of the Virtual Service has no meaning (re-encryption forces transparency to be off). The transparency setting can still be modified by the API, and is honored when re-encrypt is disabled on the Virtual Service. |
| UseforSnat | B | N | 0 – Disabled<br><br>1 – Enabled | By default, when the LoadMaster is being used to NAT Real Servers, the source IP address used on the Internet is that of the LoadMaster. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | Enabling this option allows the Real Servers configured to use the Virtual Service as the source IP address instead.<br><br>If the Real Servers are configured on more than one Virtual Service which has this option set, only connections to destination port 80 will use this Virtual Service as the source IP address. |
| QoS | S | 0 – Normal Service | 0 - Normal-Service<br><br>1 - Minimize-Cost<br><br>2 - Maximize-Reliability<br><br>4 - Maximize-Throughput<br><br>8 - Minimize-Delay<br><br>16 - Pass Through | The Quality of Service (QoS) parameter sets a Type of Service (ToS) in the IP header of packets that leave the Virtual Service. This means that the next device or service that deals with the packets will know how to treat and prioritise this traffic. Higher priority packets are sent from the LoadMaster before lower priority packets. |
| StartTLSMode | I | | 0-6 | 0 = HTTP/HTTPS (the **Service Type** needs to be set to **HTTP/HTTPS** for this to work)<br><br>The Virtual Service Type must be set to STARTTLS for the remaining values to be set:<br><br>1 = SMTP (STARTTLS if requested)<br><br>2 = SMTP (STARTTLS always)<br><br>3 = FTP<br><br>4 = IMAP<br><br>6 = POP3 |
| ExtraPorts | S | <unset> | 3-65530 | Specify extra ports that the Virtual Service |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | will listen to. To remove any existing extra ports, set the **ExtraPorts** parameter to an empty string. |

When setting the persistence method to **cookie**, **active-cookie**, **cookie-src** or **active-cook-src**, the cookie name must also be set within the command.
For example:
**https://<LoadMasterIPAddress>/access/modvs?vs=10.0.2.194&port=80&prot=tcp&persist=cookie&cookie=<cookie name>&**

#### 3.6.1.4 SSL Properties

| Name | Type | Default | Range | Description |
|---|---|---|---|---|
| CertFile | S | <unset> | | A list of certificate identifiers, separated by spaces. When used with the **addvs** command, all certificates required for the VS must be specified in a single space-separated list. Similarly, when using the **modvs** command, the entire list of certificates required for the VS must be specified.<br><br>There is a limit of 8099 characters when assigning certificates to a Virtual Service using the API. |
| Ciphers | S | Default assignment | All supported ciphers | Multiple ciphers can be assigned by inserting a colon between each cipher. When ciphers are assigned in this way, a **Cipher Set** called **Custom_<VirtualServiceID>** will be created/updated.<br><br>**Note:** The assigned ciphers list will be overwritten when ciphers are added in this way. Ensure to include all ciphers to be assigned.<br><br>**Note:** Do not try to set the **CipherSet** parameter and the **Ciphers** parameter at the same time - |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | use one or the other. Custom cipher sets can be created using a different command. For more information, refer to the **Modify a Custom Cipher Set/Create a New Custom Cipher Set** section |
| CipherSet | S | Default | All available cipher sets | This parameter can be used to assign a cipher set to a Virtual Service. System-defined cipher sets and custom cipher sets can be assigned using this parameter. The valid values are below:<br>■Default<br>■Default_NoRc4<br>■BestPractices<br>■Intermediate_compatibility<br>■Backward_compatibility<br>■WUI<br>■FIPS<br>■Legacy<br>■Null_Ciphers<br>■ECDSA_Default<br>■ECDSA_BestPractices<br>■<NameOfCustomCipherSet><br>Do not try to set the **CipherSet** parameter and the **Ciphers** parameter at the same time - use one or the other. Custom cipher sets can be created using a different command. For more information, refer to the **Modify a Custom Cipher** |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | **Set/Create a New Custom Cipher Set** section. |
| Tls13CipherSet | S | | All TLS1.3 available cipher sets | This parameter can be used to assign TLS1.3 cipher sets to a Virtual Service. Multiple ciphers can be specified using a space and colon separated list. You cannot unset this parameter - at least one cipher set must be specified.<br>The list of supported TLS1.3 Ciphers (and valid values) is as follows:<br>- TLS_AES_256_GCM_SHA384<br>- TLS_CHACHA20_POLY1305_SHA256<br>- TLS_AES_128_GCM_SHA256<br>- TLS_AES_128_CCM_8_SHA256<br>- TLS_AES_128_CCM_SHA256 |
| ClientCert | I | 0 | 0-6 | 0 = No client certificates required<br>1 = Client certificates required<br>2 = Client certificates and add headers<br>3 = Client Certificates and pass DER through as SSL-CLIENT-CERT<br>4 = Client Certificates and pass DER through as X-CLIENT-CERT<br>5 = Client Certificates and pass DER through as SSL-CLIENT-CERT<br>6 = Client Certificates and pass PEM through as X-CLIENT-CERT |
| PassCipher | B | | 0 - Disabled<br>1 - Enabled | When this parameter is enabled, the LoadMaster adds X-SSL headers containing client SSLinformation such as TLS version, TLS cipher, client certificate serial number, and SNI host.<br>Note: SSLAcceleration must be enabled to |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | enable the PassCipher parameter. |
| SSLReencrypt | B | N | 0 - Disabled<br>1 - Enabled | This parameter is only relevant if **SSL Acceleration** is enabled.<br>When this option is enabled, the SSL data stream is re-encrypted before sending to the Real Server. |
| PassSNI | B | | 0 - Disabled<br>1 - Enabled | To enable or disable the **PassSNI** parameter. |
| SSLReverse | B | N | 0 - Disabled<br>1 - Enabled | Enabling this parameter means that the data from the LoadMaster to the Real Server is re-encrypted. |
| SSLRewrite | S | <unset> | <unset>, http, https | When the Real Server rejects a request with a HTTP redirect, the requesting Location URL may need to be converted to specify HTTPS instead of HTTP (and vice versa). |
| ReverseSNIHostname | S | <unset> | | Specify the SNI Hostname that should be used when connecting to the Real Servers. This parameter relates to the **Reencryption SNI Hostname** field in the WUI. |
| SecurityHeaderOptions | I | 0 - Don't add the Strict Transport Security Header | 0 - Don't add the Strict Transport Security Header<br>1 - Add the Strict Transport Security Header - no | Enable this option to add the Strict-Transport-Security header to all LoadMaster-generated messages (ESP and error messages).<br>**Note:** You can configure the maximum age for the message by setting the **SecurityHeaderAge** parameter.<br>To retrieve the current value of the SecurityHeaderAge parameter, run the following command:<br>**`/access/get?param=securityheaderage`** |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | subdomains<br>2 - Add the Strict Transport Security Header - include subdomains<br>4 - Add the Strict Transport Security Header - no subdomains + preload<br>6 - Add the Strict Transport Security Header - include subdomains + preload | To set the parameter, run the following command:<br>**`/access/set?param=securityheaderage&value=<value>`**<br>Valid values for this parameter range from **86400** (1 day) to **94608000** (2 years). |
| SSLAcceleration | B | N | 0 - Disabled<br>1 - Enabled | Enable SSL handling on this Virtual Service. |
| OCSPVerify | B | 0 – Disabled | 0 – Disabled<br>1 – | Verify (using Online Certificate Status Protocol (OCSP)) that the client certificate is valid. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | Enabled | |
| TLSType | B | Disabled if SSL Acceleration is not enabled.<br>TLS1.1, TLS1.2, and TLS1.3 are enabled when SSL Acceleration is enabled. | 0 – 30 bitmask | Specify which of the following protocols to support; SSLv3, TLS1.0, TLS1.1, TLS1.2, or TLS1.3. The protocols can be enabled and disabled using a bitmask value. Refer to the table below to find out what number corresponds to which settings. |
| NeedHostName | B | 0 – Disabled | 0 - Disabled<br>1 - Enabled | When this parameter is enabled, the hostname is always required to be sent in the TLS client hello message. If it is not sent, the connection will be dropped. |
| IntermediateCerts | S | By default all intermediate certificates are assigned | Valid cert names | Assign intermediate and root certificates to the specified Virtual Service. This provides the ability to restrict access. You cannot add a certificate to an already assigned list of certificates - all certificates that should be assigned to the Virtual Service must be specified in the one **modvs** command. If you enter more than one certificate name, separate them using a plus symbol (**+**). |

#### 3.6.1.4.1 TLSType Parameter

For the **TLSType** parameter, the protocols can be enabled and disabled using a bitmask value.

The valid bitmask values vary depending on whether the **SSLOldLibraryVersion** parameter is enabled or disabled. Refer to the relevant section below to find out what number corresponds to which settings.

**SSLOldLibraryVersion Disabled**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

If the **SSLOldLibraryVersion** parameter is disabled, the bitmask values and settings are as outlined in the table below:

| Number | SSLv3 | TLS1.0 | TLS1.1 | TLS1.2 | TLS1.3 |
|---|---|---|---|---|---|
| 0 | Enabled | Enabled | Enabled | Enabled | Enabled |
| 1 | Disabled | Enabled | Enabled | Enabled | Enabled |
| 2 | Enabled | Disabled | Enabled | Enabled | Enabled |
| 3 | Disabled | Disabled | Enabled | Enabled | Enabled |
| 4 | Enabled | Enabled | Disabled | Enabled | Enabled |
| 5 | Disabled | Enabled | Disabled | Enabled | Enabled |
| 6 | Enabled | Disabled | Disabled | Enabled | Enabled |
| 7 | Disabled | Disabled | Disabled | Enabled | Enabled |
| 8 | Enabled | Enabled | Enabled | Disabled | Enabled |
| 9 | Disabled | Enabled | Enabled | Disabled | Enabled |
| 10 | Enabled | Disabled | Enabled | Disabled | Enabled |
| 11 | Disabled | Disabled | Enabled | Disabled | Enabled |
| 12 | Enabled | Enabled | Disabled | Disabled | Enabled |
| 13 | Disabled | Enabled | Disabled | Disabled | Enabled |
| 14 | Enabled | Disabled | Disabled | Disabled | Enabled |
| 15 | Disabled | Disabled | Disabled | Disabled | Enabled |
| 16 | Enabled | Enabled | Enabled | Enabled | Disabled |
| 17 | Disabled | Enabled | Enabled | Enabled | Disabled |
| 18 | Enabled | Disabled | Enabled | Enabled | Disabled |
| 19 | Disabled | Disabled | Enabled | Enabled | Disabled |
| 20 | Enabled | Enabled | Disabled | Enabled | Disabled |
| 21 | Disabled | Enabled | Disabled | Enabled | Disabled |
| 22 | Enabled | Disabled | Disabled | Enabled | Disabled |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | | |
|---|---|---|---|---|---|
| 23 | Disabled | Disabled | Disabled | Enabled | Disabled |
| 24 | Enabled | Enabled | Enabled | Disabled | Disabled |
| 25 | Disabled | Enabled | Enabled | Disabled | Disabled |
| 26 | Enabled | Disabled | Enabled | Disabled | Disabled |
| 27 | Disabled | Disabled | Enabled | Disabled | Disabled |
| 28 | Enabled | Enabled | Disabled | Disabled | Disabled |
| 29 | Disabled | Enabled | Disabled | Disabled | Disabled |
| 30 | Enabled | Disabled | Disabled | Disabled | Disabled |

### SSLOldLibraryVersion Enabled

If the **SSLOldLibraryVersion** parameter is enabled, **TLS1.3** is not available and the range of the bitmask value is 0-14, as outlined in the table below.

| Number | SSLv3 | TLS1.0 | TLS1.1 | TLS1.2 |
|---|---|---|---|---|
| 0 | Enabled | Enabled | Enabled | Enabled |
| 1 | Disabled | Enabled | Enabled | Enabled |
| 2 | Enabled | Disabled | Enabled | Enabled |
| 3 | Disabled | Disabled | Enabled | Enabled |
| 4 | Enabled | Enabled | Disabled | Enabled |
| 5 | Disabled | Enabled | Disabled | Enabled |
| 6 | Enabled | Disabled | Disabled | Enabled |
| 7 | Disabled | Disabled | Disabled | Enabled |
| 8 | Enabled | Enabled | Enabled | Disabled |
| 9 | Disabled | Enabled | Enabled | Disabled |
| 10 | Enabled | Disabled | Enabled | Disabled |
| 11 | Disabled | Disabled | Enabled | Disabled |
| 12 | Enabled | Enabled | Disabled | Disabled |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| 13 | Disabled | Enabled | Disabled | Disabled |
| 14 | Enabled | Disabled | Disabled | Disabled |

Another way of determining the correct bitmask value to set for the **TLSType** parameter is outlined in the partial table and explanation below.

| **Dec Bit Values** | 16 | 8 | 4 | 2 | 1 | **Values Set** |
|---|---|---|---|---|---|---|
| | **TLS1.3** | **TLS1.2** | **TLS1.1** | **TLS1.0** | **SSLv3** | |
| **0** | off | off | off | off | off | All TLS types enabled |
| **3** | off | off | off | on | on | 1.1,1.2,1.3 enabled |
| **23** | on | off | on | on | on | Only TLS1.2 enabled |
| **15** | off | on | on | on | on | Only TLS1.3 enabled |

Here are some notes about the above table:

- For all TLS types that you want to enable, you leave the bit off and turn on the rest
- A value of 31 is not possible (all bits on) because you would be disabling all TLS types so valid values are 0 - 30
- When TLS1.3 is not available (if the **SSLOldLibraryVersion** is enabled) then the range becomes 0 - 15. However, 15 is not a valid value so the valid range is 0 - 14

Another way of thinking about this is by adding 16+8+4+2+1=31 and then whatever TLS type you want on, you subtract from 31.

If TLS 1.3 is not available, then you leave out the TLS 1.3 column above and add 8+4+2+1.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.6.1.5 Advanced Properties

| Name | Type | Default | Range | Description |
|---|---|---|---|---|
| HTTPReschedule | B | 0 - Disabled | 0 - Disabled<br>1 - Enabled | **Note:** This is an experimental feature. Do not enable it unless you speak to Kemp Support first.<br>**Note:** This parameter is not available in the PowerShell API module because it is experimental.<br>If this parameter is enabled and content switching is not in use, this forces the reselection of a Real Server for each request. By default, the Real Server is selected only once per connection.<br>The **Persist** parameter must be set to **none** to use the **HTTPReschedule** parameter. |
| CopyHdrFrom | S | <unset> | | This is the name of the source header field to copy into the new header field before the request is sent to the Real Servers. |
| CopyHdrTo | S | <unset> | | Used in conjunction with the **CopyHdrFrom** parameter.<br>The name of the header field into which the source header is to be |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | copied. |
| AddVia | I | | 0 = Legacy Operation (X-Forwarded-For)<br>1 = X-Forwarded-For (+ Via)<br>2 = None<br>3 = X-ClientSide (+ Via)<br>4 = X-ClientSide (No Via)<br>5 = X-Forwarded-For (No Via)<br>6 = Via Only | This corresponds to the **Add HTTP Headers** field in the WUI. Select which headers are to be added to HTTP requests. X-ClientSide and X-Forwarded-For are only added to non-transparent connections. |
| AllowHTTP2 | B | 0 – Disabled | 0 – Disabled<br>1 – Enabled | Enable HTTP2 for this Virtual Service. SSL Acceleration must be enabled before HTTP2 can be enabled. The Best Practices cipher set should be used when HTTP2 is enabled. |
| Cache | B | N | 0 - Caching Disabled<br>1 – Caching | Enable or disable the caching of URLs. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | Enabled | |
| Compress | B | N | 0 – Disabled<br>1 - Enabled | When enabled, files sent from the LoadMaster are compressed with Gzip. |
| CachePercent | I | 0 | 0-100 | This parameter is only relevant if caching is enabled. Specify the maximum percentage of cache space permitted for this Virtual Service. |
| DefaultGW | A | <unset> | | Specify the Virtual Service-specific default gateway to be used and to send responses back to clients. If not set, the global default gateway will be used. |
| ErrorCode | I | 0 | 200-505 | If no Real Servers are available, the LoadMaster can terminate the connection with a HTTP error code. Specify the error code number in this parameter. To unset the error code, set the parameter to an empty string.<br>In LoadMaster firmware version 7.2.52 it is possible to upload an error file using the API to add to the error response. To retrieve the Virtual Service ID, run the listvs command. For further details refer to the |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | **Upload Error File** section. |
| ErrorUrl | S | <unset> | | When no Real Servers are available and an error response is sent back to the client, a redirect URL can also be specified. |
| PortFollow | I | <unset> | 0 and 3-65530 | This parameter was depreciated as of 7.1-24. For LoadMasters with version 7.1-24 or higher, use the **FollowVSID** parameter to set port following.<br>Specify the ID of the Virtual Service to follow. Setting this value to 0 disables port following. 1 and 2 are not valid values so ensure that the Virtual Service that you want to follow has a value between 3 and 65530. |
| FollowVSID | I | <unset> | | Specify the ID of the Virtual Service to follow. |
| LocalBindAddrs | A | <unset> | A space separated list of IP addresses | This corresponds to the **Alternate Source Address** in the **Advanced Properties** section of the WUI. **Allow connections scaling over 64K Connections** needs to be enabled in **L7 Configuration** for this feature to work. |
| NRequestRules | I | <unset> | | This displays the number |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | (Read only) | | | of HTTP Header Modification request rules. |
| NResponseRules | I (Read only) | <unset> | | This displays the number of HTTP Header Modification response rules. |
| RequestRules | List (Read only) | | | The list of request rules that are assigned to the Virtual Service. |
| ResponseRules | List (Read only) | | | The list of response rules that are assigned to the Virtual Service. |
| StandbyAddr | A | <unset> | | Specify the IP address of the “Sorry” server that is to be used when no other Real Servers are available. This server will not be health checked and is assumed to be always available. |
| StandbyPort | I | <unset> | | Specify the port of the “Sorry” server. |
| NonLocalSorryServer | B | <unset> | 0 - Disabled<br>1 - Enabled | Set this parameter to 1 (enabled) if you are adding a non-local sorry server using the **StandByAddr** and **StandByPort** parameters. |
| Verify | I | 0 | 0-7 (bitmask) | Refer to the **Verify Parameter** section for further information on the **Verify** parameter. |
| AltAddress | A | <unset> | IP address | Specify the alternate address for this Virtual |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | Service. |
| AddVia | I | | 0-6 | Specify which headers to be added to HTTP requests. X-ClientSide and X-Forwarded-For are only added to non-transparent connections.<br>0 = Legacy Operation(X-Forwarded-For)<br>1 = X-Forwarded-For (+ Via)<br>2 = None<br>3 = X-ClientSide (+ Via)<br>4 = X-ClientSide (No Via)<br>5 = X-Forwarded-For (No Via)<br>6 = Via Only |
| PreProcPrecedence | S | <unset> | | This parameter should be used in conjunction with **PreProcPrecedencePos**. This parameter is used to specify the name of the existing rule whose position you wish to change.<br>This parameter relates to **Content Matching Rules** only. |
| PreProcPrecedencePos | Int16 | <unset> | | This parameter, in conjunction with the **PreProcPrecedence** parameter, is used to change the position of the |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | rule in a sequence of rules. For example a position of **2** means the rule will be checked second.<br><br>This parameter relates to the **Content Matching Rules** only. |
| RequestPrecedence | String | <unset> | This parameter should be used in conjunction with **RequestPrecedencePos.** This parameter is used to specify the name of the existing request rule whose position you wish to change.<br><br>This parameter relates to the following rule types:<br><br>**Content Matching**<br><br>**Add Header**<br><br>**Delete Header**<br><br>**Replace Header**<br><br>**Modify URL** |
| RequestPrecedencePos | Int16 | <unset> | This parameter, in conjunction with the **RequestPrecedence** parameter, is used to change the position of the rule in a sequence of rules. For example a position of **2** means the rule will be checked second. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| ResponsePrecedence | String | <unset> | This parameter should be used in conjunction with **ResponsePrecedencePos**. This parameter is used to specify the name of the existing response rule whose position you wish to change.<br>This parameter relates to the following rule types:<br>**Content Matching**<br>**Add Header**<br>**Delete Header**<br>**Replace Header** |
| ResponsePrecedencePos | Int16 | <unset> | This parameter, in conjunction with the **ResponsePrecedence** parameter, is used to change the position of the rule in a sequence of rules. For example, a position of **2** means the rule will be checked second. |
| MatchBodyPrecedence | String | <unset> | This parameter should be used in conjunction with **MatchBodyPrecedencePos**. Use this parameter to specify the name of the existing body modification rule that you want to change the position of.<br>This parameter relates to |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | **Body Modification** rules only. |
| MatchBodyPrecedencePos | Int16 | <unset> | Use this parameter, in conjunction with the **MatchBodyPrecedence** parameter, to change the position of the rule in a sequence of rules. For example, a position of **2** means the rule is checked second. |

3.6.1.5.1 Upload Error File

As of LoadMaster firmware version 7.2.52, it is also possible to upload the error file. To upload an error file using the RESTful API, run the following command:

```
curl -u "<Username>:<Password>" -k -X POST --data-binary "@<PathToFile>"
"https://<LoadMasterIPAddress>/access/uploadvserrfile?vs=<VirtualServiceID>"
```

3.6.1.5.2 Verify Parameter

**Verify** is a bitmask. The valid values of the **Verify** parameter are as follows:

- Bit 0: set this to **1** to enable detection intrusion

  > Bit 0 must be set to **1** to use the other two bits.

- Bit 1 determines whether to reject or drop a connection. Setting it to 1 will drop the connection.
- Bit 2 determines whether to give just warnings on bad requests or also on malicious (but not invalid) requests

  > Bits 3 to 7 cannot be set – an error message displays if you try to do this.

The following table lists the valid integers and the values they set the fields to when used:

| Integer | Detect Malicious Requests | Intrusion Handling | Warnings Checkbox |
|---|---|---|---|
| 0 | Disabled | N/A | N/A |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| 1 | Enabled | Drop Connection | Unchecked |
| 2 | Enabled | Send Reject | Unchecked |
| 3 | Enabled | Send Reject | Unchecked |
| 4 | Enabled | Drop Connection | Checked |
| 5 | Enabled | Drop Connection | Checked |
| 6 | Enabled | Send Reject | Checked |
| 7 | Enabled | Send Reject | Checked |

You cannot set the **Verify** parameter to a value above 7 – 7 is the maximum value.

#### 3.6.1.6 WAF Settings

| Name | Type | Default | Range | Description |
|---|---|---|---|---|
| Intercept | B | 0 | 0 – Disabled<br>1 – Enabled | Enable/disable the Web Application Firewall (WAF) for this Virtual Service. |
| InterceptOpts | S | <unset> | | Most of the fields in the **WAF Options** section of the Virtual Service modify screen in the LoadMaster WUI can be set using this parameter. For more information, refer to the **WAF InterceptOpts Parameter** section. |
| InterceptPOSTOtherContentTypes | S | <unset> | | When the **otherctypesenable** parameter is enabled, use the **InterceptPOSTOtherContentTypes** parameter to enter a comma-separated list of POST content types allowed for WAF analysis, for example **text/plain,text/css**. By |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | default, all types (other than XML/JSON) are enabled. To set this to any other content types, set the value to **any**.<br><br>Enabling the inspection of any other content types may increase system resource utilization (CPU and memory). A specific list of content types should be considered. |
| AlertThreshold | I | 0 - disabled | 0 - 100000 | This is the threshold of incidents per hour before sending an alert. Setting this to **0** disables alerting. |

3.6.1.6.1 WAF InterceptOpts Parameter

The WAF **InterceptOpts** parameter is a special parameter – it can be used to set the value for multiple fields, rather than just one field as with most other parameters. The **InterceptOpts** parameter allows the specification of most of the fields in the **WAF Options** section of the Virtual Service modify screen in the LoadMaster WUI.

To enable WAF, set the **Intercept** parameter to **1**.

The names of the specific WUI fields that the **InterceptOpts** parameter is related to, are listed in the table below.

One or more field values can be set in one command. Multiple values can be set in the one command by separating the values with a semi-colon, for example:

```
https://<LoadMasterIPAddress>/access/modvs?vs=<VirtualServiceIPAddress>&port=<Port>&prot=<tcp/udp>&InterceptOpts=opnormal;auditnone;reqdataenable;resdataenable;jsondisable;xmldisable
```

The table below outlines what each of the values mean.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

The values that are related to the same WUI option are mutually exclusive. For example, you cannot set **Basic Operation** to both **opnormal** and **opblock**.

| Value | Related WUI Option | Default | Meaning |
|---|---|---|---|
| opnormal | **Default Operation** | Audit Only | Set the **Basic Operation** to **Audit Only** |
| opblock | **Default Operation** | Audit Only | Set the **Basic Operation** to **Block Mode** |
| auditnone | **Audit mode** | No Audit | Set the **Audit mode** to **No Audit**. No data is logged. |
| auditrelevant | **Audit mode** | No Audit | Set the **Audit mode** to **Audit Relevant**. Logs data which is of a warning level and higher. |
| auditall | **Audit mode** | No Audit | Set the **Audit mode** to **Audit All**. Logs all data through the Virtual Service.<br>The **Audit All** option is not recommended for use in normal operation. **Audit All** should only be used when troubleshooting a specific problem. |
| reqdataenable | **Inspect HTML POST Request Content** | Disabled | Enable the **Inspect HTML POST Request Content** option |
| reqdatadisable | **Inspect HTML POST Request Content** | Disabled | Disable the **Inspect HTML POST Request Content** option |
| resdataenable | **Process Response Data** | Disabled | Enable the **Process Response Data** option |
| resdatadisable | **Process Response Data** | Disabled | Disable the **Process Response Data** option |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| jsondisable | **Enable JSON Parser** | Enabled | Disable the JSON parser.<br>This option is only relevant if the **Inspect HTML POST Request Content** option is enabled. |
| jsonenable | **Enable JSON Parser** | Enabled | Enable the JSON parser.<br>This option is only relevant if the **Inspect HTML POST Request Content** option is enabled. |
| xmldisable | **Enable XML Parser** | Enabled | Disable the XML parser.<br>This option is only relevant if the **Inspect HTML POST Request Content** option is enabled. |
| xmlenable | **Enable XML Parser** | Enabled | Enable the XML parser.<br>This option is only relevant if the **Inspect HTML POST Request Content** option is enabled. |
| otherctypesdisable | **Enable Other Content Types** | Disabled | Disable verification of POST content types (other than XML/JSON). |
| otherctypesenable | **Enable Other Content Types** | Disabled | Enable verification of POST content types (other than XML/JSON).<br>Enabling the inspection of any other content types may increase system resource utilization (CPU and memory). A specific list of content types should be considered.<br>When this option is enabled, the **InterceptPOSTOtherContentTypes** parameter can be used to enter a comma-separated list of POST content types allowed for WAF analysis. By default, all types (other than XML/JSON) are enabled. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.6.1.6.2 Assign a WAF Rule to a Virtual Service

All rules for a particular WAF ruleset can be assigned to a Virtual Service by running the following command.

**https://<LoadMasterIPAddress>/access/vsaddwafrule?vs=<VSIPAddress>&port=<Port>&prot=<tcp/udp>&rule=<Prefix>/<RuleName>**

For example:

**https://10.11.0.30/access/vsaddwafrule?vs=10.11.0.35&port=80&prot=tcp&rule=C/modsecurity_crs_13_xml_enabler**

The <RuleName> must be preceded with the relevant letter or word and a forward slash. The letter/word used depends on the type of rule being added:

> This is case sensitive. The letter/word needs to be in in the correct case (as per the case used in this document below) for the command to work.

- C or Custom
- Z or ApplicationGeneric
- A or ApplicationSpecific
- G or Generic

> All parameters listed in the example command above are required for the **vsaddwafrule** command. If any of the parameters is omitted, a **String value missing** error will be displayed.

Multiple rules can be assigned in the same command by separating them with a space (or **%20**). For example:

**https://10.11.0.30/access/vsaddwafrule?vs=10.11.0.35&port=80&prot=tcp&rule=C/modsecurity_crs_13_xml_enabler%20C/modsecurity_crs_10_ignore_static**

View a list of rules and rule IDs for an active ruleset by running the **vslistwafruleids** command, for example:

**https://10.11.0.30/access/vslistwafruleids?vs=10.11.0.35&port=80&prot=tcp&rule=G/ip_reputation**

A list of rules and their IDs will be displayed for the specified ruleset, for example:

```
<Response stat="200" code="ok">
<Success>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
<Data>
<ip_reputation>
<InactiveRule1>
2200000:REPUTATION/MALICIOUS:SLR: Client IP in Blocklist.
</InactiveRule1>
<InactiveRule2>
2200002:REPUTATION/ANONYMIZER:SLR: Client IP in TOR Exit Nodes Blocklist.
</InactiveRule2>
</ip_reputation>
</Data>
</Success>
</Response>
```

The ID is the number displayed before the rule name.

When adding a ruleset, you can specify the specific rules to not enable within the ruleset by specifying the rule IDs to not enable, for example:

**https://10.154.11.100/access/vsaddwafrule?vs=10.154.11.141&port=8443&prot=tcp&rule=G/ip_reputation&disablerules=2200000**

To disable a specific rule (or rules) (and not an entire ruleset), run the **vsaddwafrule** command with a blank **rule** parameter, for example:

**https://10.154.11.100/access/vsaddwafrule?vs=10.154.11.102&port=443&prot=tcp&rule=&disablerules=960020,958291**

**Related WUI item**

Virtual Services > View/Modify Services > Modify > WAF Options > Manage Rules

3.6.1.6.3 Unassign an WAF Rule from a Virtual Service

An WAF rule can be unassigned from a Virtual Service by running the following command. This command related to the **Available Rules** and **Assigned Rules** fields in the Modify Virtual Service screen in the WUI.

**https://<LoadMasterIPAddress>/access/vsremovewafrule?vs=<VSIPAddress>&port=<Port>&prot=<tcp/udp>&rule=C/<RuleName>**

For example:

**https://10.11.0.30/access/vsremovewafrule?vs=10.11.0.35&port=80&prot=tcp&rule=C/modsecurity_crs_13_xml_enabler**

The <RuleName> must be preceded with the relevant letter/word and a forward slash. The letter/word used depends on the type of rule being removed:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- C or Custom
- Z or ApplicationGeneric
- A or ApplicationSpecific
- G or Generic

> All of the parameters listed in the example command above are required for the **vsremovewafrule** command. If any of them are omitted, a **String value missing** error will be displayed.

**Related WUI item**

Virtual Services > View/Modify Services > Modify > WAF Options > Assign Rules

### 3.6.1.7 ESP Options

| Name | Type | Default | Range | Description |
|---|---|---|---|---|
| AllowedHosts | S | <unset> | | This parameter is only relevant when ESP is enabled. Specify all the virtual hosts that can be accessed using this Virtual Service. |
| AllowedDirectories | S | <unset> | You can specify up to 254 characters for this parameter. | This parameter is only relevant when ESP is enabled. Specify all the virtual directories that can be accessed using this Virtual Service. |
| Domain | S | <unset> | | The Single Sign On (SSO) domain in which this |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | Virtual Service will operate. |
| Logoff | S | <unset> | You can specify up to 255 characters for this parameter. | This parameter is only relevant when ESP is enabled and when the **Client Authentication Mode** is set to **Form Based**. Specify the string that the LoadMaster should use to detect a logout event. Multiple logoff strings can be specified by using a space-separated list.<br><br>If the URL to be matched contains sub-directories before the specified string, the **Logoff String** will not be matched. Therefore, the LoadMaster will not log the user off. |
| AddAuthHeader | S | <unset> | You can specify up to 255 characters for this parameter. | This option is only available if |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | **SAML** is selected as the **InputAuthMode**. Specify the name of the HTTP header. This header is added to the HTTP request from the LoadMaster to the Real Server and its value is set to the user ID for the authenticated session. You can unset the value of this parameter by running the **modvs** command with the **addauthheader** parameter set to an empty string, for example: **addauthheader =** |
| DisplayPubPriv | B | 1 – Enabled | 0 – Disabled<br>1 – Enabled | Display the public/private option on the login page. Based on the option the user selects on the login form, the |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | session timeout value will be set to the value specified for either the public or private timeout. |
| DisablePasswordForm | B | 0 – Disabled | 0 – Disabled<br>1 – Enabled | Enabling this option removes the password field from the login page. This may be needed when password validation is not required, for example if using RSA SecurID authentication in a singular fashion. |
| Captcha | B | 0 – Disabled | 0 – Disabled<br>1 – Enabled | Enable this parameter to allow CAPTCHA verification on the login page.<br>The LoadMaster only supports CAPTCHA v2. The InputAuthMode must be set to 2 |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | |
|---|---|
| | (Form Based) for the CAPTCHA parameters to be relevant |
| | All CAPTCHA parameters must be set before it can be used. |
| | Both the LoadMaster and the client machine must be able to access Google for this to work. |
| | Before the CAPTCHA has been correctly answered, the submit button |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | on the login form is disabled. If the user does not submit the form within two minutes of answering the CAPTCHA, the CAPTCHA times out (Google-specified timeout), and the user must verify a new CAPTCHA (the submit button is disabled until the new CAPTCHA has been verified). |
| CaptchaPublicKey | S | <unset> | The key that was provided as the public key when you signed up for the CAPTCHA service. |
| CaptchaPrivateKey | S | <unset> | The key that was provided as the private key when you signed up for the CAPTCHA service. |
| CaptchaAccessUrl | S | www.google.com/recaptcha/api.js | The URL of the service that provides the |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | CAPTCHA challenge.<br>Do not start this URL with https.<br>Only CAPTCHA V2 is currently supported. |
| CaptchaVerifyUrl | S | www.google.com/recaptcha/api/siteverify | The URL of the service that verifies the response to the CAPTCHA challenge.<br>Do not start this URL with https.<br>Only CAPTCHA V2 is currently supported. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| ESPLogs | I | 7 | Integer 0-7 | Enable ESP logging. Valid values are below:<br>0 = Logging off<br>1 = User Access<br>2 = Security<br>3 = User Access and Security<br>4 = Connection<br>5 = User Access and Connection<br>6 = Security and connection<br>7 = User Access, Security and Connection<br>**Note:** The only valid values for SMTP services are 0 and 4. For SMTP services, security issues are always logged. Nothing is logged for user access because there are no logins. |
| SMTPAllowedDomains | S | <unset> | | Specify all the permitted domains that are allowed to |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | be received by this Virtual Service. |
| ExcludedDirectories | S | <unset> | | This parameter is only relevant when ESP is enabled. Any virtual directories specified within this field will not be pre-authorized on this Virtual Service and are passed directly to the relevant Real Servers. |
| EspEnabled | B | N | 0 – Disabled<br>1 - Enabled | Enable or disable the Edge Security Pack (ESP) features. |
| InputAuthMode | I | 0 | 0-8 | Specify the client authentication method to be used:<br>0 = Delegate to Server<br>1 = Basic Authentication<br>2 = Form Based<br>4 = Client Certificate<br>5 = NTLM |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | 6 = SAML<br>7 = Pass Post<br>8 = OIDC / OAUTH |
| OutputAuthMode | I | Dependent on InputAuthMode value | 0-4 | Specify the server authentication mode to be used:<br>0 = None<br>1 = Basic Authentication<br>2 = Form Based<br>3 = KCD<br>4 = Server Token |
| TokenServerFQDN | S | <unset> | You can specify up to 127 characters for this parameter. | This parameter is only relevant when using **SAML** as the **Client Authentication Mode** (InputAuthMode) and **Server Token** as the **Server Authentication Mode** (OutputAuthMode). When set, the LoadMaster contacts the token server at |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | the given FQDN during sign-on and obtains a permanent access token from that token server. If this parameter is unset, then the LoadMaster obtains the token from the Real Server. |
| ServerFbaPath | S | <unset> | Only relevant when using form-based authentication as the **Server Authentication Mode** ( **OutputAuthMode**). Set the authentication path for server-side Form Based Authentication (FBA). When used in Exchange environments, this does not need to be set. |
| ServerFBAPost | S | <unset> | Only relevant when using form-based authentication as the **Server** |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | **Authentication Mode** ( **OutputAuthMode**). Set the format string used to generate POST body for server side FBA. The value must be base64-encoded.<br><br>When used in Exchange environments, this does not need to be set. |
| ServerFbaUsernameOnly | B | 0 – Disabled | 0 – Disabled<br><br>1 - Enabled | This option is only relevant if the **InputAuthMode** is set to **2** (Form Based), the **OutputAuthMode** is set to **2** (Form Based), and the **ServerFbaPath** has been entered. Enable this option to send the username only (without the domain part) in the server-side form based authentication POST request. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| OutConf | S | <unset> | | Enter the name of the outbound SSO domain. |
| SingleSignOnDir | S | <unset> | - Blank<br>- Dual Factor Authentication<br>- Exchange<br>- Français%20Canadien%20-%20Blank<br>- Français%20Canadien%20-%20Exchange<br>- Português%20do%20Brasil%20-%20Blank<br>- Português%20do%20Brasil%20-%20Exchange | This parameter relates to the **SSO Image Set** drop-down in the **ESP Options** section of the modify Virtual Service screen. Specify the name of the image set to be used for the login screen. If no image set is specified, the default **Exchange** image set will be used. |
| SingleSignOnMessage | S | <unset> | You can specify up to 255 characters for this parameter. | Specifies the SSO message that is displayed. The **SingleSignOnMessage** parameter accepts HTML code, so you can insert an image if required. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | |
|---|---|
| | There are several characters that are not supported. These are the grave accent character ( ` ) and the single quote ('). If a grave accent character is used in the **SingleSignOnMessage**, the character will not display in the output, for example a`b`c becomes abc. If a single quote is used, |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | users will not be able to log in. |
| AllowedGroups | S | <unset> | You can specify up to 2048 characters for this parameter. | Specify the groups that are allowed to access this Virtual Service.<br>If the parameter value is longer than the maximum length of a HTTP GET query (1024 characters), you must set the **HTTP Method** to **POST**. |
| GroupSIDs | S | <unset> | This parameter allows a list of group SIDs of up to 64 bytes and 2048 characters in length. | Specify the group security identifiers (SIDs) that are allowed to access this Virtual Service.<br>Each group is |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | |
|---|---|
| | separated by a semi-colon. Spaces are used to separate bytes in certain group SIDs. Here is an example:<br>**S-1-5-21-703902271-2531649136-2593404273-1606**<br>SIDs can be found by using the **get-adgroup-Identity GroupName** command.<br>If the parameter value is longer than the maximum length of HTTP GET query (1024 characters), you must set the **HTTP Method** |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | to **POST**. |
| IncludeNestedGroups | B | 0 - Disabled | 0 – Disabled<br>1 - Enabled | This parameter relates to the **AllowedGroups** parameter. Enable this option to include nested groups in the authentication attempt. If this option is disabled, only users in the top-level group will be granted access. If this option is enabled, users in both the top-level and first sub-level group will be granted access. |
| SteeringGroups | String | <unset> | You can specify up to 2048 characters for this parameter. | Enter the Active Directory group names that will be used for steering traffic. Use a semi-colon to separate multiple group names. The steering group index number corresponds to |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | the location of the group in this list.<br><br>If the parameter value is longer than the maximum length of a HTTP GET query (1024 characters), you must set the **HTTP Method** to **POST**. |
| VerifyBearer | Boolean | 0 - Disabled | 0 - Disabled<br>1 - Enabled | Enable this option to verify if the authentication header contains a bearer record. This is used when doing JSON web token validation. |
| BearerCertificateName | String | <unset> | A valid name of an uploaded certificate. | This option is only visible if the **VerifyBearer** parameter is |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | enabled.<br><br>Specify the name of the relevant certificate (this must be first uploaded to the LoadMaster using the **addcert** command) containing a Public Key used to validate the authenticity of the JSON Web Token Signature. This is used when doing JSON web token validation. |
| BearerText | String | <unset> | This option is only visible if the **VerifyBearer** parameter is enabled.<br><br>You can enter up to five bearer header validation strings (comma-separated list). This is used when doing JSON web token |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | validation. |
| ExcludedDomains | String | <unset> | | Any virtual directories specified within this field will not be pre-authorized on this Virtual Service and will be passed directly to the relevant Real Servers. Multiple excluded domains can be specified by using a space-separated list. |
| AltDomains | String | <unset> | | Specify alternative domains to be assigned to a Virtual Service when configuring multi-domain authentication. To specify multiple alternative domains, use a space separated list. |
| SameSite | I | | 0 – System Default<br>1 – SameSite=None<br>2 - SameSite=LAX<br>3 - SameSite=Strict | Allows the SameSite attribute to be explicitly |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | 4 - SameSite Option Not Added | specified for cookies used by LoadMaster Edge Security Pack. This influences the way browsers will use cookies across sites. |
| UserPwdChangeURL | String | <unset> | | This is relevant when using form-based LDAP authentication. Specify the URL that users can use to change their password. If a user's password has expired, or if they must reset their password, this URL and the **UserPwdChangeMsg** is displayed on the login form.<br><br>This URL must be put into the exception list for authentication, if required. |
| UserPwdChangeMsg | String | <unset> | | This parameter is only relevant if the |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | **UserPwdChangeURL** parameter is set. Specify the text to be displayed on the login form when the user must reset their password. |
| UserPwdExpiryWarn | Boolean | 0 - Disabled | 0 - Disabled<br>1 - Enabled | By default, SSO users are notified about the number of days before they must change their password. If you disable this option, the password expiry notification will not appear on the login forms. This parameter is only relevant if the **InputAuthMode** is set to **Form Based** (**2**) and the **UserPwdChangeURL** is set.<br>The language of the warning text is based on the **SSO Image Set** that is selected (English, French, or Portuguese). |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| UserPwdExpiryWarnDays | Integer | 15 | 1 - 30 | Specify the number of days to show the warning before the password is expired. This parameter is only relevant if the **InputAuthMode** is set to **Form Based** (**2**) and the **UserPwdChangeURL** is set. |

#### 3.6.1.8 Real Servers

| Name | Type | Default | Range | Description |
|---|---|---|---|---|
| CheckType | S | <tcp> | The default value is dependent on the Virtual Service port. The list of values is:<br>icmp<br>https<br>http<br>tcp<br>smtp<br>nntp<br>ftp | Specify which protocol is to be used to check the health of the Real Server. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | telnet<br>pop3<br>imap<br>rdp<br>bdata<br>ldap<br>none | |
| LdapEndpoint | S | <unset> | An existing endpoint name | Specify the name of an LDAP endpoint to use for the health checks. If **LDAP** is selected as the **CheckType**, the server IP address (or addresses) and ports from the LDAP endpoint configuration are used instead of the Real Server IP address and port. For further information on LDAP endpoints, refer to the **LDAP Configuration** section. |
| CheckHost | A | <unset> | | The **CheckUse1.1** parameter must be enabled to set the **CheckHost** value. When using HTTP/1.1 checking, the Real Servers require a Hostname be supplied in each request. If no value is set then this value is the IP address of the Virtual Service. |
| CheckPattern | S | <unset> | | When the **CheckType** is set to **http** or **https** - this corresponds to the **Reply 200 Pattern** in the WUI. This parameter only applies when the **HTTP Method** is set to **GET** or **POST**. When the **CheckType** is set to **bdata**: Specify the hexadecimal string which will be searched for in |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | the response. Specify an empty value to unset CheckPattern. |
| CheckUrl | S | <unset> | | When the **CheckType** is set to **http** or **https** - by default, the health checker tries to access the URL / to determine if the machine is available. A different URL can be set in the **CheckUrl** parameter.<br><br>When the **CheckType** is set to **bdata**: Specify a hexadecimal string to send to the Real Server.<br><br>The maximum character length for the **CheckUrl** parameter value is 126 characters. |
| CheckCodes | S | <unset> | 300-599 | A space-separated list of HTTP status codes that should be treated as successful when received from the Real Server. |
| CheckHeaders | S | <unset> | | Specify up to four additional headers/fields which will be sent with each health check request. Separate the pairs with a pipe, for example; **Host:xyc\|UserAgent:prq**. |
| MatchLen | S | 0 | 0-8000 | This parameter is only relevant when the **CheckType** is set to **bdata**. Specify the number of bytes to find the **CheckPattern** within. |
| CheckUse1.1 | B | N | 0 – Disabled<br><br>1 - Enabled | By default, the health checker uses HTTP/1.0 when checking the Real Server status. Enabling CheckUse1.1 means HTTP/1.1 is used (which is more efficient).<br><br>Optimization only works on HTTP (not |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | HTTPS) connections. |
| CheckPort | I | <unset> | 3-65530 | The port to be checked. If a port is not specified, the Real Server port is used. Specify 0 to unset CheckPort. |
| NumberOfRSs | I (Read only) | <unset> | | This displays the number of Real Servers that are assigned to the Virtual Service. |
| NRules | I (Read only) | <unset> | | This displays the number of rules assigned to a Real Server when content switching is enabled. |
| RuleList | List(Read only) | | | A list of content rules assigned to the Real Servers. |
| CheckUseGet | I | N | 0 - HEAD<br>1 - GET<br>2 - POST<br>3 - OPTIONS | When accessing the health check URL - the system can use the HEAD, the GET, the POST or the OPTIONS method. |
| ExtraHdrKey | S | <unset> | | Specify the key for the extra header to be inserted into every request sent to the Real Servers. |
| ExtraHdrValue | S | <unset> | | Specify the value for the extra header to be inserted into every request sent to the Real Servers. |
| CreateSubVS | | <unset> | | This parameter can be used to create a SubVS within a Virtual Service. This parameter has no value (entering **createsubvs=** will create a SubVS). |
| SubVS | I (Read Only) | | 0 – Disabled<br>1 – Enabled | This parameter displays details of any SubVSes which exist in the Virtual Service. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| CheckPostData | S | <unset> | Supports up to 2047 characters | This parameter is only relevant if the **HTTP Method** is set to **POST**. When using the **POST** method, up to 2047 characters of POST data can be sent to the server. |
| RSRulePrecedence | String | <unset> | | This parameter should be used in conjunction with **RSRulePrecedencePos**. This parameter is used to specify the name of the existing rule whose position you wish to change. |
| RSRulePrecedencePos | Int16 | <unset> | | This parameter, in conjunction with the **RSRulePrecedence** parameter, is used to change the position of the rule in a sequence of rules. For example, a position of **2** means the rule will be checked second. |
| EnhancedHealthchecks | Boolean | 0 – Disabled | 0 – Disabled<br>1 – Enabled | Enabling the **EnhancedHealthchecks** parameter provides an additional health check parameter – **RsMinimum**. If the **EnhancedHealthchecks** parameter is disabled, the Virtual Service will be considered available if at least one Real Server is available. If the **EnhancedHealthchecks** parameter is enabled, you can specify the minimum number of Real Servers which should be available to consider the Virtual Service to be available. |
| RsMinimum | Integer | 1 | 1 to the number of Real Servers | This parameter can only be set using the **modvs** command if the **EnhancedHealthchecks** parameter |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | configured | is enabled. Specify the minimum number of Real Servers required to be available for the Virtual Service to be considered up. If less than the minimum amount of Real Servers are available, a critical log is generated. If some Real Servers are down but it has not reached the minimum amount specified, a warning is logged. If the email options are configured, an email will be sent to the relevant recipients.<br><br>When retrieving the value of this parameter – 0 is the default value if there are no Real Servers or 1 Real Server in the Virtual Service. However, 1 is always the minimum in reality. |

#### 3.6.1.9 Miscellaneous

| Name | Type | Default | Range | Description |
|---|---|---|---|---|
| Adaptive | S (Read only) | <unset> | | This parameter is read only and will only be displayed when the **Scheduling Method** is set to **resource based (adaptive)**. |
| MultiConnect | B | 0 | 0 - Disabled<br>1 - Enabled | Enabling this option permits the LoadMaster to manage connection handling between the LoadMaster and the Real Servers. Requests from multiple clients will be sent over the same TCP connection.<br><br>Multiplexing only works for simple HTTP GET operations. This parameter cannot be enabled in certain situations, for example if WAF, ESP or SSL Acceleration is enabled. |
| non_local | B | 0 - | 0 – | By default, only Real Servers on local networks |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | Disabled | Disabled<br>1 – Enabled | can be assigned to a Virtual Service. Enabling this option will allow a non-local Real Server to be assigned to the Virtual Service.<br>This option will only be available if **NonLocalRS** has been enabled and the **Transparent** option has been disabled on the relevant Virtual Service. |

### 3.6.2 Adding a Virtual Service Using a Template

To add a Virtual Service and automatically configure it with a template, run the following command:

```
https://<LoadMasterIPAddress>/access/addvs?vs=<VSIPAddress>&port=<port>&prot=<tcp/udp>&template=<TemplateName>
```

The port and protocol parameters are required, but if the template sets the ports then the values entered in the command will be ignored.

For commands on adding, removing and listing templates, refer to the **Manage Templates** section.

### 3.6.3 Manage Templates

#### 3.6.3.1 Export a Virtual Service as a Template

An existing Virtual Service can be exported as a template by running the following command:

```
https://<LoadMasterIPAddress>/access/exportvstmplt?vs=<VirtualServiceIPAddress>&port=<VirtualServicePort>&prot=<tcp/udp>
```

The Virtual Service index can also be entered for the **vs** parameter (and the other parameters are then not needed). To retrieve the Virtual Service ID, run the **listvs** command. For further information, refer to the **Virtual Service Control** section.

#### 3.6.3.2 Upload a Template

Templates can be uploaded by running the following cURL command:

```
curl -X POST --data-binary "@<TemplateFileName.tmpl>" -k https://bal:<password>@<LoadMasterIPAddress>/access/uploadtemplate
```

#### 3.6.3.3 Display a List of Installed Templates

To display a list of the templates that exist on the LoadMaster, run the following command:

```
https://<LoadMasterIPAddress>/access/listtemplates
```

#### 3.6.3.4 Delete a Template

To delete a template from the LoadMaster, run the following command:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

**https://<LoadMasterIPAddress>/access/deltemplate?name=<TemplateName>**

### 3.6.4 Manage SSO

#### 3.6.4.1 SSO Domains

Single-Sign On Domains can be managed by the following commands.

When the **kcdciphersha1** parameter is enabled, the AES256 SHA1 KCD cipher is used (by default the RC4 cipher is used).

To retrieve the value of the **kcdciphersha1** parameter, run the following command:

**https://<LoadMasterIPAddress>/access/get?param=kcdciphersha1**

To enable or disable the **kcdciphersha1** parameter, run the following command:

**https://<LoadMasterIPAddress>/access/set?param=kcdciphersha1&value=1**

0 - Disabled

1 - Enabled

After changing the value of the **kcdciphersha1** parameter, you can run the **logging/ssoflush** command to flush the SSO authentication cache.

To add a domain:

**https://<LoadMasterIPAddress>/access/adddomain?domain=<DomainName>**

> You can specify up to 64 characters in the **domain** parameter.
> The maximum number of SSO domains that are allowed is 128.

To delete a domain:

**https://<LoadMasterIPAddress>/access/deldomain?domain=<DomainName>**

To show details of all domains:

**https://<LoadMasterIPAddress>/access/showdomain**

To show details of a specific domain:

**https://<LoadMasterIPAddress>/access/showdomain?domain=<DomainName>**

To modify a specific domain:

**https://<LoadMasterIPAddress>/access/moddomain?domain=<DomainName>**
**[&paramname=value...]**

**moddomain** accepts the following additional (optional) parameters:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| Name | Type | Default | Range | Additional Information |
|---|---|---|---|---|
| auth_type | S | LDAP-StartTLS | LDAP-Unencrypted<br>LDAP-StartTLS<br>LDAP-LDAPS<br>RADIUS<br>RSA-SECURID<br>KCD<br>Certificates<br>RADIUS and LDAP-Unencrypted<br>RADIUS%20and%20LDAP-StartTLS<br>RADIUS%20and%20LDAP-LDAPS<br>RSA-SECURID%20and%20LDAP-Unencrypted<br>RSA-SECURID%20and%20LDAP-StartTLS<br>RSA-SECURID%20and%20LDAP-LDAPS<br>OIDC-OAUTH | Specify the transport protocol used to communicate with the authentication server. |
| ldap_endpoint | S | None | The name of an existing LDAP endpoint | Specify the LDAP endpoint to use. For further information on LDAP endpoints, refer to the **LDAP Configuration** section. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| radius_shared_secret | S (masked) | <unset> | | The shared secret to be used between the RADIUS server and the LoadMaster. |
| radius_send_nas_id | B | 0 - Disabled | 0 - Disabled<br>1 - Enabled | If this parameter is disabled (default), a NAS identifier is not sent to the RADIUS server. If it is enabled, a Network Access Server (NAS) identifier string is sent to the RADIUS server. By default, this is the hostname. Alternatively, if a value is specified in the **radius_nas_id** parameter, this value is used as the NAS identifier. If the NAS identifier cannot be added, the RADIUS access request is still processed. This field is only available if the **auth_type** is set to a RADIUS option. |
| radius_nas_id | S | The hostname | | If the **radius_send_nas_id** parameter is enabled, the **radius_nas_id** parameter is relevant. When specified, this value is used as the NAS identifier. Otherwise, the hostname is used as the NAS identifier. If the NAS identifier cannot be |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | added, the RADIUS access request is still processed.<br><br>This parameter is only relevant if the **auth_type** is set to a RADIUS option and the **radius_send_nas_id** parameter is enabled. |
| logon_fmt | S | Principalname | not%20specified<br><br>Principalname<br><br>Username<br><br>Username%20only | Specify the logon string format used to authenticate to the LDAP/RADIUS server.<br><br>The **Username%20only** value is only available if the **auth_type** is set to a **RADIUS** or **RSA-SecurID** protocol. The **Username** value is not available if the **auth_type** is set to **RADIUS** or a **RADIUS and LDAP** protocol. |
| logon_fmt2 | S | Principalname | Not%20specified<br><br>Principalname<br><br>Username | Specify the logon string format used to authenticate to the server. |
| logon_domain | S | <unset> | | This parameter corresponds with the **Domain/Realm** field in the WUI. The login domain to be used. This is also used with logon format to construct the normalized user name, for example:<br><br>Principalname: |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | <username>@<domain><br>Username:<br><domain>\<username> |
| logon_ transcode | B | 0 | 0 - Disabled<br>1 - Enabled | Enable or disable the transcode of logon credentials from ISO-8859-1 to UTF-8, when required. |
| user_acc_ control | I | 0 | 0-300 | Specify the range in which periodic User Access Control (UAC) checks are performed. When an interval value is specified in the range of 1 to 300 minutes, the periodic UAC check is performed per user for the requests received after the interval expiry.<br>If the interval value is set to 0 minutes, then the UAC check is not performed. |
| max_ failed_ auths | I | 0 | 0-999 | The maximum number of failed login attempts before the user is locked out.<br>0 – Never lock out. |
| sess_tout_ idle_pub | I | 900 | 60-604800 | The session idle timeout value in seconds. This value is used in a public environment. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| sess_tout_duration_pub | I | 1800 | 60-604800 | The maximum duration timeout value for the session in seconds. This value is used in a public environment. |
| sess_tout_idle_priv | I | 900 | 60-604800 | The session idle timeout value in seconds. This value is used in a private environment. |
| sess_tout_duration_priv | I | 2800 | 60-604800 | The maximum duration timeout value for the session in seconds. This value is used in a private environment. |
| sess_tout_type | S | idle time | idle time<br>max duration | Specify the type of session timeout to be used. |
| testuser | S | <unset> | | The username that will be used to check the authentication server(s), if you are not using an LDAP endpoint. |
| testpass | S (masked) | <unset> | | The password of the user that is used to check the authentication server(s), if you are not using an LDAP endpoint. |
| reset_fail_tout | I | 60 | 60-86400 | The number of seconds that must elapse before the **Failed Login Attempts** counter is reset to 0. This value must be less than the **unblock_tout**. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| unblock_ tout | I | 1800 | 60-86400 | The timeout value (in seconds) before a blocked account is automatically unblocked. This must be greater than the **reset_ fail_tout** value. |
| server | S | <unset> | | The address(s) of the server(s) that are to be used to validate this domain.<br>IPv6 is not supported for RADIUS authentication. |
| server2 | A | <unset> | Valid IP address | When using dual factor authentication, use the **server** parameter to set the address of the RADIUS server(s) and use the **server2** parameter to set the address of the LDAP server(s). |
| kerberos_ domain | S | <unset> | | The Kerberos Realm |
| kerberos_ kdc | S | <unset> | | The Kerberos Key Distribution Center |
| kcd_ username | S | <unset> | | The **kcd_username** should not contain double or single quotes. |
| kcd_ password | S | <unset> | | The **kcd_password** should not contain double or single quotes. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| ldap_admin | S | <unset> | | This, along with the **ldap_password**, is used to log in to the database to check if the user from the certificate exists. |
| ldap_password | S | <unset> | | This, along with the **ldap_admin**, is used to log in to the database to check if the user from the certificate exists. |
| cert_check_asi | B | 0 - Disabled | 0 - Disabled<br>1 - Enabled | This option is only available when the **Authentication Protocol** is set to **Certificates**. When this option is enabled - in addition to checking the validity of the client certificate, the client certificate will also be checked against the altSecurityIdentities (ASI) attribute of the user on the Active Directory. |
| cert_check_cn | B | 0 - Disabled | 0 - Disabled<br>1 - Disabled | Enabling this parameter allows a fallback to check the Common Name (CN) in the certificate when the SAN is not available. |
| server_side | B | Y – Outbound KCD SSO domain | Y = Outbound KCD SSO domain<br>N = Inbound configuration | Specify whether the configuration is inbound or outbound. |
| idp_entity_id | S | <unset> | | Specify the Identity Service Provider (IdP) Entity ID. This is relevant |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | when using SAML. The maximum number of characters permitted in this field is 255. |
| idp_sso_url | S | <unset> | | Specify the IdP Single Sign On (SSO) URL. This is relevant when using SAML. The maximum number of characters permitted in this field is 255. |
| Idp_logoff_url | S | <unset> | | Specify the IdP Logoff URL. This is relevant when using SAML. The maximum number of characters permitted in this field is 255. |
| idp_cert | S | <unset> | | Specify the IdP certificate to use for verification processing. |
| idp_match_cert | B | 0 - Disabled | 0 - Disabled<br>1 - Enabled | If this option is enabled, the IdP certificate assigned must match the certificate in the IdP SAML response. |
| sp_entity_id | S | <unset> | | Relevant when using SAML - the Service Provider (SP) entity ID is an identifier that is shared to enable the IdP to understand, accept and have knowledge of the entity when request messages are sent from the LoadMaster. This must correlate to the |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | identifier of the relying party on the AD FS server. The maximum number of characters permitted in this field is 255. |
| sp_cert | S | <unset> | It is optional to sign requests that are sent in the context of logon. Currently, the LoadMaster does not sign those requests.<br><br>In the context of log off requests – it is mandatory and these requests must be signed. This is to avoid any spoofing and to provide extra security in relation to log off functionality. This ensures that users are not being hacked and not being logged off unnecessarily.<br><br>In the **sp_cert** parameter, you can choose to use a self-signed certificate or third party certificate to perform the signing.<br><br>To specify a self-signed certificate, set **sp_cert** to **useselfsigned**. To use a third party certificate, specify the name of the certificate to use (this |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | certificate must be uploaded to the intermediate certificate section of the LoadMaster before it can be selected). |
| ldapephc | B | 1 - Enabled | 0 - Disabled<br>1 - Enabled | Enable this parameter to use the LDAP endpoint admin username and password for the health check. |
| oidc_app_id | S | <unset> | | Add the Application (client) ID of the application. The maximum number of characters permitted in this field is 255. |
| oidc_redirect_uri | S | <unset> | | Specify the redirect Uniform Resource Identifier (URI) or URIs (reply URLs). You can enter multiple URIs separated by a space. A maximum of 255 characters can be specified for the oidc_**redirect_uri** parameter. Once a value is set for this parameter, you cannot unset it. |
| oidc_auth_ep_url | S | <unset> | | Specify the authorization end point URL of the application. Ensure to use the correct URL format. The maximum number of characters permitted in this field is |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | 255. |
| oidc_ token_ep_ url | S | <unset> | Specify the token end point URL of the application. Ensure to use the correct URL format. The maximum number of characters permitted in this field is 255. |
| oidc_ logoff_url | S | <unset> | Specify the logoff URL of the application. Ensure to use the correct URL format. The maximum number of characters permitted in this field is 255. |
| oidc_secret | S | <unset> | Specify the OIDC application secret of the application. |

To show the locked users, run the following command:

**https://<LoadMasterIPAddress>/access/showdomainlockedusers?**

To unlock specified users, run the following command:

**https://<LoadMasterIPAddress>/access/unlockdomainusers?domain=<DomainName>&users=<exampleuser>**

3.6.4.1.1 Upload RSA Files

If using **RSA-SecurID** as the **Authentication Protocol**, files need to be uploaded to the LoadMaster for the authentication to work.

To upload the **RSA Authentication Manager Config File**, run the following command:

**curl -X POST --data-binary "@<RSAConfigFileName.zip>" -k https://<username>:<password>@<LoadMasterIPAddress>/access/setrsaconfig**

To upload the **RSA Node Secret File**, run the following command:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
curl -X POST --data-binary "@<NodeSecretFileName.zip>" -k
https://<username>:<password>@<LoadMasterIPAddress>/access/setrsanodesecret?r
sanspwd=<RSANodeSecretPassword>
```

3.6.4.1.2 Upload an Identity Provider (IdP) Metadata File (if using SAML)

The **uploadsamlidpmd** command is used to upload an IdP metadata file. This simplifies the configuration of the IdP attributes, including the **IdP Entity ID**, **IdP SSO URL** and **IdP Logoff URL**. The metadata file can be downloaded from the IdP. To upload an IdP metadata file, run the following command:

```
https://<LoadMasterIPAddress>/access/uploadsamlidpmd?domain=<DomainName>
```

3.6.4.1.3 Download the Service Provider Certificate (if using SAML)

If using a self-signed certificate, the **downloadsamlspcert** command is used to download the certificate from the LoadMaster. This certificate must be installed on the IdP server (for example AD FS) to be added to the relying party signature.

The AD FS server will require this certificate for use of the public key to verify the signatures that the LoadMaster generates.

To download the certificate, run the following command:

```
https://<LoadMasterIPAddress>/access/downloadsamlspcert?domain=<DomainName>
```

3.6.4.1.4 Sessions

The commands in this section relate to the open SSO sessions.

To filter the list of open sessions by user, run the **search** command and specify the user, for example:

```
https://<LoadMasterIPAddress>/access/ssodomain/search?domain=<DomainName>&use
r=<Username>
```

> The match is based on a substring of the username and is not exact.

> The **user** parameter is not case sensitive.

To retrieve a list of all open sessions for a specific SSO domain, run the following command:

```
https://<LoadMasterIPAddress>/access/ssodomain/queryall?domain=<DomainName>
```

This returns the number of active user and cookie sessions.

To return sessions within a particular range, run the **querysessions** command, for example:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
https://<LoadMasterIPAddress>/access/ssodomain/querysessions?domain=<DomainName>&startsession=1&endsession=1000
```

This returns sessions in sequence, as they appear in the cache.

If you do not specify the **startsession** and **endsession** parameters, the first 1000 sessions display.

> The maximum number of SSO sessions that can be returned in a single **querysessions** API call is limited to 1000. If the maximum number of SSO sessions exceeds 1000, you must use multiple **querysessions** API calls.

To kill a particular session, run the following command:

```
https://<LoadMasterIPAddress>/access/ssodomain/killsession?domain=<DomainName>&key=<<Cookie>/<Username>,<SourceIPAddress>>
```

For the **key** parameter, you can either specify the **Cookie** or **<Username>,<SourceIPAddress>**.

For example, if using a cookie:

```
https://10.154.11.180/access/ssodomain/killsession?domain=qasp.com&key=b6bfa66e23ee2d9c3267704bfd20f053
```

Or if using **<Username>,<SourceIPAddress>**:

```
https://10.154.11.180/access/ssodomain/killsession?domain=kempqaesp.net&key="esptest1@kempqaesp.net,172.21.135.241"
```

To kill all open sessions for a particular domain, run the following command:

```
https://<LoadMasterIPAddress>/access/ssodomain/killallsessions?domain=<DomainName>
```

#### 3.6.4.2 SSO Image Sets

Custom SSO image sets can be managed by using the following commands:

```
https://<LoadMasterIPAddress>/access/listssoimages
https://<LoadMasterIPAddress>/access/delssoimage?name=<Imagesetname>
```

To upload an SSO image set, use the below command:

```
curl -X POST --data-binary "@<pathToImageSet>" -k
https://<LoadMasterIPAddress>/access/ssoimages?
```

The custom SSO image set must be in the format of a .tar file. A template tar file is available from the Kemp Support site: Single Sign-On Custom Images. This can then be modified to gain the desired look and feel. For further information, please refer to the Custom Authentication Form, Technical Note.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

### 3.6.5 Cache Configuration

File extensions can be added or deleted from the list of file extensions that should not be cached by using the following commands:

```
https://<LoadMasterIPAddress>/access/addnocache?param=<FileExtension>
https://<LoadMasterIPAddress>/access/delnocache?param=<FileExtension>
```

The <FileExtension> string must begin with a ".", for example:

```
https://<LoadMasterIPAddress>/access/addnocache?param=.jpg
```

Related parameters that can be managed using **get** and **set** commands are detailed in the following table. Refer to the **Using get and set commands** section for the **get** and **set** commands.

| Name | Type | Range | Description |
|---|---|---|---|
| cachesize | I | 1-409 | Specifies the cache size. |
| hostcache | B | 0 - Disabled<br>1 – Enabled | Enable or disable using the host cache. |

Items are held in the cache for 15 minutes (or until the cache is flushed by refreshing the page (for example, by pressing **Ctrl + F5** on your keyboard).

### 3.6.6 Compression Options

File extensions can be added or deleted from the list of file extensions that should not be compressed by using the following commands:

```
https://<LoadMasterIPAddress>/access/addnocompress?param=<.FileExtension>
https://<LoadMasterIPAddress>/access/delnocompress?param=<.FileExtension>
```

The <FileExtension> string must begin with a "."

### 3.6.7 Kubernetes Settings

This section provides details about the LoadMaster RESTful API commands you can use to configure the Kubernetes Ingress Controller functionality.

#### 3.6.7.1 Upload a Kube Config File

To upload a Kube config file to the LoadMaster, run the **addlmingressk8sconf** as a cURL command. For example:

```
curl -X POST --data-binary "@<KubeConfigFilename>" -k
https://<Username>:<Password>@<LoadMasterIPAddress>/access/addlmingressk8sconf
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.6.7.2 Delete the Kube Config File

To delete the existing Kube config file from the LoadMaster, run the **dellmingressk8sconf** command. For example:

```
/access/dellmingressk8sconf
```

#### 3.6.7.3 List the Contexts in the Kube Config File

To list the contexts in the Kube config file that is installed on the LoadMaster, run the **showlmingressk8sconf** command. For example:

```
/access/showlmingressk8sconf
```

#### 3.6.7.4 Check the Operations Mode

To check what **Operations Mode** is currently selected, run the **getlmingressmode** command. For example:

```
/access/getlmingressmode
```

#### 3.6.7.5 Set the Operations Mode

To set the **Operations Mode**, run the **setlmingressmode** command. For example:

```
/access/setlmingressmode?mode=<Service/Ingress>
```

#### 3.6.7.6 Check the Namespace being Watched

To check what namespace is currently being watched, run the **getlmingressnamespace** command. For example:

```
/access/getlmingressnamespace
```

#### 3.6.7.7 Set the Namespace to Watch

To set the **Namespace to Watch**, run the **setlmingressnamespace** command. For example:

```
/access/setlmingressnamespace?namespace=<Namespace>
```

#### 3.6.7.8 Check the Watch Timeout

To check the current **LMingress Watch Timeout** (in seconds), run the **getlmingresswatchtimeout** command. For example:

```
/access/getlmingresswatchtimeout
```

#### 3.6.7.9 Set the Watch Timeout

To set the **LMingress Watch Timeout** (in seconds), run the **setlmingresswatchtimeout** command. For example:

```
/access/setlmingresswatchtimeout?watchtimeout=<TimeoutInSeconds>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.6.7.10 Restart the Ingress Controller

To restart the LoadMaster Ingress Controller, run the **restartlmingress** command. For example:

```
/access/restartlmingress
```

### 3.6.8 Legacy WAF Settings

> The following commands only work on a LoadMaster with an WAF-enabled license.

If you have a WAF license and WAF Support, Kemp provides a number of commercial rules, such as **ip_reputation**, which can be set to automatically download and update on a daily basis. These commercial rules are targeted to protect against specific threats. The Kemp-provided commercial rules are available when signed up to WAF Support.

You can also upload other rules such as the ModSecurity core rule set which contains generic attack detection rules that provide a base level of protection for any web application.

You can also write and upload your own custom rules if desired.

With the WAF-enabled LoadMaster, you can choose whether to use Kemp-provided rules, custom rules which can be uploaded or a combination of both. The sections below provide details about commands that are specific to commercial rules, custom rules and a command which relates to both types of rule.

#### 3.6.8.1 Commands Relating to Commercial Rule Files

The commands in this section are all related to commercial rule files.

##### 3.6.8.1.1 Display the Commercial WAF Rule Settings

The **getwafsettings** command displays the values of the WAF options relating to commercial rules that appear in the **WAF Settings** screen on the LoadMaster WUI.

```
https://<LoadMasterIPAddress>/access/getwafsettings
```

**Related WUI Item**

Virtual Services > WAF Settings

##### 3.6.8.1.2 Enable Automatic Commercial Rule File Updates

The **setwafautoupdate** command allows you to enable the automatic downloading of updates to commercial WAF rule files. When this option is enabled, updated rules are downloaded on a daily


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

basis from Kemp. The default installation time for these rule updates is 4am. The time at which the installation of these rule file updates can be set by running the **SetWafInstallTime** command. For more information, refer to the **Set the Time of the Automatic Commercial Rule File Installation** section.

You can see what this is currently set to by running the **GetWafSettings** command. For more information, refer to the  section.

**https://<LoadMasterIPAddress>/access/setwafautoupdate?enable=<yes/no>**

**Related WUI Item**

Virtual Services > WAF Settings > Enable Automatic Rule Updates

3.6.8.1.3 Enable/Disable Automatic Installation of Commercial Rule File Updates

Automatic installation of updated commercial rule files can be enabled/disabled by running the following command.

https://<LoadMasterIPAddress>/access/setwafautoinstall?enable=<yes/no>

**Related WUI Item**

Virtual Services > WAF Settings > Enable Automated Installs

3.6.8.1.4 Set the Time of the Automatic Commercial Rule File Installation

The time of day of the automatic commercial rule file installation can be set by running the following command. This relates to the **When to Install** drop-down menu in the **WAF Settings** screen in the WUI.

**https://<LoadMasterIPAddress>/access/setwafinstalltime?hour=<hour>**

The hour is the hour value from the 24-hour clock (0-23), for example 13 is 1pm:

**https://10.11.0.31/access/setwafinstalltime?hour=13**

The range is 0-23. Minutes cannot be specified.

**Related WUI Item**

Virtual Services > WAF Settings > When to Install

3.6.8.1.5 Download WAF Commercial Rule File Updates Now

The WAF commercial rule file updates can be manually downloaded to the LoadMaster by running the following command. This relates to the **Download Now** button in the **WAF Settings** screen in the WUI.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

https://<LoadMasterIPAddress>/access/downloadwafrules

**Related WUI Item**

Virtual Services > WAF Settings > Download Now

> If there are no updates because the latest rules have already been downloaded, a message will be displayed which says **No updates available**.

3.6.8.1.6 Display the WAF Rule Change Log

A log of the changes which have been made to the Kemp WAF rule set can be downloaded by running the following command.

**https://<LoadMasterIPAddress>/access/getwafchangelog**

3.6.8.1.7 Manually Install Commercial Rule Files

The commercial rule files can be manually installed by running the following command. This relates to the **Install Now** button in the **WAF Settings** screen in the WUI.

**https://<LoadMasterIPAddress>/access/maninstallwafrules**

**Related WUI Item**

Virtual Services > WAF Settings > Install Now

> An error message will be displayed if any problems occur while installing the rules.

### 3.6.8.2 Commands Relating to Custom Rule Files

The commands in this section are all related to custom rules.

3.6.8.2.1 Upload a Custom Rule File or Rule Set

A WAF custom rule file can be uploaded by running a cURL command with the **addwafcustomrule** command and the **filename** parameter (required), for example:

```
curl -X POST --data-binary "@<FileName.conf>" -k
https://bal:<BalPassword>@<LoadMasterIPAddress>/access/addwafcustomrule?filen
ame=<FileName.conf>
```

In addition to uploading individual custom rule files, you can also upload custom rule sets (.tar.gz files). An example of uploading the OWASP core rule set is below:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
curl -X POST --data-binary "@owasp-modsecurity-crs-master.tar.gz" -k
https://bal:<BalPassword>@<LoadMasterIPAddress>/access/addwafcustomrule?filen
ame= SpiderLabs-owasp-modsecurity-crs-2.2.9-5-gebe8790.tar.gz
```

This relates to the **Custom Rules** section in the **WAF Settings** screen in the LoadMaster WUI.

**Related WUI Item**

Virtual Services > WAF Settings > Custom Rules

3.6.8.2.2 Delete a Custom Rule File

A custom rule file can be deleted by running the following command:

```
https://<LoadMasterIPAddress>/access/delwafcustomrule?filename=<filename>
```

For example:

```
https://10.11.0.30/access/delwafcustomrule?filename= modsecurity_crs_10_
ignore_static
```

> This does not delete the associated data file.

**Related WUI Item**

Virtual Services > WAF Settings > Custom Rules > Delete

3.6.8.2.3 Download a Custom Rule File

A custom rule file can be downloaded to your local machine by running the following command:

```
https://<LoadMasterIPAddress>/access/downloadwafcustomrule?filename=<filename>
```

For example:

```
https://10.11.0.30/access/downloadwafcustomrule?filename=modsecurity_crs_55_
response_profiling
```

If you run this command using cURL the file will be downloaded to your working directory in Linux.

**Related WUI Item**

Virtual Services > WAF Settings > Custom Rule Data > Download

3.6.8.2.4 Upload a Custom Rule Data File

A custom rule data file can be uploaded by running a cURL command with the **addwafcustomdata** command and the **filename** parameter (required), for example:

```
curl -X POST --data-binary "@<FileName.data>" -k
https://bal:<BalPassword>@<LoadMasterIPAddress>/access/addwafcustomdata?filen
ame=<filename.data>
```

**Related WUI Item**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Virtual Services > WAF Settings > Custom Rule Data > Add Data File

3.6.8.2.5 Delete a Custom Rule Data File

A custom rule data file can be deleted by running the following command:

**https://<LoadMasterIPAddress>/access/delwafcustomdata?filename=<filename.data>**

**Related WUI Item**

Virtual Services > WAF Settings > Custom Rule Data > Delete

3.6.8.2.6 Download a Custom Rule Data File

A custom rule data file can be downloaded by running the following command:

**https://<LoadMasterIPAddress>/access/downloadwafcustomdata?filename=<filename>**

For example:

**https://10.11.0.30/access/downloadwafcustomdata?filename=modsecurity_35_bad_robots**

**Related WUI Item**

Virtual Services > WAF Settings > Custom Rule Data > Download

### 3.6.8.3 Command Relating to Custom and Commercial Rules

The command in this section is related to both commercial and custom rules.

3.6.8.3.1 List WAF Rules

The **listwafrules** command displays a list of all installed rules (commercial and custom rules).

It also shows if the rules are active or not by displaying either **Active** or **Inactive** in the tag name. Active rules are ones that have been assigned to one or more Virtual Services.

**https://<LoadMasterIPAddress>/access/listwafrules**

**Related WUI Item**

Virtual Services > WAF Settings > Custom Rules

Virtual Services > View/Modify Services > Modify > WAF Options > Available Rules

### 3.6.8.4 Commands Relating to Remote Logging

The commands in this section relates to the WAF remote logging feature which allows the WAF audit logs to be sent to a central log repository.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.6.8.4.1 Set the WAF Logging Format

Set the WAF logging format by using the following command:

**https://<LoadMasterIPAddress>/access/setwaflogformat?logformat=<json/native>**

3.6.8.4.2 Disable Remote Logging

WAF remote logging can be disabled by running the following command:

**https://<LoadMasterIPAddress>/access/disablewafremotelogging**

3.6.8.4.3 Enable Remote Logging

WAF remote logging can be enabled by running the following command:

**https://<LoadMasterIPAddress>/access/enablewafremotelogging?remoteuri=<Remote ServerConsoleURI>&username=<RemoteUsername>&passwd=<RemotePassword>**

3.6.8.4.4 Save Temporary WAF Remote Log Data

Temporary WAF remote log data can be saved to your local machine by running the following command:

**https://<LoadMasterIPAddress>/access/logging/savemlogcdata**

3.6.8.4.5 Clear Temporary WAF Remote Log Data

Temporary WAF remote log data can be cleared by running the following command:

**https://<LoadMasterIPAddress>/access/logging/clearmlogcdata**

This removes all of the temporary WAF remote log data. This data is created when WAF remote logging is enabled on the LoadMaster and the remote log server is down or too slow to process the amount of logs generated. These log files are temporary and get automatically deleted/cleared once the data/logs have been sent to the remote log server.

### 3.6.9 WAF Settings

> The following commands only work on a LoadMaster with an WAF-enabled license.

To enable legacy WAF, run the following command:

**access/modvs?vs=1&InterceptMode=1**

To enable OWASP WAF, run the following command:

**access/modvs?vs=1&InterceptMode=2**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> You cannot switch from one WAF mode to another. You must first disable WAF (set **InterceptMode** to **0**) and then you can switch to the other mode.

You can configure the following WAF parameters using the **modvs** command:

| Name | Type | Default | Range | Description |
|---|---|---|---|---|
| Intercept | B | 0 | 0 – Disabled<br>1 – Enabled | You can set the **Intercept** parameter to **1** to enable legacy WAF. Setting **Intercept** to **0** disables WAF. |
| InterceptMode | B | 0 | 0 – Disabled<br>1 – Legacy<br>2 – OWASP | You cannot switch from one WAF mode to another. You must first disable WAF (set **InterceptMode** to **0**) and then you can switch to the other mode. |
| InterceptOpts | S | <unset> | | Most of the fields in the **WAF Options (Legacy)** section of the Virtual Service modify screen in the LoadMaster WUI can be set using this parameter. For further details, refer to the **WAF InterceptOpts Parameter** section. |
| OwaspOpts | S | <unset> | | Some of the OWASP WAF Virtual Service fields can be set using this parameter. For further details, refer to the **WAF OwaspOpts Parameter** section. |
| BlockingParanoia | I | 1 | 1 - 4 | The paranoia level at which the OWASP engine blocks |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | the request coming from the server. |
| ExecutingParanoia | I | 1 | 1 - 4 | The paranoia level at which the OWASP engine logs requests that are coming from the server. This value should not be lower than the **BlockingParanoia** level |
| AnomalyScoringThreshold | I | 100 | 1 - 10000 | Set the Anomaly Scoring Threshold value. Every detection rule in the CRS raises the anomaly score. If the cumulative anomaly score per request hits the configured limit, the request will be blocked |
| pcrelimit | I | 10000 | 1000 - 9999999 | This setting sets the maximum iterations that the internal PCRE engine will use to resolve a regular expression before failing a match. |
| JSONDLimit | I | 10000 | 1000 - 99999 | This value sets the maximum depth that will be accepted during JSON parsing. Lower values may cause a valid match to fail. Higher values may cause the WAF engine to run slower. |
| AlertThreshold | I | 0 - disabled | 0 - 100000 | This is the threshold of incidents per hour before sending an alert. Setting this to 0 disables alerting. |
| BodyLimit | I | | 1024 – 52428800 | Set the maximum size of |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | POST request bodies (in bytes) that the WAF engine will allow through. Higher values require more memory resources and may impact WAF engine performance. The default value is 1048576 bytes. |
| PostOtherContentTypes | S | | | When the **otherctypesenable** parameter is enabled, use the **POSTOtherContentTypes** parameter to enter a comma separated list of POST content types allowed for WAF analysis, for example text/plain,text/css. By default, all types (other than XML/JSON) are enabled. To set this to any other content types, set the value to any. |
| IPReputationBlocking | B | 0 | 0 – Disabled<br>1 – Enabled | Enables the checking of client addresses against the IP reputation database. |
| RuleSets | S | | | In OWASP CRS rulesets are described by three digit numbers. Specify the three digit number of the rulesets you wish to enable. For example: RuleSets=911, 913, 920…. |
| ExcludedWorkLoads | S | | | Specify a list of workloads |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | that the customer is running. By default, some workloads cause a lot of false positives, if someone is running one of workloads (drupal, wordpress, nextcloud, dokuwiki, cpanel, xenforo), add its name to the list will stop certain checks that are known to cause problems. |
| BlockedCountries | S | | Enter the two letter country codes that are to be blocked. |
| AuditParts | S | ABEFHKZ | Enter a valid string which contains the sections that are to be put in the wafaudit log for each request. Currently, only four values B, E, F, H are enabled. |
| CustomRules | | | Specify a list of custom rules that are to be configured for the Virtual Service. |
| DisabledRules | | | Specify a list of disabled rule IDs. |

3.6.9.0.1 WAF OwaspOpts Parameter

The WAF **OwaspOpts** parameter is a special parameter – it can be used to set the value for multiple fields, rather than just one field as with most other parameters.

To enable OWASP WAF, set the **InterceptMode** parameter to **2**.

The names of the specific WUI fields that the **OwaspOpts** parameter is related to, are listed in the table below.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

One or more field values can be set in one command. Multiple values can be set in the one command by separating the values with a semi-colon, for example:

```
/access/modvs?vs=<VirtualServiceIPAddress>&port=<Port>&prot=<tcp/udp>&OWASPOpts=auditnone;reqdataenable;resdataenable;jsondisable;xmldisable
```

The table below outlines what each of the values mean.

> The values that are related to the same WUI option are mutually exclusive. For example, you cannot set **Enable JSON Parser** to both **jsondisable** and **jsonenable**.

| Value | Related WUI Option | Default | Meaning |
|---|---|---|---|
| auditnone | **Audit mode** | No Audit | Set the **Audit mode** to **No Audit**. No data is logged. |
| auditrelevant | **Audit mode** | No Audit | Set the **Audit mode** to **Audit Relevant**. Logs data which is of a warning level and higher. |
| auditall | **Audit mode** | No Audit | Set the **Audit mode** to **Audit All**. Logs all data through the Virtual Service.<br>The **Audit All** option is not recommended for use in normal operation. **Audit All** should only be used when troubleshooting a specific problem. |
| reqdataenable | **Inspect HTML POST Request Bodies** | Disabled | Enable the **Inspect HTML POST Request Bodies** option. This verifies the data supplied in POST requests. |
| reqdatadisable | **Inspect HTML POST Request Bodies** | Disabled | Disable the **Inspect HTML POST Request Bodies**option. |
| resdataenable | **Process HTTP Responses** | Disabled | Enable the **Process HTTP Responses**option. This verifies data sent from the Real Servers. This can be CPU and memory intensive. |
| resdatadisable | **Process HTTP** | Disabled | Disable the **Process HTTP Responses** option. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | Responses | | |
|---|---|---|---|
| jsondisable | **Enable JSON Parser** | Enabled | Disable the JSON parser.<br>This option is only relevant if the **Inspect HTML POST Request Bodies**option is enabled. |
| jsonenable | **Enable JSON Parser** | Enabled | Enable the JSON parser. This enables the verification of JSON POSTs.<br>This option is only relevant if the **Inspect HTML POST Request Bodies**option is enabled. |
| xmldisable | **Enable XML Parser** | Enabled | Disable the XML parser.<br>This option is only relevant if the **Inspect HTML POST Request Bodies**option is enabled. |
| xmlenable | **Enable XML Parser** | Enabled | Enable the XML parser. This enables the verification of XML POSTs.<br>This option is only relevant if the **Inspect HTML POST Request Bodies**option is enabled. |
| otherctypesdisable | **Enable Other Content Types** | Disabled | Disable verification of POST content types (other than XML/JSON). |
| otherctypesenable | **Enable Other Content Types** | Disabled | Enable verification of POST content types (other than XML/JSON).<br>Enabling the inspection of any other content types may increase system resource utilization (CPU and memory). A specific list of content types should be considered.<br>When this option is enabled, the **POSTOtherContentTypes** parameter can be used to enter a comma-separated list of POST content types allowed for WAF analysis. By default, all types (other than XML/JSON) are enabled. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.6.9.1 OWASP Custom Rulesets

To add a new custom rule file, run the **addowaspcustomrule** command. For example:

**/access/addowaspcustomrule?filename=owasp-cus.conf**

To delete an existing rule file, run the **delowaspcustomrule** command. For example:

**/access/delowaspcustomrule?filename=owasp-cus**

To download a custom rule file, run the **downloadowaspcustomrule** command. For example:

**/access/downloadowaspcustomrule?filename=<filename>**

The **filename** parameter is mandatory. Specify the name of the OWASP custom rule file to download in the **filename** parameter. You can get the filename by going to **Web Application Firewall > Custom Rules** in the WUI. If you run the command using a web browser, the file will download to the location specified in your browser settings.

#### 3.6.9.2 OWASP Custom Data File

To add a custom data file, run the **addowaspcustomdata** command. For example:

**/access/addowaspcustomdata?filename=owasp-cust.data**

To delete an existing data file, run the **delowaspcustomdata** command. For example:

**/access/delowaspcustomdata?filename=owasp-cust**

To download a custom data file, run the **downloadowaspcustomdata** command. For example:

**/access/downloadowaspcustomdata?filename=<filename>**

The **filename** parameter is mandatory. Specify the name and extension (either **.txt** or **.data**) of the OWASP custom data file to download in the **filename** parameter. You can get the filename by going to **Web Application Firewall > Custom Rules** in the WUI. If you run the command using a web browser, the file will download to the location specified in your browser settings.

#### 3.6.9.3 OWASP Rules

To list all available OWASP rules, run the **owasprules** command. For example:

**/access/owasprules**

To show all OWASP rules and their enablement state for a Virtual Service, run the **owasprules?vs=<VSIndex>** command. For example:

**/access/owasprules?vs=1**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

To show an OWASP rule and its enablement state for a Virtual Service, run the **owasprules?vs=<VSIndex>&rule=<RuleId>** command. For example:

**/access/owasprules?vs=1&rule=911100**

> To get the rule ID of a OWASP rule, check the user interface (**Virtual Services > View/Modify Services > Modify > WAF > Manage Rules** and expand the relevant rule section to see the associated rule ids) or run the **owasprules** command. You can also specify a prefix, such as 913 for the **scanner-detection** rules, to enable/disable/view all rules that contain that prefix in their ID. For more information on the OWASP rules including a list of IDs for each ruleset and rule, refer to the OWASP Standard Rules Technical Note.

To specify that a custom rule should run before the OWASP Core Rule Set (CRS), enable the **runfirst** parameter. For example:

**owasprules?vs=<VSIndex>&rule=<RuleName>&runfirst=1**

If the **runfirst** parameter is disabled, the custom rule runs after the CRS.

To turn off all OWASP rules for a particular ruleset of a Virtual Service, run the **owasprules?vs=<VSIndex>&rule=<RuleId>&enable=<yes/no>** command. For example:

**/access/owasprules?vs=1&rule=911100&enable=no**

To filter the list of rules, run the **owasprules?vs=<VSIndex>&filter=<term>&enable=<yes/no>** command. For example, to filter the list of OWASP rules that contain the value SQL:

**/access/owasprules?vs=1&filter=sql&enable=yes**

To enable/disable all rules for a Virtual Service, run the **owasprules?vs=<VSIndex>&enable=<yes/no>** command. For example:

**/access/owasprules?vs=1&enable=yes**

## 3.7 Global Balancing

### 3.7.1 Manage Fully Qualified Domain Names (FQDNs)

#### 3.7.1.1 Add FQDN

An FQDN can be added by running the following command:

**https://<LoadMasterIPAddress>/access/addfqdn?fqdn=<FQDNName>**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

**fqdn** is a required parameter for this command.

#### 3.7.1.2 Delete FQDN

An FQDN can be deleted by running the following command:

**https://<LoadMasterIPAddress>/access/delfqdn?fqdn=<FQDNName>**

**fqdn** is a required parameter for this command.

#### 3.7.1.3 List FQDNs

The existing FQDNs can be listed by running the following command:

**https://<LoadMasterIPAddress>/access/listfqdns**

Example output for the **listfqdns** command is provided below:

```
<Response stat="200" code="ok">
<Success><Data><fqdn><FullyQualifiedDomainName>www.example.com.</FullyQualifiedDomainNam
e>
<SelectionCriteria>rr</SelectionCriteria>
<FailTime>0</FailTime>
<SiteRecoveryMode>auto</SiteRecoveryMode>
<Mapping>1</Mapping>
<failover>N</failover>
<publicRequestValue>3</publicRequestValue>
<privateRequestValue>3</privateRequestValue>
<LocalSettings>0</LocalSettings>
<UnanimousChecks>N</UnanimousChecks>
<Map><Status>Up</Status>
<Index>1</Index>
<IPAddress>172.16.193.50</IPAddress>
<Cluster>LocalLM</Cluster>
<Checker>clust</Checker>
<CheckerPort>0</CheckerPort>
<Weight>1000</Weight>
<MappedAddress>172.16.193.50</MappedAddress>
<MappedPort>80</MappedPort>
<MappedName>HTTP VS</MappedName>
<Enable>Y</Enable>
</Map></fqdn><fqdn><FullyQualifiedDomainName>www.example.com.</FullyQualifiedDomainName>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
<SelectionCriteria>rr</SelectionCriteria>
<FailTime>0</FailTime>
<SiteRecoveryMode>auto</SiteRecoveryMode>
<Mapping>3</Mapping>
<failover>N</failover>
<publicRequestValue>0</publicRequestValue>
<privateRequestValue>0</privateRequestValue>
<LocalSettings>0</LocalSettings>
<UnanimousChecks>N</UnanimousChecks>
<Map><Status>Down</Status>
<Index>3</Index>
<IPAddress>1.1.1.1</IPAddress>
<Cluster>RemoteLM</Cluster>
<Checker>clust</Checker>
<CheckerPort>0</CheckerPort>
<Weight>1000</Weight>
<MappedAddress>172.16.193.254</MappedAddress>
<MappedPort>80</MappedPort>
<MappedName>HTTP VS</MappedName>
<Enable>Y</Enable>
</Map></fqdn></Data>
</Success>
</Response>
```

#### 3.7.1.4 Show FQDN

The **showfqdn** command displays various details relating to the specified FQDN:

**https://<LoadMasterIPAddress>/access/showfqdn?fqdn=<FQDNName>**

Example output for the **showfqdn** command is provided below:

```
<Response stat="200" code="ok">
<Success>
<Data>
<fqdn>
<Status>Up</Status>
<FullyQualifiedDomainName>www.example.com.</FullyQualifiedDomainName>
<SelectionCriteria>rr</SelectionCriteria>
<FailTime>0</FailTime>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
<SiteRecoveryMode>auto</SiteRecoveryMode>
<Mapping>1</Mapping>
<failover>N</failover>
<publicRequestValue>3</publicRequestValue>
<privateRequestValue>3</privateRequestValue>
<LocalSettings>0</LocalSettings>
<UnanimousChecks>N</UnanimousChecks>
<Map><Status>Up</Status>
<Index>1</Index>
<IPAddress>172.16.193.50</IPAddress>
<Cluster>LocalLM</Cluster>
<Checker>clust</Checker>
<CheckerPort>0</CheckerPort>
<Weight>1000</Weight>
<MappedAddress>172.16.193.50</MappedAddress>
<MappedPort>80</MappedPort>
<MappedName>HTTP VS</MappedName>
<Enable>Y</Enable>
</Map></fqdn></Data>
</Success>
</Response>
```

#### 3.7.1.5 Modify FQDN

An existing FQDN can be modified by running the following command:

**`https://<LoadMasterIPAddress>/access/modfqdn?fqdn=<FQDNName>`**

The **modfqdn** command accepts the following optional parameters:

| Name | Type | Default | Range | Additional Information |
|---|---|---|---|---|
| SelectionCriteria | S | rr | rr = round robin<br>wrr = weighted round robin<br>fw = fixed | The selection criteria for addresses associated with the FQDN. For a description of each of these options, refer to the **GEO, Feature Description** on the Kemp Documentation Page. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | weighting<br>rsr = real server load<br>prx = proximity<br>lb = location based<br>all = all available | |
| FailTime | I | 0 | 0-1440 (minutes) | If a failure delay is not set, normal health checking is performed. If set, this parameter defines the number of minutes to wait after a failure before finally disabling it. Once it is disabled, it will not normally be brought back into operation. |
| siterecoverymode | S | auto | auto – automatic<br>manual - manual | This parameter defines the Site Recovery Mode.<br>If this is set to automatic, upon site recovery the site is brought back into operation immediately.<br>If this is set to manual, once the site has failed, the site is disabled. Manual intervention is required to restore normal operation. |
| failover | B | 0 – disabled | 0 – Disabled<br>1 – Enabled | This parameter is only relevant if the **SelectionCriteria** is set to **lb** (Location Based).<br>Enable/disable FQDN failover. |
| publicRequestValue | I | 0 – Public Sites Only | 0 – Public Sites Only | Restrict responses to clients from public IP addresses to specific classes of site. For an explanation of the different |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | 1 – Prefer Public Sites<br>2 – Prefer Private Sites<br>3- Any Sites | settings and their values please see the section **Public Requests & Private Requests** below including the table |
| privateRequestValue | I | 0 – Private Sites Only | 0 – Private Sites Only<br>1 – Prefer Private Sites<br>2 – Prefer Public Sites<br>3 – Any Sites | Restrict responses to clients from private IP addresses to specific classes of site. For an explanation of the different settings and their values please see the section **Public Requests & Private Requests** below including the table |
| ecsforpubpriv | B | 0 – Disabled | 0 – Disabled<br>1 – Enabled | When this parameter is disabled, the device uses the client request's source IP address to determine if the request is public or private. When enabled, the device uses the EDNS Client Subnet (ECS) value instead (if one is received) to determine if the request is public or private. This option becomes inactive in either of the following conditions:<br>• The **EDNS Client Subnet (ECS)** option (in **Global Balancing > Miscellaneous Params**) is disabled.<br>• The **Public Requests** and **Private Requests** values are both set to **All Sites**. |
| LocalSettings | B | 0 – Disabled | 0 – Disabled | Enabling this parameter provides two additional parameters for the FQDN – |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | 1 – Enabled | **localttl** and **localsticky**. |
| localttl | I | Defaults to the value of the global **ttl** value when an FQDN is created. | 1 to 86400 | The Time To Live (TTL) value dictates how long the reply from the GEO LoadMaster can be cached by other DNS servers or client devices. The time interval is defined in seconds. This value should be as practically low as possible. The default value for this field is 10. |
| localsticky | I | Defaults to the value of the global **persist** value when an FQDN is created. | 0 to 86400 | Stickiness, also known as persistence, is the property that enables all name resolution requests from an individual client to be sent to the same resources until a specified period of time has elapsed. |
| unanimouschecks | B | 0 – Disabled | 0 – Disabled<br>1 – Enabled | When this parameter is enabled, if any IP addresses fail health checking - the other FQDN IP addresses which belong to the same cluster will be forced down. |

**Public Requests & Private Requests**

The Public Requests & Private Requests options replace the old Isolate Public/Private Sites option which was available on LoadMasters with firmware up to and including 7.1-28. The new settings offer administrators greater flexibility when configuring an FQDN.

These new settings allow administrators to selectively respond with public or private sites based on whether the client is from a public or private IP. For example, administrators may wish to allow only private clients to be sent to private sites.

The following table outlines settings and their configurable values:

| Setting | Value | Client Type | Site Types Allowed |
|---|---|---|---|
| **PublicRequests** | Public Only | Public | Public |
| | Prefer Public | Public | Public, Private if no public |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | Prefer Private | Public | Private, Public if no private |
| | All Sites | Public | Private and Public |
| **Private Requests** | Private Only | Private | Private |
| | Prefer Private | Private | Private, Public if no private |
| | Prefer Public | Private | Public, Private if no public |
| | All Sites | Private | Private and Public |

#### 3.7.1.6 Add Map

A map can be added to the FQDN by running the following command:

```
https://<LoadMasterIPAddress>/access/addmap?fqdn=<FQDNName>&ip=<IPAddressToAdd>&clust=<ClusterName>
```

The **clust** parameter is optional.

> In LoadMaster firmware versions prior to 7.2.57, there is an entry limit of 64 IP addresses per FQDN. If you attempt to add more than this, you get an error message saying **Too many IP addresses already specified**.

> The entry limit was increased to 256 IP addresses in LoadMaster firmware version 7.2.57. If you attempt to add more than this, you get an error message saying **Limit of 256 IP Addresses has been reached for the FQDN**. It is recommended that the LoadMaster should have sufficient memory space (minimum 8GB of RAM) to configure the maximum of 256 IP addresses per FQDN.

> Kemp does not recommend downgrading the LoadMaster firmware version to a previous version where the endpoint limit of IP addresses per FQDN is smaller than the number of IP addresses in your configured FQDNs.

#### 3.7.1.7 Modify a Map

To modify a map, run the following command:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
https://<LoadMasterIPAddress>/access/modmap?fqdn=<FQDNName>&ip=<IPAddressToModify>
```

The modmap command accepts the following optional parameters:

| Name | Type | Default | Range | Additional Information |
|---|---|---|---|---|
| Checker | S | icmp | none<br>icmp<br>tcp<br>clust<br>http<br>https | Specify the type of checking to be done on this IP address |
| checkerurl | S | / | Maximum of 127 characters | By default, the health checker tries to access the URL forward slash (/) to determine if the machine is available. You can specify a different URL using the **checkerurl** parameter. The URL must begin with a forward slash (/). The URL cannot contain **http:** or **https:**. The URL can be a maximum of 127 characters. |
| checkercodes | S | | 300-599 | A space-separated list of HTTP status codes that should be treated as successful when received from the server. There is a maximum of 32 codes. There is a limit of 127 characters. |
| checkerhost | S | | | A hostname can be supplied in the request to the server. If this is not set, the server address is sent as the host. There is a limit of 127 characters. Allowed characters: alphanumerics and **-._:** |
| checkerhttpmethod | S | get | 1 - GET<br>2 - POST | When accessing the health check URL, the system can use either the **GET** or the **POST** method. If **POST** is selected, the **checkerpostdata** parameter is also valid. |
| checkerpostdata | S | | | Up to 2047 characters of POST data can be |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | passed to the server. This parameter is only relevant if the **checkerhttpmethod** parameter is set to **2** (POST). |
| Weight | I | 1000 | 1-65535 | Specify the weight associated with the IP address. The address with the highest weight is returned. This is only relevant if the **Selection Criteria** for the FQDN is set to **Weighted Round Robin** or **Fixed Weighting**. |
| Enable | B | 1 – Enabled | 1 – Enable<br>0 – Disable | Enable or disable the IP address. |
| Cluster | I | <unset> | | Specify the ID number of the cluster to associate with the IP address. |
| MapAddress | A | <unset> | | This is only relevant when the **Selection Criteria** is set to **Real Server Load**, the **Checker** is set to **Cluster Checks** and the cluster is of type **Remote LM** or **Local LM**.<br><br>Enter a Virtual Service IP address to be mapped from the relevant LoadMaster. |
| MapPort | I | <unset> | | This is only relevant when the **Selection Criteria** is set to **Real Server Load**, the **Checker** is set to **Cluster Checks** and the cluster is of type **Remote LM** or **Local LM**.<br><br>This parameter is used in conjunction with the **MapAddress** parameter to specify an IP address and port combination to be mapped.<br><br>If this parameter is not set, the health check will check all Virtual Services with the same IP address as the one selected. If one of them is in an “Up” status, the FQDN will show as “Up”. If a port is specified, the health check will only check against the health of that Virtual Service when |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

checking the health of the FQDN.

> The maximum length of an API call is 1024 characters. If you want to make a larger call, use the POST method.

To delete a health check, set the **checker** parameter to **none**. For example:

**/access/modmap?fqdn=<FQDN>&ip=<IPAddress>&checker=none**

#### 3.7.1.8 Delete a Map

To delete a map, run the following command:

**https://<LoadMasterIPAddress>/access/delmap?fqdn=<FQDNName>&ip=<IPAddressToDelete>**

#### 3.7.1.9 Change the Location of a Map

To change the location of a map, run the following command:

**https://<LoadMasterIPAddress>/access/changemaploc?fqdn=<FQDNName>&ip=<IPaddress>&lat=<LatitudeSeconds>&long=<LongituteSeconds>**

> This command is only relevant when the **Selection Criteria** for the FQDN is set to **Proximity**.

The **lat** and **long** values should be entered as an integer containing the total seconds. This total seconds value is converted to degrees, minutes and seconds when displayed in the WUI.

> To set north and east coordinates use a positive integer value. To set south and west coordinates use a negative integer value.

There are 60 seconds in a minute and 60 minutes in a degree.

- Degrees = º
- Minutes = ‘
- Seconds = “
- 60” = 1’
- 3600” = 1º
- 3660 = 1º1’
- 3661 = 1º1’1”


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

You can also represent this as a decimal value for degrees where the minutes and seconds are divided by 3600 to get the decimal value.

#### 3.7.1.10 Add a Location

To add a country or continent, run the following command:

```
https://<LoadMasterIPAddress>/access/addcountry?fqdn=<FQDNName>&ip=<IPAddress
>&countrycode=<TwoCharacterCountry/ContinentCode>&iscontinent=<yes/no>
```

> This command is only relevant when the **Selection Criteria** for the FQDN is set to **Location Based**. Refer to the **Modify FQDN** section for details on how to modify the **Selection Criteria**.

> The FQDN name is case sensitive.

> The country code and continent codes used are the standard ISO codes.

> When adding a country - the **iscontinent** parameter must be set to **no**.

> When adding a continent - the **iscontinent** parameter must be set to **yes**.

> The value for **countrycode** should be in uppercase.

> To specify everywhere as the country, type **ALL** as the country code and set the **iscontinent** parameter to **yes.**

To add a custom location, run the following command:

```
https://<LoadMasterIPAddress>/access/addcountry?fqdn=<FQDNName>&ip=<IPAddress
>&customlocation=<CustomLocationName>
```

It is also possible to add a country/continent and a custom location in the one command – simply include all of the parameters, for example:

```
https://<LoadMasterIPAddress>/access/addcountry?fqdn=<FQDNName>&ip=<IPAddress
>&countrycode=<TwoCharacterCountry/ContinentCode>&iscontinent=<yes/no>&custom
location=<CustomLocationName>
```

#### 3.7.1.11 Remove a Location

To remove a country, run the following command:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

**https://<LoadMasterIPAddress>/access/removecountry?fqdn=<FQDNName>&ip=<IPAddress>&countrycode=<TwoCharacterCountry/ContinentCode>&iscontinent=<yes/no>**

> This command is only relevant when the **Selection Criteria** for the FQDN is set to **Location Based**.

> The FQDN name is case sensitive.

> When removing a country - the **iscontinent** parameter must be set to **no**.

> When removing a continent - the **iscontinent** parameter must be set to **yes**.

> The value for **countrycode** should be in uppercase.

> To specify everywhere as the country, type **ALL** as the country code and set the **iscontinent** parameter to **yes**.

To remove a custom location, run the following command:

**https://<LoadMasterIPAddress>/access/removecountry?fqdn=<FQDNName>&ip=<IPAddress>&customlocation=<CustomLocationName>**

It is also possible to remove a country/continent and a custom location in the one command – simply include all of the parameters, for example:

**https://<LoadMasterIPAddress>/access/removecountry?fqdn=<FQDNName>&ip=<IPAddress>&countrycode=<TwoCharacterCountry/ContinentCode>&iscontinent=<yes/no>&customlocation=<CustomLocationName>**

#### 3.7.1.12 Change Checker Address

To change the address of a checker, run the following command:

**https://<LoadMasterIPAddress>/access/changecheckeraddr?fqdn=<FQDNName>&ip=<MapIPAddress>&checkerip=<CheckerIPAddress>&port=<CheckPort>**

The **changecheckeraddr** command requires the following parameters:

| Name | Type | Default | Range | Additional Information |
|---|---|---|---|---|
| checkerip | S | <unset> | | Specify the address used to health check the IP address. |
| port | I | 80 | 1-65530 | Specify the port used to health check the IP address. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Specifying an empty value for the the **checkerip** or **port** parameters sets them to their default values (blank for the **checkerip** and **80** for the **port**).

#### 3.7.1.13 Additional Records

You can add a new **TXT**, **CNAME** and **MX** record to an FQDN by running the **addrr** command. For example:

**/access/addrr?fqdn=<FQDNName>&type=txt&rdata=<ResourceRecordData>**

**/access/addrr?fqdn=<FQDNName>&type=cname&name=<Name>**

**/access/addrr?fqdn=<FQDNName>&type=mx&rdata=<ResourceRecordData>**

You can modify an existing **TXT**, **CNAME** and **MX** record by running the **modrr** command. For example:

**/access/modrr?fqdn=<FQDNName>&type=txt&param=rdata&value=<UpdatedResourceRecordData>&id=<IndexOfRecord>**

**/access/modrr?fqdn=<FQDNName>&type=cname&param=name&value=<UpdatedName>&id=<IndexOfRecord>**

**/access/modrr?fqdn=Example.com&type=mx&id=<IndexOfRecord>&param=<rdata/priority>&value=<Value>**

> When modifying an MX record, you can specify either the rdata or priority as the param, depending on what parameter you want to modify the value for.

You can delete an existing **TXT**, **CNAME** and **MX** record by running the **dellrr** command. For example:

**/access/delrr?fqdn=<FQDNName>&id=<Index>**

> To retrieve the Index number of an existing record, run the showfqdn command.

### 3.7.2 Manage Clusters

#### 3.7.2.1 List Clusters

Existing clusters can be listed by running the following command:

**`https://<LoadMasterIPAddress>/access/listclusters`**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.7.2.2 Show Cluster

Details about a specific cluster can be displayed by running the following command:

**https://<LoadMasterIPAddress>/access/showcluster?id=<ClusterID>**

> **id** is a required parameter for this command.

> The **Address** entry is deprecated.

#### 3.7.2.3 Add Cluster

A cluster can be added by running the following command:

**https://<LoadMasterIPAddress>/access/addcluster?ip=<ClusterIPAddress>&name=<ClusterName>**

> The **ip** and **name** parameters are required for this command.

#### 3.7.2.4 Delete Cluster

A cluster can be deleted by running the following command:

**https://<LoadMasterIPAddress>/access/delcluster?ip=<ClusterIPAddress>**

> The **ip** parameter is required for this command.

#### 3.7.2.5 Modify Cluster

A cluster can be modified by running the following command:

**https://<LoadMasterIPAddress>/access/modcluster?id=<ClusterID>**

The **modcluster** commands accepts the following optional parameters:

| Name | Type | Default | Range | Additional Information |
|---|---|---|---|---|
| type | S | Default | default<br>remoteLM<br>localLM | Change the type of the cluster |
| name | S | | | Specify a name for the cluster |
| checker | S | none | none<br>tcp | Specify the method used to check the status of the cluster |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | icmp | |
| checkerport | I | 0 | 1-65530 | Set the port used for checking the cluster. This parameter is only relevant if the **checker** is set to **tcp**. |
| enable | B | 1 – Enabled | 1 = Enabled<br>0 = Disabled | Enable/disable the cluster |

#### 3.7.2.6 Change Cluster Location

To change a cluster location, run the following command:

**`https://<LoadMasterIPAddress>/access/clustchangeloc?ip=<ClusterIPAddress>&latsecs=<LatitudeSeconds>&longsecs=<LongitudeSeconds>`**

The **latsecs** and **longsecs** values should be entered as an integer containing the total seconds. This total seconds value is converted to degrees, minutes and seconds when displayed in the WUI.

There are 60 seconds in a minute and 60 minutes in a degree.

- Degrees = º
- Minutes = ‘
- Seconds = “
- 60” = 1’
- 3600” = 1º
- 3660 = 1º1’
- 3661 = 1º1’1”

You can also represent this as a decimal value for degrees where the minutes and seconds are divided by 3600 to get the decimal value.

### 3.7.3 Miscellaneous Params

#### 3.7.3.1 List the Miscellaneous Parameters

To list the GEO miscellaneous parameters, run the following command:

**`https://<LoadMasterIPAddress>/access/listparams`**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.7.3.2 Modify Miscellaneous Parameters

The GEO miscellaneous parameters can be modified by running the following command:

**`https://<LoadMasterIPAddress>/access/modparams`**

The **modparams** command accepts the following optional parameters:

| Name | Type | Default | Range | Additional Information |
|---|---|---|---|---|
| zone | S | <unset> | | Specify the zone name. |
| PerZoneSOA | B | 0 - Disabled | 0 - Disabled<br>1 - Enabled | If this option is enabled, the Source of Authority (SOA) parameters are applied only to the zone. If it is disabled, the SOA parameters apply to all Fully Qualified Domain Names (FQDNs). The Apply to Zone Only option is disabled by default. |
| SourceOfAuthority | S | <unset> | | Set the response set for Source of Authority requests. |
| namesrv | S | <unset> | | Set the response sent for Name Server requests. |
| SOAEmail | S | <unset> | | Email address of the person responsible for the zone and to which email may be sent to report errors or problems. This is the email address of a suitable DNS administrator but more commonly the technical contact for the domain.<br>By convention (in RFC 2142) it is suggested that the reserved mailbox hostmaster is used for this purpose but any valid email address will work.<br>The format is **<MailboxName>.<Domain>.com**, for example, **hostmaster.example.com** (uses a full stop (**.**) rather than the usual **@** symbol because the **@** symbol has other uses in the zone file) but mail is sent to **hostmaster@example.com**. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| dclustunavail | B | | 0 - Disabled<br>1 - Enabled | This option is disabled by default. When this option is enabled, requests to the cluster are dropped if a GEO cluster is disabled. |
| glueip | S | | | This option allows you to set the IP address of the name server to return in additional records in a DNS response. To unset the **Glue Record IP** so that 0.0.0.0 is returned, set the glueip parameter to an empty string. |
| TTL | I | <unset> | 1-86400 | Set the Time To Live (TTL) (in seconds) of the responses returned by the LoadMaster. |
| Txt | S | | | This option allows you to modify the TXT record. |
| EDNSECS | B | | 0 - Disabled<br>1 - Enabled | The **EDNS Client Subnet (ECS)** option is enabled by default on new installations but if you are upgrading a LoadMaster that previously used GEO functionality then the option is disabled. When enabled, the ECS field (if included in the request) is used to determine the client location. When disabled, this field is ignored. |
| persist | I | 0 | 0-86400 | This corresponds with the **Stickiness** WUI field. This determines how long (in seconds) a specific response will be returned to a host. |
| CheckInterval | I | 120 | 9-3600 | Set how often (in seconds) that devices will be checked.<br><br>**Note:** The interval value must be greater than the **ConnTimeout** value multiplied by the **RetryAttempts** value (Interval > Timeout * Retry + 1). This is to ensure that the next health check does not start before the previous one completes. If the timeout or |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

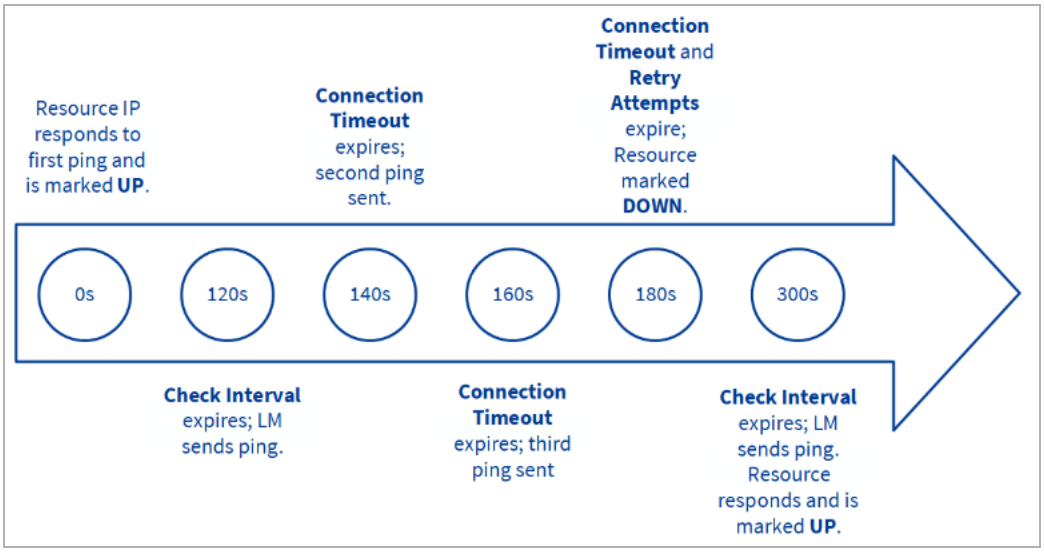
| | | | | |
|---|---|---|---|---|
| | | | | retry values are increased to a value that breaks this rule, the interval value will be automatically increased. |
| ConnTimeout | I | 20 | 4-60 | Set the timeout (in seconds) for the check request. |
| RetryAttempts | I | 2 | 2-10 | Set the number of times the check will be retried before the device is marked as failed. |

The timeline diagram below illustrates what happens from the time a resource IP is added or enabled, to when it goes down and then comes back up again:

When a resource IP is enabled/created, an ICMP request is sent by the LoadMaster to the resource IP. Assuming it responds, the resource is marked UP.

After 120 seconds has elapsed (the default Check Interval), an ICMP request is sent to the resource IP. If 20 seconds (the default Connection Timeout) elapses and the IP fails to respond, the LoadMaster will send up to two additional requests (the default Retry Attempts) and wait for 20 seconds between each. If all three of these requests receive no response, then the resource is marked down, and the Check Interval timer is reset.

After 120 seconds elapses, the LoadMaster attempts to send an ICMP request to the resource IP. If the resource has now come back up and responds before the Connection Timeout elapses, the LoadMaster marks it UP and resets the Check Interval timer.





© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.7.3.3 Upload a Location Data Patch File

A location data update file can be uploaded. To do this, run a cURL command:

```
curl -X POST --data-binary "@<GEOPatchFileName>" -k
https://<username>:<password>@<LoadMasterIPAddress>/access/locdataupdate
```

### 3.7.4 IP Range Selection Criteria

#### 3.7.4.1 List the IP Addresses

To list the IP addresses set for the IP range selection criteria, run the following command:

```
https://<LoadMasterIPAddress>/access/listips
```

#### 3.7.4.2 Show IP Address Details

To show details of a specific IP address which is set for the IP range selection criteria, run the following command:

```
https://<LoadMasterIPAddress>/access/showip?ip=<IPAddress>
```

#### 3.7.4.3 Add IP Address

To add an IP address to the IP range selection criteria, run the following command:

```
https://<LoadMasterIPAddress>/access/addip?ip=<IPAddress>
```

#### 3.7.4.4 Delete IP Address

To delete an IP address from the IP range selection criteria, run the following command:

```
https://<LoadMasterIPAddress>/access/delip?ip=<IPAddress>
```

#### 3.7.4.5 Change the Location for an IP Address

To change the location for an IP address, run the following command:

```
https://<LoadMasterIPAddress>/access/modiploc?ip=<IPAddress>&lat=<LatitudeMin
utes>&long=<LongitudeMinutes>
```

The **lat** and **long** values should be entered as an integer containing the total seconds. This total seconds value is converted to degrees, minutes and seconds when displayed in the WUI.

There are 60 seconds in a minute and 60 minutes in a degree.

- Degrees = º
- Minutes = ‘
- Seconds = “
- 60” = 1’


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- 3600” = 1°
- 3660 = 1°1’
- 3661 = 1°1’1”

You can also represent this as a decimal value for degrees where the minutes and seconds are divided by 3600 to get the decimal value.

#### 3.7.4.6 Delete IP Location

To delete the location for an IP address, run the following command:

**https://<LoadMasterIPAddress>/access/delipploc?ip=<IPAddress>**

#### 3.7.4.7 Add IP Country

To add a country association to an existing IP address, run the following command:

**https://<LoadMasterIPAddress>/access/addipcountry?ip=<IPAddress>&<param>=<value>**

| Name | Mandatory | Type | Default | Range | Additional Information |
|---|---|---|---|---|---|
| countrycode | No | S | <unset> | Valid country code | A valid, uppercase, two-digit country code must be used. |
| customloc | No | S | <unset> | Existing custom location | The name of an existing custom location. |

> Either the **countrycode** or **customloc** parameter must be entered when running the command.

#### 3.7.4.8 Remove IP Country

To remove the country association from an IP address, run the following command:

**https://<LoadMasterIPAddress>/access/removeipcountry?ip=<IPAddress>**

#### 3.7.4.9 List the Custom Locations

To list the existing custom locations, run the following command:

**https://<LoadMasterIPAddress>/access/listcustomlocation**

#### 3.7.4.10 Add a Custom Location

A custom location can be added by running the following command:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

**https://<LoadMasterIPAddress>/access/addcustomlocation?location=<CustomLocationName>**

> The **location** parameter is required.

#### 3.7.4.11 Edit a Custom Location

To rename an existing custom location, run the following command:

**https://<LoadMasterIPAddress>/access/editcustomlocation?cloldname=<OldCustomLocationName>&clnewname=<NewCustomLocationName>**

#### 3.7.4.12 Delete a Custom Location

To remove an existing custom location, run the **deletecustomlocation** command, using the following format:

**https://<LoadMasterIPAddress>/access/deletecustomlocation?clName=<CustomLocationName>**

### 3.7.5 IP Access List Settings

Refer to the subsections below for details on the RESTful API commands relating to the IP access-list settings.

#### 3.7.5.1 Retrieve the IP Access List Settings

To retrieve the IP access-list settings, run the following command:

**https://<LoadMasterIPAddress>/access/geoacl/getsettings**

#### 3.7.5.2 Enable/Disable Automatic IP Access List Updates

To enable/disable automatic updates, run the following command:

**https://<LoadMasterIPAddress>/access/geoacl/setautoupdate?enable=<1/0>**

#### 3.7.5.3 Enable/Disable Automatic Installation of the IP Access List Updates

To enable/disable automatic installation of the updates, run the following command:

**https://<LoadMasterIPAddress>/access/geoacl/setautoinstall?enable=<1/0>**

#### 3.7.5.4 Set the Time of the Automatic Installation

To set the time of the automatic installation, run the following command:

**https://<LoadMasterIPAddress>/access/geoacl/setinstalltime?hour=<hour>**

The hour is the hour value from the 24-hour clock (0-23), for example 13 is 1pm:

**https://10.11.0.31/access/geoacl/setinstalltime?hour=13**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

The range is 0-23. Minutes cannot be specified. It is not possible to set the install time if automatic installation is disabled.

#### 3.7.5.5 Download the Updates Now

To download the updates now, run the following command:

**https://<LoadMasterIPAddress>/access/geoacl/updatenow**

#### 3.7.5.6 Install the Updates Now

To install any downloaded updates now, run the following command:

**https://<LoadMasterIPAddress>/access/geoacl/installnow**

#### 3.7.5.7 View the Access List

To retrieve the access-list, run the following command:

**https://<LoadMasterIPAddress>/access/geoacl/downloadlist**

#### 3.7.5.8 View Changes to the Access List

To retrieve a list of changes which were made to the access-list, run the following command:

**https://<LoadMasterIPAddress>/access/geoacl/downloadchanges**

#### 3.7.5.9 View the User-Defined Allow List

To retrieve the contents of the user-defined allow list (which overrides the access-list), run the following command:

**https://<LoadMasterIPAddress>/access/geoacl/listcustom**

#### 3.7.5.10 Add an Address to the Allow List

To add an IP address or network (in CIDR format) to the allow list, run the following command:

**https://<LoadMasterIPAddress>/access/geoacl/addcustom?addr=<Address>**

#### 3.7.5.11 Remove an IP Address or Network from the Allow List

To remove an IP address or network from the allow list, run the following command:

**https://<LoadMasterIPAddress>/access/geoacl/removecustom?addr=<Address>**

### 3.7.6 Configure DNSSEC

To configure DNSSEC using the API, use the commands outlined in the below sections.

#### 3.7.6.1 Generate the Key Signing Keys (KSKs)

To generate the KSKs, run the following command:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
https://<LoadMasterIPAddress>/access/geogenerateksk?algorithm=<Algorithm>&key
size=<KeySize>
```

| Name | Type | Default | Range | Description |
|---|---|---|---|---|
| algorithm | S | RSASHA256 | RSASHA256, NSEC3RSASHA1, NSEC3RSASHA1 | Specify the cryptographic algorithm to use. If this parameter is omitted, the default value is used. |
| keysize | I | 2048 | 1024, 2048, 4096 | Specify the key size (in bits). If this parameter is omitted, the default value is used. |

#### 3.7.6.2 Import the KSKs

To import the KSKs, run the following cURL command:

```
curl -F "publickey=@/tmp/example.com.+008+62284.key" -F
"privatekey=@/tmp/example.com.+008+62284.private" -k
https://<Username>:<Password>@<LoadMasterIPAddress>/access/geoimportksk
```

This command uploads both KSK files at the same time.

#### 3.7.6.3 Delete the KSK Files

To delete the KSK files, run the following command:

```
https://<LoadMasterIPAddress>/access/geodeleteksk
```

#### 3.7.6.4 Enable/Disable DNSSEC

To enable/disable DNSSEC, run the following command:

```
https://<LoadMasterIPAddress>/access/geosetdnssec?enable=<yes/no>
```

#### 3.7.6.5 Retrieve the DNSSEC Configuration Settings

To retrieve the DNSSEC settings, run the following command:

```
https://<LoadMasterIPAddress>/access/geoshowdnssec
```

### 3.7.7 GSLB Statistics

To retrieve the Global Server Load Balancing (GSLB) statistics, run the following command:

```
https://<LoadMasterIPAddress>/access/geostats
```

### 3.7.8 Enable/Disable GEO

#### 3.7.8.1 Check if GEO is Enabled

To check if GEO is enabled, run the following command:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

**https://<LoadMasterIPAddress>/access/isgeoenabled**

#### 3.7.8.2 Enable GEO

GEO can be enabled by running the following command:

**https://<LoadMasterIPAddress>/access/enablegeo**

#### 3.7.8.3 Disable GEO

GEO can be disabled by running the following command:

**https://<LoadMasterIPAddress>/access/disablegeo**

## 3.8 Statistics

Statistics for all the Virtual Services and Real Servers can be obtained by using the **stats** command.

> If you run the **stats** command on the admin node when using LoadMaster clustering – the output will show the combined totals of all machines.

**https://<LoadMasterIPAddress>/access/stats**

If the command executes without error, the statistics for all the Virtual Services and Real Servers are returned in the following format.

> The Real Server statistics are returned on a per Virtual Service basis.

```
<Response stat="200" code="ok">
<Success>
<Data>
<CPU>
<total>
<User>0</User>
<System>1</System>
<Idle>99</Idle>
<IOWaiting>0</IOWaiting>
</total>
<cpu0>
<User>0</User>
<System>0</System>
<HWInterrupts>0</HWInterrupts>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

<SWInterrupts>0</SWInterrupts>
<Idle>99</Idle>
<IOWaiting>0</IOWaiting>
</cpu0>
<cpu1>
<User>1</User>
<System>0</System>
<HWInterrupts>0</HWInterrupts>
<SWInterrupts>0</SWInterrupts>
<Idle>99</Idle>
<IOWaiting>0</IOWaiting>
</cpu1>
</CPU>
<Memory>
<MBtotal>2003</MBtotal>
<memused>312140</memused>
<MBused>304</MBused>
<percentmemused>15</percentmemused>
<memfree>1739060</memfree>
<MBfree>1698</MBfree>
<percentmemfree>85</percentmemfree>
</Memory>
<Network>
<eth0>
<ifaceID>0</ifaceID>
<speed>10000</speed>
<in>0.0</in>
<inbytes>149</inbytes>
<inbytesTotal>1511851</inbytesTotal>
<out>0.0</out>
<outbytes>122</outbytes>
<outbytesTotal>5702883</outbytesTotal>
</eth0>
<bnd2>
<ifaceID>2</ifaceID>
<speed>1000</speed>
<in>0.0</in>


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
<inbytes>0</inbytes>
<inbytesTotal>3960</inbytesTotal>
<out>0.0</out>
<outbytes>0</outbytes>
<outbytesTotal>38396</outbytesTotal>
</bnd2>
</Network>
<DiskUsage>
<partition>
<name>/var/log</name>
<GBtotal>7.19</GBtotal>
<GBused>0.02</GBused>
<percentused>0</percentused>
<GBfree>7.17</GBfree>
<percentfree>100</percentfree>
</partition>
<partition>
<name>/var/log/userlog</name>
<GBtotal>7.68</GBtotal>
<GBused>0.02</GBused>
<percentused>0</percentused>
<GBfree>7.67</GBfree>
<percentfree>100</percentfree>
</partition>
</DiskUsage>
<ClientLimits>
<Totals>
<CurrentConnections>0</CurrentConnections>
<CurrentConnectionsBlocked>0</CurrentConnectionsBlocked>
<SuccessfulConnectionAttempts>0</SuccessfulConnectionAttempts>
<SuccessfulRequestAttempts>0</SuccessfulRequestAttempts>
<SuccessfulMatchedRuleAttempts>0</SuccessfulMatchedRuleAttempts>
<ConnectionAttemptsBlocked>0</ConnectionAttemptsBlocked>
<RequestAttemptsBlocked>0</RequestAttemptsBlocked>
<MatchedRulesBlocked>0</MatchedRulesBlocked>
</Totals>
<glbcps> </glbcps>
```



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

<glbrps> </glbrps>
</ClientLimits>
<CountryCounts>
<DifferentCountries>0</DifferentCountries>
<Total> </Total>
<LastHour> </LastHour>
<LastDay> </LastDay>
</CountryCounts>
<VStotals>
<ConnsPerSec>0</ConnsPerSec>
<TotalConns>0</TotalConns>
<BitsPerSec>0</BitsPerSec>
<TotalBits>0</TotalBits>
<BytesPerSec>0</BytesPerSec>
<TotalBytes>0</TotalBytes>
<PktsPerSec>0</PktsPerSec>
<TotalPackets>0</TotalPackets>
</VStotals>
<Vs>
<VSAddress>10.35.48.17</VSAddress>
<VSPort>80</VSPort>
<VSProt>tcp</VSProt>
<Index>3</Index>
<Status>down</Status>
<ErrorCode>0</ErrorCode>
<Enable>1</Enable>
<TotalConns>0</TotalConns>
<TotalPkts>0</TotalPkts>
<TotalBytes>0</TotalBytes>
<TotalBits>0</TotalBits>
<ActiveConns>0</ActiveConns>
<BytesRead>0</BytesRead>
<BytesWritten>0</BytesWritten>
<ConnsPerSec>0</ConnsPerSec>
<ConnsRateBlocked>0</ConnsRateBlocked>
<RequestsRateBlocked>0</RequestsRateBlocked>
<MaxConnsBlocked>0</MaxConnsBlocked>


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
<WafEnable>0</WafEnable>
<InterceptMode>0</InterceptMode>
</Vs>
<Vs>
<VSAddress>10.35.48.24</VSAddress>
<VSPort>80</VSPort>
<VSProt>tcp</VSProt>
<Index>1</Index>
<Status>down</Status>
<ErrorCode>0</ErrorCode>
<Enable>1</Enable>
<TotalConns>0</TotalConns>
<TotalPkts>0</TotalPkts>
<TotalBytes>0</TotalBytes>
<TotalBits>0</TotalBits>
<ActiveConns>0</ActiveConns>
<BytesRead>0</BytesRead>
<BytesWritten>0</BytesWritten>
<ConnsPerSec>0</ConnsPerSec>
<ConnsRateBlocked>0</ConnsRateBlocked>
<RequestsRateBlocked>0</RequestsRateBlocked>
<MaxConnsBlocked>0</MaxConnsBlocked>
<WafEnable>0</WafEnable>
<InterceptMode>2</InterceptMode>
<Requests>0</Requests>
<Incidents>0</Incidents>
<Incidents_Hour>0</Incidents_Hour>
<Incidents_Day>0</Incidents_Day>
<Incidents_Dayover>0</Incidents_Dayover>
</Vs>
<TPS>
<Total>0</Total>
<SSL>0</SSL>
</TPS>
<Timestamp>
<Sec>1637849344</Sec>
<Usec>682846</Usec>
```



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
<Period>5006303</Period>
</Timestamp>
<ChangeTime>1637849309</ChangeTime>
</Data>
</Success>
</Response>
```

The statistics are explained in the table below.

| Section | Name | Additional Information |
|---|---|---|
| CPU | User | The percentage of the CPU spent processing in user mode |
| | System | The percentage of the CPU spent processing in system mode |
| | Idle | The percentage of CPU which is idle |
| | IOWaiting | The percentage of the CPU spent waiting for I/O to complete |
| | HWInterrupts | The percentage of hardware interrupts |
| | SWInterrupts | The percentage of software interrupts |
| Memory | MBtotal | The total memory available in Mb |
| | Memused | The amount of memory in use |
| | MBused | The amount of memory in use in Mb |
| | Percentmemused | The percentage of memory used |
| | Memfree | The amount of memory free |
| | MBfree | The amount of free memory in Mb |
| | Percentmemfree | The percentage of free memory |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| DiskUsage | Name | The name of the partition |
| | GBtotal | The total disk usage in Gb |
| | GBused | The amount of disk space usage in Gb |
| | Percentused | The percentage of disk space in use |
| | GBfree | The amount of disk space free |
| | Percentfree | The percentage of disk space free |
| ClientLimits | CurrentConnections | The total number of current connections |
| | CurrentConnectionsBlocked | The number of connections currently blocked |
| | SuccessfulConnectionAttempts | The number of successful connection attempts |
| | SuccessfulRequestAttempts | The number of successful request attempts |
| | SuccessfulMatchedRuleAttempts | The number of rules that were successfully matched |
| | ConnectionAttemptsBlocked | The number of connection attempts that were blocked |
| | RequestAttemptsBlocked | The number of request attempts that were blocked |
| | MatchedRulesBlocked | The number of connections that were blocked due to a matching rule limit |
| | glbcps | Global connections per second |
| | glbrps | Global requests per second |
| | DifferentCountries | The number of different countries that connections were made from |
| | LastHour | The number of different countries that connections were made from in the last hour |
| | LastDay | The number of different countries that connections were made from in the last day |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| Network | ifaceID | The ID number of the interface |
| | Speed | The speed of the link |
| | In | Inbound |
| | Out | Outbound |
| | Total (TPS) | The total number of Transactions Per Second (TPS) |
| | SSL (TPS) | The total number of SSL Transactions Per Second (TPS) |
| VStotals | ConnsPerSec | The number of connections per second |
| | TotalConns | The total number of Virtual Service connections |
| | BitsPerSec | The number of bits per second |
| | BytesPerSec | The number of bytes per second |
| | PktsPerSec | The number of packets per second |
| | TotalPackets | The total number of packets transferred |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| Vs | VSAddress | The IP address of the Virtual Service |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| | VSPort | The port of the Virtual Service |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| | VSProt | The protocol of the Virtual Service. This will either be **tcp** or **udp**. |
| | Index | The index (ID) number of the Virtual Service |
| | ErrorCode | The error code |
| | Enable | Displays whether the Virtual Service is enabled (1) or disabled (0) |
| | TotalConns | The total number of connections made |
| | TotalPkts | The total number of packets |
| | TotalBytes | The total number of bytes |
| | TotalBits | The total number of bits |
| | ActiveConns | The total number of connections that are currently active. When using ESP, all connections going through the login process are counted as active connections for the Virtual Service. They are not counted as active connections for the Real Server because they are not actual connections to the Real Server. The WUI page displays the number of active connections associated with the Real Servers, while SNMP displays the number of active connections for the Virtual Service. Without ESP, these values are identical. When using ESP, the Virtual Service counts can be much higher than the final counts going to the Real Servers, due to the above reason. |
| | BytesRead | The total number of bytes read |
| | BytesWritten | The total number of bytes written |
| | ConnsPerSec | The total number of Virtual Service connections per second |
| | ConnsRateBlocked | The rate at which connections were blocked |
| | RequestsRateBlocked | The rate at which requested were blocked |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| | MaxConnsBlocked | The maximum number of connections blocked |
| | WafEnable | Displays whether WAF is enabled (1) or disabled (0). The WAF statistics below will only be displayed if WAF is enabled on the Virtual Service. |
| | Requests | The total number of requests handled by the WAF (shows all requests, whether they were blocked or not). Two requests will be recorded for each connection – one incoming and one outgoing request. |
| | Incidents | The total number of events handled by the WAF (requests that were blocked). |
| | Incidents_Hour | The number of events that have happened in the current hour (since xx.00.00). |
| | Incidents_Day | The number of events that have happened since midnight (local time). |
| | Incidents_Dayover | The number of times the event counter has gone over the configured warning threshold today. For example, if the threshold is set to 10 and there has been 20 events, this counter will be set to 2. The warning threshold is set on a per-Virtual Service basis by setting the **AlertThreshold** parameter. For further information, refer to the **Virtual Service Control** section. |
| ChangeTime | ChangeTime | The time of the last configuration change on the LoadMaster. The configuration has not changed if this value has not changed. This only works if session management is enabled. The time is represented in “Unix time or epoch time” (also known as Portable Operating System Interface (POSIX) time) format. This is a system for describing instants in time, defined as the number of seconds that have elapsed since 00:00:00 Coordinated Universal Time |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | |
|---|---|
| | (UTC), Thursday 1st January 1970, not counting leap seconds. For example, 1484150723 is the equivalent of GMT: Wed, 11th January 2017 16:05:23 GMT. There are conversion tools are available online to convert the value to an easily readable format. |

## 3.9 SDN Statistics

The device information for the specified SDN controller can be retrieved by running the following command:

**https://<LoadMasterIPAddress>/access/sdndeviceinfo?cid=<ControllerID>**

Example output for the **sdndeviceinfo** command is provided below:

```
<Response stat="200" code="ok">
<Success>
<Data>
<controller id="62">
<deviceinfo>
<uid>openflow:151936205333838</uid>
<name>br3</name>
<type/>
<vendor>Nicira, Inc.</vendor>
<product>Open vSwitch</product>
<firmware>2.3.1</firmware>
<serial>None</serial>
<ip>10.35.8.47</ip>
<ifcount>3</ifcount>
<status/>
<portinfo>
<port>
<id>1</id>
<name>prt3</name>
<state/>
<mac>52:34:63:89:05:17</mac>
<curspeed>current_speed=0</curspeed>
<maxspeed>max_speed=0</maxspeed>
</port>
<port>
<id>2</id>
<name>vnet5</name>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
<state/>
<mac>fe:54:00:79:04:75</mac>
<curspeed>current_speed=10000</curspeed>
<maxspeed>max_speed=0</maxspeed>
</port>
<port>
<id>local</id>
<name>br3</name>
<state/>
<mac>8a:2f:67:8c:25:4e</mac>
<curspeed/>
<maxspeed/>
</port>
</portinfo>
</deviceinfo>
<deviceinfo>
<uid>openflow:60003129350209</uid>
<name>br1</name>
<type/>
<vendor>Nicira, Inc.</vendor>
<product>Open vSwitch</product>
<firmware>2.3.1</firmware>
<serial>None</serial>
<ip>10.35.8.47</ip>
<ifcount>4</ifcount>
<status/>
<portinfo>
<port>
<id>3</id>
<name>vnet6</name>
<state/>
<mac>fe:54:00:ed:2d:aa</mac>
<curspeed>current_speed=10000</curspeed>
<maxspeed>max_speed=0</maxspeed>
</port>
<port>
<id>2</id>
<name>prt11</name>
<state/>
<mac>de:8f:f3:cc:58:7a</mac>
<curspeed>current_speed=0</curspeed>
<maxspeed>max_speed=0</maxspeed>
</port>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
<port>
<id>1</id>
<name>prt1</name>
<state/>
<mac>5e:b2:61:21:c8:20</mac>
<curspeed>current_speed=0</curspeed>
<maxspeed>max_speed=0</maxspeed>
</port>
<port>
<id>local</id>
<name>br1</name>
<state/>
<mac>36:92:91:35:d8:41</mac>
<curspeed/>
<maxspeed/>
</port>
</portinfo>
</deviceinfo>
<deviceinfo>
<uid>openflow:130736296040257</uid>
<name>br2</name>
<type/>
<vendor>Nicira, Inc.</vendor>
<product>Open vSwitch</product>
<firmware>2.3.1</firmware>
<serial>None</serial>
<ip>10.35.8.47</ip>
<ifcount>4</ifcount>
<status/>
<portinfo>
<port>
<id>2</id>
<name>vnet7</name>
<state/>
<mac>fe:54:00:85:ca:9f</mac>
<curspeed>current_speed=10000</curspeed>
<maxspeed>max_speed=0</maxspeed>
</port>
<port>
<id>1</id>
<name>prt2</name>
<state/>
<mac>8a:8d:81:78:10:8b</mac>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
<curspeed>current_speed=0</curspeed>
<maxspeed>max_speed=0</maxspeed>
</port>
<port>
<id>3</id>
<name>prt22</name>
<state/>
<mac>d2:10:88:e8:98:f6</mac>
<curspeed>current_speed=0</curspeed>
<maxspeed>max_speed=0</maxspeed>
</port>
<port>
<id>local</id>
<name>br2</name>
<state/>
<mac>76:e7:6a:7c:17:41</mac>
<curspeed/>
<maxspeed/>
</port>
</portinfo>
</deviceinfo>
<deviceinfo>
<uid>openflow:217995646047043</uid>
<name>br4</name>
<type/>
<vendor>Nicira, Inc.</vendor>
<product>Open vSwitch</product>
<firmware>2.3.1</firmware>
<serial>None</serial>
<ip>10.35.8.47</ip>
<ifcount>4</ifcount>
<status/>
<portinfo>
<port>
<id>2</id>
<name>vnet4</name>
<state/>
<mac>fe:54:00:ab:30:91</mac>
<curspeed>current_speed=10000</curspeed>
<maxspeed>max_speed=0</maxspeed>
</port>
<port>
<id>1</id>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
                <name>prt4</name>
                <state/>
                <mac>f2:fc:c5:31:1e:a0</mac>
                <curspeed>current_speed=0</curspeed>
                <maxspeed>max_speed=0</maxspeed>
                </port>
                <port>
                <id>3</id>
                <name>vnet8</name>
                <state/>
                <mac>fe:54:00:6a:f8:4e</mac>
                <curspeed>current_speed=10000</curspeed>
                <maxspeed>max_speed=0</maxspeed>
                </port>
                <port>
                <id>local</id>
                <name>br4</name>
                <state/>
                <mac>c6:44:11:0b:93:43</mac>
                <curspeed/>
                <maxspeed/>
                </port>
                </portinfo>
                </deviceinfo>
                </controller>
                </Data>
                </Success>
        </Response>
```

The output is described in the table below.

| Section | Name | Additional Information |
|---|---|---|


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| Device Information | uid | The Unique Identifier (UID) for the device. |
| | name | The name of the device. |
| | vendor | The device vendor. |
| | product | The type of device. |
| | firmware | The firmware version of the device. |
| | serial | The serial number of the device. |
| | ip | The IP address of the device. |
| | ifcount | The number of interfaces on the device. |
| | status | The status of the device. |
| Port Information | id | The ID number of the port. |
| | name | The name of the port. |
| | mac | The MAC address of the port. |
| | curspeed | The current speed of the port. |
| | maxspeed | The maximum speed of the port. |

The path information for the specified SDN controller (and corresponding Virtual Service configuration on the LoadMaster) can be retrieved by running the following command:

**https://<LoadMasterIPAddress>/access/sdnpathinfo?cid=<ControllerID>**

Example output for the **sdnpathinfo** command is provided below:

```
<Response stat="200" code="ok">
        <Success>
                <Data>
                        <pathinfo>
                                <path>
                                        <dir>fwd</dir>
                                        <source>10.35.8.49</source>
                                        <dest>10.35.8.89</dest>
                                        <pathelem>
                                                <switch>
                                                        <idx>0</idx>
                                                        <name>baloo</name>
                                                        <dpid>00:08:a0:1d:48:92:4
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
                </switch>
                <inport>
                        <idx>25</idx>
                        <name>25</name>
                        <byte>3397596</byte>
                </inport>
                <outport>
                        <idx>14</idx>
                        <name>14</name>
                        <byte>3395099</byte>
                </outport>
        </pathelem>
        <pathelem>
                <switch>
                        <idx>1</idx>
                        <name>bagheera</name>
                        <dpid>00:08:40:a8:f0:87:0
                </switch>
                <inport>
                        <idx>15</idx>
                        <name>15</name>
                        <byte>3388430</byte>
                </inport>
                <outport>
                        <idx>6</idx>
                        <name>6</name>
                        <byte>1566302</byte>
                </outport>
        </pathelem>
</path>
<path>
        <dir>rev</dir>
        <source>10.35.8.89</source>
        <dest>10.35.8.49</dest>
        <pathelem>
                <switch>
                        <idx>0</idx>
                        <name>baloo</name>
                        <dpid>00:08:a0:1d:48:92:4
                </switch>
                <inport>
                        <idx>25</idx>
                        <name>25</name>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
                                        <byte>3397596</byte>
                                </inport>
                                <outport>
                                        <idx>14</idx>
                                        <name>14</name>
                                        <byte>3395099</byte>
                                </outport>
                        </pathelem>
                        <pathelem>
                                <switch>
                                        <idx>1</idx>
                                        <name>bagheera</name>
                                        <dpid>00:08:40:a8:f0:87:0
                                </switch>
                                <inport>
                                        <idx>15</idx>
                                        <name>15</name>
                                        <byte>3388430</byte>
                                </inport>
                                <outport>
                                        <idx>6</idx>
                                        <name>6</name>
                                        <byte>1566302</byte>
                                </outport>
                        </pathelem>
                </path>
        </pathinfo>
    </Data>
  </Success>
</Response>
```

The output is described in the table below.

| Section | Name | Additional Information |
|---|---|---|
| path | dir | The direction of the path. |
| | source | The source IP address. |
| | dest | The destination IP address. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| switch | idx | The index number of the switch along the path. |
| | name | The name of the switch. |
| | dpid | The Data Path ID (DPID) of the switch. |
| inport | idx | The switch port number of the inbound traffic. |
| | name | The name of the inbound port. |
| | byte | The number of bytes transferred on the port. |
| outport | idx | The switch port number of the outbound traffic. |
| | name | The name of the outbound port. |
| | byte | The number of bytes transferred on the port. |

## 3.10 Real Servers

A Real Server can be managed by using one of the commands below.

**https://<LoadMasterIPAddress>/access/showrs?vs=<IPaddr>&port=<Port>&prot=<tcp/udp>&rs=<RS IPaddr>&rsport=<RS-Port>**
**https://<LoadMasterIPAddress>/access/delrs?vs=<IPaddr>&port=<Port>&prot=<tcp/udp>&rs=<RS IPaddr>&rsport=<RS-Port>**
**https://<LoadMasterIPAddress>/access/delrs?vs=<IPaddr>&port=<Port>&prot=<tcp/udp>&rs=!<RSIndex>**
**https://<LoadMasterIPAddress>/access/addrs?vs=<IPaddr>&port=<Port>&prot=<tcp/udp>&rs=<RS IPaddr>&rsport=<RS-Port>**
**https://<LoadMasterIPAddress>/access/modrs?vs=<IPaddr>&port=<Port>&prot=<tcp/udp>&rs=<RS IPaddr>&rsport=<RS-Port>**

The **rs** parameter accepts integers (ID), service names (for SubVSs) and IP addresses. The ID can be found in the **<RSIndex>** element when doing a **showvs** command, for example:

```
...
<Rs>
<Status>Up</Status>
<VSIndex>1</VSIndex>
<RsIndex>3</RsIndex>
<Addr>10.154.201.3</Addr>
<Port>80</Port>
<Forward>nat</Forward>
<Weight>1000</Weight>
<Limit>0</Limit>
<Enable>Y</Enable>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
<Critical>N</Critical>
</Rs>
...
```

| Id | IP Address | Port | Forwarding method | Weight | Limit | Rules Status | Operation |
|---|---|---|---|---|---|---|---|
| 5 | 10.154.11.73 | 80 | nat | 1000 | 0 | 1 Enabled | Disable Modify Delete |

Alternatively, check the **Modify Virtual Service** screen in the WUI, which lists Real Server ID in the **Id** column in the **Real Servers** section.

For the **rs** parameter, when using <RSIndex>, always precede it with an exclamation mark ('!').

For example:

**https://<LoadMasterIPAddress>/access/showrs?vs=<IPaddr>&port=<Port>&prot=<tcp/udp>&rs=!<RSIndex>**

The Real Server IP address (that the **rs** parameter can be set to) can be in either IPv4 or IPv6 formats:

- Example IP**v**4 address:10.11.0.24
- Example IP**v**6 address: fdce:9b36:e54f:110::40:14

Some SubVS parameters, such as **critical**, need to be modified using the **RsIndex** of the SubVS, for example:

**https://<LoadMasterIPAddress>/access/modrs?vs=<ParentVSIndex>&rs=!<RsIndexOfTheSubVS>&critical=<0/1>**

To modify the settings of a Real Server which has been added to a SubVS, use the VS **Index** of the SubVS and the **RsIndex** of the Real Server, for example:

**https://<LoadMasterIPAddress>/access/modrs?vs=<SubVSIndex>&rs=!<RsIndex>&critical=<0/1>**

**addrs** and **modrs** accept the following additional (optional) parameters.

| Name | Type | Default | Range | Description |
|---|---|---|---|---|
| addtoallsubvs | B | 0 | 0 - Disabled<br>1 - Enabled | Enable this option when adding a Real Server to all SubVSs of a Virtual Service.<br>When using this parameter, ensure you set the **vs** parameter to the ID of the SubVS rather than the parent Virtual Service.<br>Run the **listvs** command to retrieve the **VSIndex** of the SubVS. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| weight | I | 1000 | 1-65535 | When using weighted round robin scheduling, the weight of a Real Server is used to indicate what relative proportion of traffic should be sent to the server. Servers with higher values will receive more traffic.<br>The weight of a SubVS can also be updated using the **modrs** command - set the **rs** to the number that appears in the **Id** column for the relevant SubVS in the parent Virtual Service modify screen. |
| newport | I | <unset> | 3-65535 (change the Port of the Real Server) | The port on the Real Server to be used. |
| forward | S | nat | nat, route | The type of forwarding method used. The default method is NAT. Direct server return can only be used with Layer 4 services. |
| enable | B | 1 | | Enable or disable the Real Server. |
| limit | I | 0 | 0-100000 | The maximum number of open connections that can be sent to a Real Server before it is taken out of rotation. |
| non_local | B | 0 | 0 - Disabled<br>1 - Enabled | By default only Real Servers on local networks can be assigned to a Virtual Service. Enabling this option will allow a non-local Real Server to be assigned to the Virtual Service.<br>This option will only be available if **nonlocalrs** has been enabled and the **Transparent** option has been disabled on the relevant Virtual Service. |
| critical | B | 0 | 0 - Disabled<br>1 - Enabled | Enabling this parameter indicates that the Real Server is required for the Virtual Service to be considered available. The Virtual Service will be marked as down if the Real Server has failed or is disabled. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| follow | I | <unset> | RsIndex of Real Server to follow | Specify what Real Server the health check is based on by setting this parameter to the **RsIndex** of the Real Server to be followed. This can either be set to the **RsIndex** of the same Real Server to health check based on that particular Real Server status, or another Real Server can be specified. For example – if Real Server 1 is down, any Real Servers which have their health check based on Real Server 1 will also be marked as down, regardless of their actual Real Server status. |

If the service is a Layer 7 service then setting the 'forward' parameter to 'route' will have no effect

### 3.10.1 Enabling/Disabling Real Servers

#### 3.10.1.1 Globally Enable/Disable a Real Server

A Real Server can be enabled/disabled globally, that is, for all Virtual Services by using the following commands:

**https://<LoadMasterIPAddress>/access/enablers?rs=<IPaddr>**

or

**https://<LoadMasterIPAddress>/access/disablers?rs=<IPaddr>**

The Real Server IP address (that the rs parameter can be set to) can be in either IPv4 or IPv6 formats:

- Example IP**v**4 address:10.11.0.24
- Example IP**v**6 address: fdce:9b36:e54f:110::40:14

#### 3.10.1.2 Locally Enable/Disable a Real Server

A Real Server can be disabled/enabled locally, that is, for one specific Virtual Service, by using the following commands:

**https://<LoadMasterIPAddress>/access/modrs?vs=<VirtualServiceIPAddress>&port=<Port>&prot=<tcp/udp>&rs=<RealServerIPAddress>&rsport=<port>&enable=n**

or

**https://<LoadMasterIPAddress>/access/modrs?vs=<VirtualServiceIPAddress>&port=<Port>&prot=<tcp/udp>&rs=<RealServerIPAddress>&rsport=<port>&enable=y**
**The Real Server IP address (that the rs parameter can be set to) can be in either IPv4 or IPv6 format.**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- Example IPv4 address: 10.11.0.24
- Example IPv6 address: fdce:9b36:e54f:110::40:14

## 3.11 Rules & Checking

Content Rules can be managed using the RESTful API.

### 3.11.1 Show Rules

The rules which are in use within the system can be displayed by using the **showrule** command.

```
https://<LoadMasterIPAddress>/access/showrule?[name=<Rule Name>]&[type=<0-5>]
```

Running the **showrule** command with no parameters will list all of the existing rules. The list can be reduced by either specifying the name of a rule or the type of the rules to be displayed.

The type is one of the following:

| Value | Type | Description |
|---|---|---|
| 0 | MatchContentRule | The original rules. |
| 1 | AddHeaderRule | Rule to Add header field |
| 2 | DeleteHeaderRule | Rule to Delete a header field. |
| 3 | ReplaceHeaderRule | Rule to modify a header field. |
| 4 | ModifyURLRule | URL rewrite rule. |
| 5 | ReplaceBodyRule | Rule to replace a body string. |

### 3.11.2 Delete a Rule from the System

A rule can be deleted by using the **delrule** command**.**

```
https://<LoadMasterIPAddress>/access/delrule?name=<Rule Name>
```

### 3.11.3 Add/Modify a Rule on the System

Rules can be added or modified by using the **addrule** and **modrule** commands.

```
https://<LoadMasterIPAddress>/access/addrule?name=<Rule Name>
https://<LoadMasterIPAddress>/access/modrule?name=<Rule Name>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

The following parameters can be set (dependent on the type of rule). When creating a Rule - if the "type" is not specified, it will default to zero, that is, a MatchContentRule. If "type" is not specified when performing a modify operation, the type will not be changed.

Unless modifying/adding an **AddHeaderRule**, the **pattern** parameter must be supplied.
**Type 0 (MatchContentRule)**

| Name | Type | Default | Range | Additional Information |
|---|---|---|---|---|
| matchtype | S | regex | •regex<br>•prefix<br>•postfix | The type of matching to be performed by the rule. |
| inchost | B | N | | Prepend the hostname to request URI before performing the match. |
| nocase | B | N | | Ignore case when comparing the strings. |
| negate | B | N | | Invert the sense of the match. |
| incquery | B | N | | Append the query string to the URI before performing a match. |
| header | S | <unset> | See below | The header field name that should be matched. If no header field is set, the default is to match in the URL. Set this to **body** to match |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | on the body of a request. |
| pattern | S | <unset> | | The pattern to be matched. |
| setonmatch | I | <unset> | 0-9 | If the rule is successfully matched, set the specified flag. |
| onlyonflag | I | <unset> | 0-9 | Only try to execute this rule if the specified flag is set.<br><br>Using the **onlyonflag**, **onlyonnoflag**, and **setonmatch** parameters, it is possible to make rules dependent on each other, that is, only execute a particular rule if another rule has been successfully matched. For more detailed instructions on 'chaining' rules, refer to the Content Rules, Feature Description document. |
| onlyonnoflag | I | <unset> | 0-9 | Only try to execute this rule |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | if the specified flag is not set. |
| mustfail | B | 0 - Disabled | 0 – Disabled<br>1 - Enabled | If this rule is matched, then always fail to connect. |

> The **header** parameter is optional and is the header in which the match is to be performed.

**Type 1 (AddHeaderRule)**

| Name | Type | Default | Additional Information |
|---|---|---|---|
| header | S | <unset> | Name of the header field to be added. |
| replacement | S | <unset> | The replacement string. You can enter a maximum of 255 characters in this parameter. |
| onlyonflag | I | <unset> | Range: 1-9<br>Only try to execute this rule if the specified flag is set.<br>Using the **onlyonflag**, **onlyonnoflag**, and **setonmatch** parameters, it is possible to make rules dependent on each other, that is, only execute a particular rule if another rule has been successfully matched. For more detailed instructions on 'chaining' rules, refer to the Content Rules, Feature Description document. |
| onlyonnoflag | I | <unset> | Range: 1-9<br>Only try to execute this rule if the specified flag is not set. |

**Type 2 (DeleteHeaderRule)**

| Name | Type | Default | Additional Information |
|---|---|---|---|
| pattern | S | <unset> | The pattern to be matched. |
| onlyonflag | I | <unset> | Range: 1-9 |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | Only try to execute this rule if the specified flag is set.<br><br>Using the **onlyonflag**, **onlyonnoflag**, and **setonmatch** parameters, it is possible to make rules dependent on each other, that is, only execute a particular rule if another rule has been successfully matched. For more detailed instructions on 'chaining' rules, refer to the Content Rules, Feature Description document. |
| onlyonnoflag | I | <unset> | Range: 1-9<br><br>Only try to execute this rule if the specified flag is not set. |

**Type 3 (ReplaceHeaderRule)**

| Name | Type | Default | Additional Information |
|---|---|---|---|
| header | S | <unset> | The header field name where the substitution should be performed. |
| replacement | S | <unset> | The replacement string. |
| pattern | S | <unset> | The pattern to be matched. |
| onlyonflag | I | <unset> | Range: 1-9<br><br>Only try to execute this rule if the specified flag is set.<br><br>Using the **onlyonflag**, **onlyonnoflag**, and **setonmatch** parameters, it is possible to make rules dependent on each other, that is, only execute a particular rule if another rule has been successfully matched. For more detailed instructions on 'chaining' rules, please refer to the Content Rules, Feature Description document. |
| onlyonnoflag | I | <unset> | Range: 1-9<br><br>Only try to execute this rule if the specified flag is not set. |

**Type 4 (ModifyURLRule)**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| Name | Type | Default | Additional Information |
|---|---|---|---|
| replacement | S | <unset> | How the URL is to be modified. |
| pattern | S | <unset> | The pattern to be matched. |
| onlyonflag | I | <unset> | Range: 1-9<br>Only try to execute this rule if the specified flag is set.<br>Using the **onlyonflag**, **onlyonnoflag**, and **setonmatch** parameters, it is possible to make rules dependent on each other, that is, only execute a particular rule if another rule has been successfully matched. For more detailed instructions on 'chaining' rules, please refer to the Content Rules, Feature Description document. |
| onlyonnoflag | I | <unset> | Range: 1-9<br>Only try to execute this rule if the specified flag is not set. |

**Type 5 (ReplaceBodyRule)**

| Name | Type | Default | Additional Information |
|---|---|---|---|
| replacement | S | <unset> | The replacement string. |
| pattern | S | <unset> | The pattern to be matched. |
| onlyonflag | I | <unset> | Range: 1-9<br>Only try to execute this rule if the specified flag is set.<br>Using the **onlyonflag**, **onlyonnoflag**, and **setonmatch** parameters, it is possible to make rules dependent on each other, that is, only execute a particular rule if another rule has been |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | successfully matched. For more detailed instructions on 'chaining' rules, please refer to the Content Rules, Feature Description document. |
| caseindependent | B | 0 – Disabled | Enable this parameter to ignore the case of the strings when comparing.<br>0 – Disabled<br>1 - Enabled |
| onlyonnoflag | I | <unset> | Range: 1-9<br>Only try to execute this rule if the specified flag is not set. |

### 3.11.4 Add/Delete Real Server Rule

Rules can be added or deleted from Real Servers by using the **addrsrule** and **delrsrule** commands:

```
https://<LoadMasterIPAddress>/access/addrsrule?vs=<IPaddr>&port=<Port>&prot=<tcp/udp>&rs=<RS IPaddr>&rsport=<RS-Port>&rule=<RuleName>
https://<LoadMasterIPAddress>/access/delrsrule?vs=<IPaddr>&port=<Port>&prot=<tcp/udp>&rs=<RS IPaddr>&rsport=<RS-Port>&rule=<RuleName>
```

The **rs** parameter also accepts integers (ID). The ID (Real Server index) can be found in the **<RSIndex>** element when doing a **showvs** command, for example:

```
...
<Rs>
<Status>Up</Status>
<VSIndex>1</VSIndex>
<RsIndex>3</RsIndex>
<Addr>10.154.201.3</Addr>
<Port>80</Port>
<Forward>nat</Forward>
<Weight>1000</Weight>
<Limit>0</Limit>
<Enable>Y</Enable>
<Critical>N</Critical>
</Rs>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

...

### 3.11.5 Add/Delete SubVS Rule

Content rules can be added or deleted from SubVSs by using the **addrsrule** and **delrsrule** commands:

```
https://<LoadMasterIPAddress>/access/addrsrule?vs=<IPaddr>&port=<Port>&prot=<tcp/udp>&rs=!<RsIndexOfSubVS>&rule=<RuleName>
https://<LoadMasterIPAddress>/access/delrsrule?vs=<IPaddr>&port=<Port>&prot=<tcp/udp>&rs=!<RsIndexOfSubVS>&rule=<RuleName>
```

To get the **RsIndex** or **VsIndex**, run the **listvs** command. For further information, refer to the **Virtual Service Control** section.

To add a content rule to a Real Server which is assigned to a SubVS, run the following command:

```
https://<LoadMasterIPAddress>/access/addrsrule?vs=<VSIndexOfSubVS>&rs=<RealServerIPAddress>&rsport=<RealServerPort>&rule=<RuleName>
```

Content rules can be added to a SubVS, by using the **addprerule**, **addresponserule** and **addrequestrule** commands, depending on the type of rule being added:

```
https://<LoadMasterIPAddress>/access/addprerule?vs=<VSIndexOfSubVS>&rule=<RuleName>
https://<LoadMasterIPAddress>/access/addresponserule?vs=<VSIndexOfSubVS>&rule=<RuleName>
https://<LoadMasterIPAddress>/access/addrequestrule?vs=<VSIndexOfSubVS>&rule=<RuleName>
```

Content rules can be deleted from a SubVS, by using the **delprerule**, **delresponserule** and **delrequestrule** commands, depending on the type of rule being deleted:

```
https://<LoadMasterIPAddress>/access/delprerule?vs=<VSIndexOfSubVS>&rule=<RuleName>
https://<LoadMasterIPAddress>/access/delresponserule?vs=<VSIndexOfSubVS>&rule=<RuleName>
https://<LoadMasterIPAddress>/access/delrequestrule?vs=<VSIndexOfSubVS>&rule=<RuleName>
```

> Virtual Services and SubVSs share the same attributes. If you want to apply a content rule to a SubVS, you must know the **RsIndex** (ID) of the SubVS. To find the **RsIndex**, run the **listvs** command and scroll down to find the **RsIndex** parameter you want to edit.

### 3.11.6 Add Virtual Service Rules

Rules can be added to Virtual Services by using the **addprerule**, **addresponserule**, **addrequestrule** and **addresponsebodyrule** commands:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
https://<LoadMasterIPAddress>/access/addprerule?vs=<IPaddr>&port=<Port>&prot=
<tcp/udp>&rule=<RuleName>
https://<LoadMasterIPAddress>/access/addresponserule?vs=<IPaddr>&port=<Port>&
prot=<tcp/udp>&rule=<RuleName>
https://<LoadMasterIPAddress>/access/addrequestrule?vs=<IPaddr>&port=<Port>&p
rot=<tcp/udp>&rule=<RuleName>
https://<LoadMasterIPAddress>/access/addresponsebodyrule?vs=<IPaddr>&port=<Po
rt>&prot=<tcp/udp>&rule=<RuleName>
```

> If Kerberos Constrained Delegation (KCD) is enabled on the Virtual Service, it is not possible to add a response body rule.

### 3.11.7 Delete Virtual Service Rules

Rules can be deleted from Virtual Services by using the **delprerule**, **delresponserule**, **delrequestrule** and **delresponsebodyrule** commands:

```
https://<LoadMasterIPAddress>/access/delprerule?vs=<IPaddr>&port=<Port>&prot=
<tcp/udp>&rule=<RuleName>
https://<LoadMasterIPAddress>/access/delresponserule?vs=<IPaddr>&port=<Port>&
prot=<tcp/udp>&rule=<RuleName>
https://<LoadMasterIPAddress>/access/delrequestrule?vs=<IPaddr>&port=<Port>&p
rot=<tcp/udp>&rule=<RuleName>
https://<LoadMasterIPAddress>/access/delresponsebodyrule?vs=<IPaddr>&port=<Po
rt>&prot=<tcp/udp>&rule=<RuleName>
```

### 3.11.8 Check Parameters

The Service Check Parameters can be obtained by using the following command:

```
https://<LoadMasterIPAddress>/access/showhealth?
```

The output of the **showhealth** command will display the **RetryInterval**, **Timeout** and **RetryCount** values.

The Service Check Parameters can be modified by using **modhealth** command.

| Name | Type | Range | Default | Additional Information | Mandatory |
|---|---|---|---|---|---|
| RetryInterval | I | 9-120 (901) | 9 | Defined in seconds, this is the delay between health checks. This includes clusters and FQDNs.<br>Recommended and default value: **9 seconds**<br>Valid values range from the <mininterval> (9) to the <maxinterval> (901). | N |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | | |
|---|---|---|---|---|---|
| | | | | The <mininterval> is **RetryCount** * **Timeout** + 1, that is, a value of 9 by default.<br><br>The <maxinterval> is 901 [because that is what 60 (maximum Timeout) * 15 (maximum RetryCount) + 1 is].<br><br>You can manually set the **RetryInterval** to up to 120 seconds. The **RetryInterval** value may go above 120 if the **Timeout** and **RetryCount** parameters are configured with high enough values.<br><br>If the **RetryInterval** is above 120 seconds, you must adjust the **Timeout** and **RetryCount** values to modify the **RetryInterval**. | |
| Timeout | I | 4-60 | 4 | Defined in seconds, this is the allowed maximum wait time for a reply to a health check. | N |
| RetryCount | I | 2-15 | 2 | This is the consecutive number of times in which a health check must fail before it is marked down and removed from the load balancing pool. | N |

To configure all three parameters, you must first set the **Timeout** and/or **RetryCount** in one request. Then, set the **RetryInterval** in the second request. For example:

**https://<LoadMasterIPAddress>/access/modhealth?Timeout=<TimeoutValue>&RetryCount=<CountValue>**

**https://<LoadMasterIPAddress>/access/modhealth?RetryInterval=<IntervalValue>**

The Adaptive Check parameters can be obtained by using the following command:

**https://<LoadMasterIPAddress>/access/showadaptive?**

The Adaptive Check parameters can be modified by using the following command:

**https://<LoadMasterIPAddress>/access/modadaptive?AdaptiveURL=<URL>&AdaptivePort=<Port>&<AdaptiveInterval=<Interval>&MinPercent=%Value>**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

## 3.12 Certificates & Security

### 3.12.1 Certificate Management

Certificates can be managed using the following commands.

To list the currently installed certificates and their fingerprints, run the following command:

**https://<LoadMasterIPAddress/access/listcert**

Example output for the **listcert** command is provided below:

```
<Response stat="200" code="ok">
<Success><Data><cert>
<name>ecccert</name>
<type>ECC</type>
<publickey>MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAExIIYNDHXTHHOGxWcQlNjXMwnBlZNvaEp4V4o+0yUBI
Lnf7+hEZjbTKxfAPTiBechmEe6LNapZH6M0HK8lAsG+g==</publickey>
</cert>
<cert>
<name>rsacertificate</name>
<type>RSA</type>
<modulus>EBABCF2255B7E3A784E0122057E75E5902DAD385868A405775BE6641E343E1FED9B484FD3EA0ACA6
C7EBA301EDD4AAC2BA32E1F5646611B95640B0DE311B498A153E5784C742BB4617D0C5D26A37DE893BCF56D7D
6A0E2D0A70BE8FFD2AC048151F698A006AF8AB27A7FFFA4359ABF1553347E762FA6913DAEAE17E8D24A649D99
25041267083A8A422E3EB30E93F25F9AF764E1314FB8A19943B82063F4FB0429D1428098E0F1DB5E1197DC711
59F46BE6D82E79012249377C179DC2D0704EB0CFAD904C048CC6915F457F603DD5E7D9131CEF799E86EB76183
6051AE411B330D3C39087BB9F7ABB0DDF33354AE89B29CD3943C73B99777A3D8D67E36A056A3</modulus>
</cert>
</Data>
</Success>
</Response>
```

To list the currently installed intermediate certificates, run the following command:

**https://<LoadMasterIPAddress/access/listintermediate**

To return an existing certificate as a BLOB, run the following command:

**https://<LoadMasterIPAddress/access/readcert?cert=<CertName>**

To return an existing intermediate certificate as a BLOB, run the following command:

**https://<LoadMasterIPAddress/access/readintermediate?cert=<CertName>**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

By default, for the **readcert** and **reasintermediate** commands, the BLOB is in PEM format. There is an optional parameter called **outform** that can be used to specify the format – either **PEM** or **DER**, for example:

```
https://<LoadMasterIPAddress/access/readcert?cert=<CertName>&outform=<PEM/DER>
```

DER is Base64-encoded because it is a binary format.

To upload a certificate, run the following cURL command:

```
curl -X POST --data-binary "@<Filename>.<Exension>" -k
https://<LoadMasterIPAddress/access/addcert?cert=<CertName>&password=<Passwor
d>&replace=<0/1>
```

> If you are uploading a certificate and key file, insert both the certificate and key in the same file.

| Name | Type | Default | Additional Information | Mandatory |
|---|---|---|---|---|
| cert | S | <unset> | The identifier that the certificate is known as on the LoadMaster. | Y |
| password | S | <unset> | The (optional) passphrase that was used to protect the certificate when it was created. | N |
| replace | B | <unset> | 0 - Not replacing<br>1 - Replacing<br>If you are replacing a certificate which already exists in the LoadMaster, set the **replace** parameter to **1**. If you are uploading a new certificate, set **replace** to **0**. | N |

```
https://<LoadMasterIPAddress>/access/delcert?cert=<CertName>
```

> It is not possible to delete a certificate assigned to a Virtual Service. Remove the certificate from any Virtual Services before deleting.

```
https://<LoadMasterIPAddress>/access/addintermediate?cert=<CertName>
https://<LoadMasterIPAddress>/access/delintermediate?cert=<CertName>
https://<LoadMasterIPAddress>/access/backupcert?password=<Password>
https://<LoadMasterIPAddress>/access/restorecert?password=<Password>&Type=<ty
pe>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

The password (passphrase) must be alpha numeric and is case sensitive. The minimum number of characters is 7 with a maximum of 64.

The **type** parameter has three possible values:

- **full** - All Virtual Service and intermediate certificates
- **third** - Intermediate certificates only
- **vs** - Virtual Service certificates only

> The values for the **type** parameter are case sensitive. Ensure to use lowercase when setting this parameter.

**Replace** is a boolean value which tells the LoadMaster whether to replace an existing certificate with the same name or not.

Parameters relating to Certificates that can be managed using **get** and **set** commands are detailed in the following table:

| Name | Type | Additional Information |
|---|---|---|
| admincert | S | |
| localcert | S | This parameter is only relevant when using HA. |

### 3.12.2 ACME Certificates

The LoadMaster provides an option of two Automated Certificate Management Environment (ACME) providers:

- Let's Encrypt
- DigiCert

At present, you can either select Let's Encrypt or DigiCert. In a future release, you will be able to use both at the same time.

To specify which ACME provider to use, set the **acmetype** parameter. For example:

**/access/set?acmetype=<1/2>**

1 - Let's Encypt

2 - DigiCert


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

The API commands and parameters relating to ACME certificates are mostly the same, apart from a few exceptions that are specific to Let's Encrypt and DigiCert. Refer to the relevant sections below for further details.

> There are a number of legacy Let's Encrypt-specific commands that still work for backwards compatibility such as **registerleaccount**, **addlecert**, **renewlecert**, **dellecert**, **listlecert**, **leaccountinfo**, and **getlecert**. If you try to run these commands when **DigiCert** is selected as the ACME provider, you will get an error.

#### 3.12.2.1 Get an existing Let's Encrypt account

To get an existing Let's Encrypt account registered with other ACME clients such as Certbot, run the **fetchleaccount?password=<password>** command. For example:

**curl -X POST --data-binary "@account.key" -k "https://<Username>:<Password>@<LoadMasterIPAddress>/access/fetchleaccount?password=<password>"**

#### 3.12.2.2 Register a Let's Encrypt Account

To register a Let's Encrypt account to the LoadMaster, run the **registeracmeaccount** command. For example:

**/access/registeracmeaccount**

Users can also register a Let's Encrypt account using an email address as an optional parameter, run the **registeracmeaccount?email=abc@yahoo.com** command. For example:

**/access/registeracmeaccount?email=abc@yahoo.com**

#### 3.12.2.3 DigiCert Certificate Account Parameters

There are two parameters specific to configuring DigiCert account settings:

- **acmekid:** The account **Key ID** used for identification on the DigiCert account.
- **acmehmackey:** The Hash-Based Message Authentication Code (HMAC) key used to authenticate to the DigiCert account.

You can configure each of these parameters using the **set** RESTful API command. For example:

**/access/set?param=acmekid&value=<KeyID>**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.12.2.4 ACME Certificate Commands

The commands below work for both Let's Encrypt and DigiCert configurations.

##### 3.12.2.4.1 ACME Global Parameters

The ACME global parameters can be configured using the **get** or **set** commands.

To set the **Renew Period** for the ACME certificate, run the **set?param=renewperiod&value=<value>** command. For example:

**/access/set?param=renewperiod&value=<value>**

> Valid values for the **Renew Period** field range from 1 to 60 (days).

To get the details of the **Renew Period** for the ACME certificate, run the **get?param=renewperiod** command. For example:

**/access/get?param=renewperiod**

To set the ACME directory URL information, run the **set?param=directoryurl&value=<value>** command. For example:

**/access/set?param=directoryurl&value=<value>**

To get the ACME directory URL information, run the **get?param=directoryurl** command. For example:

**/access/get?param=directoryurl**

##### 3.12.2.4.2 Delete the ACME Configuration Parameters

To delete the ACME configuration parameters (which allows you to configure either the Let's Encrypt or DigiCert configuration from the start), run the **delacmeconfig** command. For example:

**/access/delacmeconfig**

> You can only delete the configuration if there are no ACME certificates.

##### 3.12.2.4.3 Request a New ACME Certificate

To request a new ACME certificate, run the **addacmecert?cert=<cert_identifier>&cn=<FQDN>&vid=<value>** command using **cert**, **cn** and **vid** as mandatory parameters.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

For example:

**/access/addacmecert?cert=<cert_identifier>&cn=<FQDN>&vid=<value>**

Other optional parameters are also available, such as:

san1,san2,..,san10, vid1,vid2,...vid10 which are for SANs and their respective VID, country, state, city, company, organization, email, key_size, and so on.

Below are some examples of commands that contain optional parameters:

**/access/addacmecert?cert=<cert_identifier>&cn=<FQDN>&vid=<value>&ec=no&key_size=4096**

**/access/addacmecert?cert=<cert_identifier>&cn=<FQDN>&vid=<value>&ec=no&key_size=2048**

**/access/addacmecert?cert=<cert_identifier>&cn=<FQDN>&vid=<value>&ec=yes**

**/access/addacmecert?cert=<cert_identifier>&cn=<FQDN>&vid=<value>&san1=<FQDN>&vid1=<value>&san2=<FQDN>&vid2=<value>**

3.12.2.4.4 Renew an ACME Certificate

To renew an ACME certificate, run the **renewacmecert?cert=<cert_identifier>** command. For example:

**/access/renewacmecert?cert=<cert_identifier>**

3.12.2.4.5 Delete an ACME Certificate

To delete an ACME certificate from the LoadMaster, run the **delacmecert?cert=<cert_identifier>** command. For example:

**/access/delacmecert?cert=<cert_identifier>**

3.12.2.4.6 List the ACME Certificates

To list the ACME certificates that are installed on the LoadMaster, run the **listacmecert** command. For example:

**/access/listacmecert**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.12.2.4.7 Get the ACME Account Information

To get the ACME account information from the LoadMaster, run the **acmeaccountinfo** command. For example:

**/access/acmeaccountinfo**

#### 3.12.2.4.8 Get Details about a Specific ACME Certificate

To get the details of a specific ACME certificate from the LoadMaster, run the **getacmecert?cert=<cert_identifier>** command. For example:

**/access/getacmecert?cert=<cert_identifier>**

### 3.12.3 Cipher Sets

Custom cipher sets can be manipulated using the commands below.

> It is not possible to modify or delete system-defined cipher sets.

#### 3.12.3.1 Modify a Custom Cipher Set/Create a New Custom Cipher Set

The **modifycipherset** command can be used to update an existing custom cipher set or create a new custom cipher set.

> If the name of an existing custom cipher set is specified, that cipher set will be updated. If a new name is used, a new cipher set will be created.

For example:

**https://<LoadMasterIPAddress>/access/modifycipherset?name=<CustomCipherSetName>&value=<Cipher(s)>**

Multiple ciphers can be assigned by separating them with a colon (**:**).

#### 3.12.3.2 Retrieve the Details of an Existing Cipher Set

The **getcipherset** command can be used to retrieve the list of ciphers which are in the specified cipher set, for example:

**https://<LoadMasterIPAddress>/access/getcipherset?name=<CipherSetName>**

The valid values for the name parameter are below:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- Default
- Default_NoRc4
- BestPractices
- Intermediate_compatibility
- Backward_compatibility
- WUI
- FIPS
- Legacy
- <NameOfCustomCipherSet>

> The values are case sensitive.

#### 3.12.3.3 Delete a Custom Cipher Set

The **delcipherset** command can be used to delete an existing custom cipher set. For example:

**`https://<LoadMasterIPAddress>/access/delcipherset?name=<CustomCipherSetName>`**

> A custom cipher set cannot be deleted if it is assigned to any Virtual Services. If this command is run when a cipher set is assigned to a Virtual Service, an error message will be returned which says **Command Failed: Cipher set in use**.

### 3.12.4 Remote Access

Parameters relating to Remote Access that can be managed using **get** and **set** commands are detailed in the following table. Refer to the **Using get and set commands** section for details on the **get** and **set** commands.

| Name | Type | Range | Additional Information |
|---|---|---|---|
| admingw | A | | When administering the LoadMaster from a non-default interface, this option allows the user to specify a different default gateway for administrative traffic only. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | To unset this, set the value to an empty string. |
| enableapi | B | no (or 0) – Disabled<br>yes - Enabled | Enables and disables the RESTful API Interface described in this document.<br>To enable the API, you must send a **GET** command along with **param=enableapi&value=yes** – in that order. (The value **1** is not supported and returns an error.) |
| eccerts | I | 0 - RSA self-signed certs<br>1 - EC certs with a RSA signature<br>2 - EC certs with an EC signature | Specify the type of self-signed certificates that the system will use. The options are described below:<br>•**RSA self-signed certs:** By default, these are RSA certificates that are signed with the Kemp RSA root certificate.<br>•**EC certs with a RSA signature:** The LoadMaster can generate an EC certificate also signed by the original RSA Kemp root certificate.<br>• **EC certs with an EC signature:** The LoadMaster can generate an EC certificate signed by the Kemp EC root certificate. In this mode, any CSRs generated will also be EC. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | You should not switch from **RSA self-signed certs** to **EC certs with an EC signature** directly. If you do this, connections will fail because there is no EC Kemp Certificate Authority (CA) certificate. To work around this, you must first switch from **RSA self-signed certs** to **EC certs with a RSA signature**.<br><br>Then, download the new EC Kemp CA certificate by clicking **Download ECC Root Cert** in the bottom-right of the WUI under the main menu after refreshing the page. After you have downloaded the certificate, you can switch to **EC certs with an EC signature** with no loss of connection. |
| outboundcipherset | S | The valid values are below:<br><br>Default<br><br>Default_NoRc4<br><br>BestPractices<br><br>Intermediate_compatibility<br><br>Backward_compatibility<br><br>WUI<br><br>FIPS<br><br>Legacy<br><br>Null_Ciphers<br><br>ECDSA_Default | Specify the cipher set to use on outbound connections (OCSP, email, LDAP, and so on). This is global for all outbound connections. For information on each of the cipher sets available, refer to the SSL Accelerated Services Feature Description.<br><br>Re-encrypt connections are not affected by the outbound cipher set. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | ECDSA_BestPractices<br><NameOfCustomCipherSet><br><EmptyString> - This resets to the default value (**None - Outbound Default**). | |
| adminclientaccess | I | 0 – Password only access (default)<br>1 – Password or client certificate<br>2 – Client certificate required<br>3 – Client certificate required (verify via OCSP) | This parameter is only relevant if Session Management is enabled. |
| allownolocaluserclientcert | B | 0 – Disabled<br>1 – Enabled | Enabling this parameter allows client certificate logins for local users even if the client certificate has been deleted from the LoadMaster. By default, this option is enabled. |
| tethering | B | 0 – Disabled<br>1 – Enabled | Allow the LoadMaster to regularly check the Kemp website for new software versions. |
| geoclients | A | | Set the addresses of the GEO LoadMasters which can retrieve service status information from the LoadMaster.<br>To unset this, set the value to an empty string. |
| geosshport | I | 3-65530 | The port over which GEO LoadMasters will communicate with each other. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| sshaccess | B | | Specify over which addresses remote administrative SSH access to the LoadMaster is allowed. |
| sshiface | S | | Specify the addresses over which remote administrative SSH access to the LoadMaster is allowed. |
| sshport | I | 3-65530 | Specify the port used to access the LoadMaster using the SSH protocol. |
| wuiaccess | B | | Enables or disables WUI access. |
| wuiiface | I | | Specifies the interface for WUI. |
| wuiport | I | | Specifies the port to access the WUI.<br><br>This has a default value of 443. |
| geopartners | A | | Set the IP address of the GEO LoadMaster partner(s). These GEO LoadMasters will keep their DNS configurations in sync.<br><br>To unset this, set the value to an empty string.<br><br>**Note:** Before partnering GEO LoadMasters, a backup should be taken of the relevant GEO LoadMaster that has the correct/preferred configuration. This backup should then be restored to the other LoadMasters that will be partnered with the original LoadMaster. For more |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | information and step-by-step instructions, refer to the GEO, Feature Description. |
| multihomedwui | B | | Allow WUI access from multiple interfaces. Apart from the main administrative interface, each interface can then be enabled to allow WUI access. |
| apiport | I | | Specify the port used to access the API interface. If the port is unset, you can access the API over the web interface port. |
| SSHPreAuth | S | Up to 5,000 characters | Set the SSH pre-authentication banner, which is displayed before the login prompt when logging in using SSH. Space characters should be escaped by entering %20.<br><br>This field accepts up to 5,000 characters. Anything past the 5,000 character limit will not be displayed. |
| geo_ssh_iface | I | | Specify the ID of the GEO interface in which the SSH partner tunnel is created, for example setting this to **0** means the interface **eth0**. This is the interface that the GEO<br><br>partners will communicate through. |

#### 3.12.4.1 Set Admin Access

The web administrative access interface and the administrative default gateway can be set in one step by running the following command with the associated parameters:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
/access/setadminaccess?wuiiface=<WUIInterfaceaddress>&wuiport=<Port>&wuidefaultgateway=<DefaultGatewayAddress>
```

Parameters relating to the **setadminaccess** command are shown in the following table:

| Parameter | Type | Range | Additional Information | Mandatory |
|---|---|---|---|---|
| wuiiface | I | Valid interface index | The index of an existing interface. This index number corresponds to the interface number in the LoadMaster WUI, for example, the index for **eth0** is **0**. | Y |
| wuiport | I | 3-65535 | Specify the port used to access the administrative web interface. | Y |
| wuidefaultgateway | S | Valid IP address | When administering the LoadMaster from a non-default interface, a different default gateway for administrative traffic only can be specified using this parameter. | N |

#### 3.12.4.2 Get GEO Partner Status

To return the status of all configured GEO partners, run the following command:

```
https://<LoadMasterIPAddress>/access/getgeopartnerstatus
```

An empty list is returned if there are no GEO partners configured. If a status for a particular partner is not known, it is reported as “Unknown”.

#### 3.12.4.3 WUI Authentication and Authorization Options

Parameters relating to WUI Authentication and Authorization Options that can be managed using **get** and **set** commands are detailed in **the following table**. Refer to the **Using get and set commands** section for the **get** and **set** commands.

| Name | Type | Range | Description |
|---|---|---|---|
| wuildapep | S | A valid LDAP endpoint name | Specify the name of the LDAP endpoint to use for WUI authentication. |
| ldapbackupserver | A | | Specifies the backup LDAP server for authentication. |
| ldapsecurity | I | 0 = Not Encrypted | Specifies the security mode for LDAP authentication. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | 1 = StartTLS<br>2 = LDAPS | |
| ldapserver | A | | Specifies the LDAP server to use for authentication. |
| ldaprevalidateinterval | B | | Specifies how often to revalidate the authentication to the LDAP server. |
| wuiservercertval | B | 0 - Disabled<br>1 - Enabled | This option is only relevant when the LDAP endpoint has either StartTLS or LDAPS selected as the LDAP Protocol. When the **wuiservercertval** parameter is enabled, it ensures that the host name or IP address that was used to initiate the secure connection resides in the Certificate Subject or Subject Alternative Names (SAN) of the certificate. |
| wuiusergroups | S | | Enter a space-separated list of existing remote user groups to assign, for example **testgroup%20testgroup2**. Set the parameter to an empty value to remove all assigned groups, for example **value=**. |
| wuinestedgroups | B | 0 = Disabled<br>1 = Enabled | Enable or disable nested remote user groups. |
| wuidomain | S | | Specify the domain to use if no domain is provided in the username when group WUI authentication is in use. It is always used as the domain for group search if the Windows logon is used in the format *prefix\username*. |
| radiusbackupport | I | 3-65535 | Specifies the TCP port for the backup RADIUS server. |
| radiusbackupsecret | S | | Specifies the password (secret) to the backup RADIUS server. |
| radiusbackupserver | A | | Specifies the backup RADIUS server to use for authentication. |
| radiusport | I | 3-65535 | Specifies the TCP port for communication to |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | the RADIUS server. |
| radiusrevalidateinterval | I | 10-86400 | Specifies when to revalidate the authentication to the RADIUS server. |
| radiussendnasid | B | 0 - Disabled<br>1 - Enabled | If this parameter is disabled (default), a NAS identifier is not sent to the RADIUS server. If it is enabled, a Network Access Server (NAS) identifier string is sent to the RADIUS server. By default, this is the hostname. Alternatively, if you specify a value in the **radiusnasid** parameter, this value is used as the NAS identifier. If the NAS identifier cannot be added, the RADIUS access request is still processed. |
| radiusnasid | S | | If the **radius_send_nas_id** parameter is enabled, the **radius_nas_id** parameter is relevant. When specified, this value is used as the NAS identifier. Otherwise, the hostname is used as the NAS identifier. If the NAS identifier cannot be added, the RADIUS access request is still processed.<br><br>This parameter is only relevant if the **radiussendnasid** parameter is enabled. |
| radiussendvendorspec | b | 0 - Disabled<br>1 - Enabled | If this parameter is disabled (default), an Attribute Value Pair (AVP) is not send to the RADIUS server. If it is enabled, an Attribute Value Pair in the RADIUS request sent to the server doing the authentication against the user trying to log in to the LoadMaster WUI. |
| radiussecret | S | | Specifies the password (secret) to the RADIUS server. |
| radiusserver | A | | Specifies the RADIUS server to use for authentication.<br><br>IPv6 is not supported for RADIUS authentication. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| sessionlocalauth | B | | Enables or disables local authentication. |
| sessionauthmode | I | Refer to the table below. | Specifies the authentication mode for the load balancer. |

The following table describes the Radius, LDAP and Local user options that are selected depending on the value given to the **sessionauthmode** parameter

| | Radius | | LDAP | Local | |
|---|---|---|---|---|---|
| **Value** | **Authent.** | **Author.** | **Authent.** | **Authent.** | **Author.** |
| 7 | No | No | No | No | No |
| 263 | Yes | No | No | Yes | Yes |
| 775 | Yes | Yes | No | Yes | Yes |
| 23 | No | No | Yes | Yes | Yes |
| 22 | No | No | Yes | No | Yes |
| 788 | Yes | Yes | Yes | No | No |
| 790 | Yes | Yes | Yes | No | Yes |
| 791 | Yes | Yes | Yes | Yes | Yes |
| 789 | Yes | Yes | Yes | Yes | No |
| 773 | Yes | Yes | No | Yes | No |
| 262 | Yes | No | No | No | Yes |
| 774 | Yes | Yes | No | No | Yes |
| 772 | Yes | Yes | No | No | No |
| 278 | Yes | No | Yes | No | No |
| 279 | Yes | No | Yes | Yes | Yes |

### 3.12.5 Admin WUI Access

Parameters relating to Admin WUI Access that can be managed using **get** and **set** commands are detailed in the following table. Refer to the **Using get and set commands** section for details on the


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

**get** and **set** commands.

| Name | Type | Range | Description |
|---|---|---|---|
| wuicipherset | S | The valid values are below:<br>Default<br>Default_NoRc4<br>BestPractices<br>Intermediate_compatibility<br>Backward_compatibility<br>WUI<br>FIPS<br>Legacy<br>Null_Ciphers<br>ECDSA_Default<br>ECDSA_BestPractices<br><NameOfCustomCipherSet> | Specify the cipher set to use for the LoadMaster WUI. |
| WUITLS13Ciphersets | S | All TLS1.3 available cipher sets | Specify which TLS1.3 cipher sets to use for WUI access. Multiple ciphers can be specified using a space or comma separated list. Also, setting this parameter value to an empty string will select the default value (that is, a combination of ciphers **TLS_AES_256_GCM_SHA384**, **TLS_CHACHA20_POLY1305_SHA256**, and **TLS_AES_128_GCM_SHA256**).<br>The list of supported TLS1.3 Ciphers is as follows:<br>- TLS_AES_256_GCM_SHA384 |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | - TLS_CHACHA20_POLY1305_SHA256<br>- TLS_AES_128_GCM_SHA256<br>- TLS_AES_128_CCM_8_SHA256<br>- TLS_AES_128_CCM_SHA256 |
| WUICACertList | S | | When assigning multiple certificates for WUI authentication, the certificates must be specified in a single space-separated list. |
| sessioncontrol | B | | Enables or disables session control. |
| sessionbasicauth | B | 0 – Disabled<br>1 – Enabled | If the **sessioncontrol** and **sessionbasicauth** parameters are both enabled, there are two levels of authentication enforced to access the LoadMaster WUI. The initial level is Basic Authentication where users log in using the bal or user logins, which are default usernames defined by the system. |
| sessionidletime | I | 60-86400 | Specifies the number of seconds that the WUI can be idle before logging the user out. This can be set from 60 to 86400 seconds. |
| sessionmaxfailattempts | I | 1-999 | Number of failed attempts before locking the user account. |
| sessionconcurrent | S | 0-9 | Limit the maximum number of concurrent logins that a single user can have to the LoadMaster WUI (a value of 0 means there is no limit). |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| WUIPreAuth | S | Up to 5,000 characters | Set the pre-authentication click through banner which will be displayed before the LoadMaster login page. This parameter can contain plain text or HTML code. The field cannot contain JavaScript. Space characters should be replaced with %20.<br><br>This field accepts up to 5,000 characters. Anything past the 5,000 character limit will not be displayed. |
| WUITLSProtocols | I | 0 – 30 bitmask | Specify whether or not it is possible to connect to the LoadMaster WUI using the following protocols; SSLv3, TLS1.0, TLS1.1, TLS1.2, or TLS1.3. The protocols can be enabled and disabled using a bitmask value. Refer to the following table to find out which number corresponds to which settings. |

| Number | SSLv3 | TLS1.0 | TLS1.1 | TLS1.2 | TLS1.3 |
|---|---|---|---|---|---|
| 0 | Enabled | Enabled | Enabled | Enabled | Enabled |
| 1 | Disabled | Enabled | Enabled | Enabled | Enabled |
| 2 | Enabled | Disabled | Enabled | Enabled | Enabled |
| 3 | Disabled | Disabled | Enabled | Enabled | Enabled |
| 4 | Enabled | Enabled | Disabled | Enabled | Enabled |
| 5 | Disabled | Enabled | Disabled | Enabled | Enabled |
| 6 | Enabled | Disabled | Disabled | Enabled | Enabled |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | | |
|---|---|---|---|---|---|
| 7 | Disabled | Disabled | Disabled | Enabled | Enabled |
| 8 | Enabled | Enabled | Enabled | Disabled | Enabled |
| 9 | Disabled | Enabled | Enabled | Disabled | Enabled |
| 10 | Enabled | Disabled | Enabled | Disabled | Enabled |
| 11 | Disabled | Disabled | Enabled | Disabled | Enabled |
| 12 | Enabled | Enabled | Disabled | Disabled | Enabled |
| 13 | Disabled | Enabled | Disabled | Disabled | Enabled |
| 14 | Enabled | Disabled | Disabled | Disabled | Enabled |
| 15 | Disabled | Disabled | Disabled | Disabled | Enabled |
| 16 | Enabled | Enabled | Enabled | Enabled | Disabled |
| 17 | Disabled | Enabled | Enabled | Enabled | Disabled |
| 18 | Enabled | Disabled | Enabled | Enabled | Disabled |
| 19 | Disabled | Disabled | Enabled | Enabled | Disabled |
| 20 | Enabled | Enabled | Disabled | Enabled | Disabled |
| 21 | Disabled | Enabled | Disabled | Enabled | Disabled |
| 22 | Enabled | Disabled | Disabled | Enabled | Disabled |
| 23 | Disabled | Disabled | Disabled | Enabled | Disabled |
| 24 | Enabled | Enabled | Enabled | Disabled | Disabled |
| 25 | Disabled | Enabled | Enabled | Disabled | Disabled |
| 26 | Enabled | Disabled | Enabled | Disabled | Disabled |
| 27 | Disabled | Disabled | Enabled | Disabled | Disabled |
| 28 | Enabled | Enabled | Disabled | Disabled | Disabled |
| 29 | Disabled | Enabled | Disabled | Disabled | Disabled |
| 30 | Enabled | Disabled | Disabled | Disabled | Disabled |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

### 3.12.6 OCSP Configuration

Parameters relating to the Online Certificate Status Protocol (OCSP) configuration that can be managed using **get** and **set** commands are detailed in the table below. Refer to the **Using get and set commands** section for details on the **get** and **set** commands.

| Name | Type | Additional Information |
|---|---|---|
| OCSPPort | I | The port of the OCSP server. |
| OCSPUseSSL | B | Use SSL to connect to the OCSP server. |
| OCSPOnServerFail | B | Treat an OCSP server connection failure or timeout as if the OCSP server had returned a valid response, that is, treat the client certificate as valid. |
| OCSPServer | A | The address of the OCSP server. This can either be in IP address or Fully Qualified Domain Name (FQDN) format. |
| OCSPUrl | S | The URL to access on the OCSP server. |
| OCSPcertChecking | B | Enabling the **OCSPcertChecking** parameter enables the LoadMaster to perform OCSP checks on certain outbound connections. This is disabled by default. |
| SSLStapling | B | Enable this parameter to enable the LoadMaster to respond to OCSP stapling requests. If a client connects using SSL and asks for an OCSP response, this is returned. Only Virtual Service certificates are validated. The system holds a cache of OCSP responses that are sent back to the client. This cache is maintained by the OCSP daemon. When the OCSP daemon sends a request to the server, it uses the name specified in the certificate (in the **Authority Information Access** field). If it cannot resolve this name, then it uses the default OCSP server specified in the **OCSPServer** parameter. |
| SSLRefreshInterval | I | Specify how often the LoadMaster should refresh the OCSP stapling information. The OCSP daemon caches the entry for up to the amount of time specified here, after which it is refreshed.<br><br>Valid values range from 3600 (1 hour (default)) to 86400 seconds (24 hours). |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

### 3.12.7 LDAP Configuration

Refer to the sections below for details about the different RESTful API commands relating to LDAP endpoint configuration.

#### 3.12.7.1 Add an LDAP Endpoint

Add a new LDAP endpoint by running the following command:

**https://<LoadMasterIPAddress>/access/addldapendpoint?name=<LDAPEndpointName>**

> The name cannot contain any spaces or special characters, for example:
> !@#$%^^&*()+={}[]|\:;"'<>?/

You can also specify the following optional parameters when running the **addldapendpoint** command. If you do not specify these parameters – default values are used.

| Name | Type | Description | Additional Information |
|---|---|---|---|
| ldaptype | I | Specify the transport protocol to use when communicating with the LDAP server. | 0 – Unencrypted (default)<br>1 – StartTLS<br>2 – LDAPS |
| server | S | Specify the address, or addresses, of the LDAP server to be used. | You can also specify a port number, if desired. Separate multiple addresses with a space. |
| vinterval | I | Specify how often to revalidate the user the with the LDAP server. | Range:<br>10 – 86400 seconds<br>Default: 60 |
| referralcount | I | The LoadMaster offers beta functionality to support LDAP referral replies from Active Directory Domain Controllers. If this is set to **0**, referral support is not enabled. Set this field to a value between **1** and **10** to enable referral chasing. The | Multiple hops may increase authentication latency. There is a performance impact that depends on the number and depth of referrals required in your configuration.<br>You must have intimate knowledge of your Active Directory structure to set the referral limit appropriately. The same credentials are used for all lookups, and so on. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | number specified will limit the number of hops (referrals chased). | The use of Active Directory Global Catalog (GC) is the preferred configuration as the primary means of resolution instead of enabling LDAP referral chasing. A GC query can be used to query the GC cache instead of relying on LDAP and the referral process. Using Active Directory GC has little or no performance drag on the LoadMaster. For steps on how to add/remove the GC, refer to the following TechNet article: https://technet.microsoft.com/en-us/library/cc755257(v=ws.11).aspx |
| timeout | I | Specify the LDAP server timeout in seconds. | The default value is **5**. Valid values range from **5** to **60**. |
| adminuser | S | Specify the username of an administrator user. | The username that is used to check the LDAP server. |
| adminpass | S | Specify the password for the specified administrator user. | The password that is used to check the LDAP server. |

#### 3.12.7.2 Modify an LDAP Endpoint

Modify an existing LDAP endpoint by running the following command:

**`https://<LoadMasterIPAddress>/access/modifyldapendpoint?name=<LDAPEndpointName>`**

You can also specify the following optional parameters when running the **modifyldapendpoint** command.

| Name | Type | Description | Additional Information |
|---|---|---|---|
| ldaptype | I | Specify the transport protocol to use when communicating with the LDAP server. | 0 – Unencrypted (default)<br>1 – StartTLS<br>2 – LDAPS |
| server | S | Specify the address, or addresses, of the LDAP server to be used. | You can also specify a port number, if necessary. Separate multiple addresses with a space. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| vinterval | I | Specify how often to revalidate the user with the LDAP server. | Range:<br>10 – 86400 seconds<br>Default: 60 |
| referralcount | I | The LoadMaster offers beta functionality to support LDAP referral replies from Active Directory Domain Controllers. If this is set to **0**, referral support is not enabled. Set this field to a value between **1** and **10** to enable referral chasing. The number specified will limit the number of hops (referrals chased). | Multiple hops may increase authentication latency. There is a performance impact that depends on the number and depth of referrals required in your configuration.<br>You must have intimate knowledge of your Active Directory structure to set the referral limit appropriately. The same credentials are used for all lookups, and so on.<br>The use of Active Directory Global Catalog (GC) is the preferred configuration as the primary means of resolution instead of enabling LDAP referral chasing. A GC query can be used to query the GC cache instead of relying on LDAP and the referral process. Using Active Directory GC has little or no performance drag on the LoadMaster. |
| timeout | I | Specify the LDAP server timeout in seconds. | The default value is **5**. Valid values range from **5** to **60**. |
| adminuser | S | Specify the username of an administrator user. | The username that is used to check the LDAP server. |
| adminpass | S | Specify the password for the specified administrator user. | The password that is used to check the LDAP server. |

#### 3.12.7.3 Delete an LDAP Endpoint

Delete an existing LDAP endpoint by running the following command:

**https://<LoadMasterIPAddress>/access/deleteldapendpoint?name=<LDAPEndpointName>**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> It is not possible to delete an LDAP endpoint that is currently in use.

#### 3.12.7.4 Retrieve Details of All LDAP Endpoints

To retrieve the details of all existing LDAP endpoints, run the following command:

**https://<LoadMasterIPAddress>/access/showldaplist**

#### 3.12.7.5 Retrieve Details of a Specific LDAP Endpoint

To retrieve the details of a specific LDAP endpoint, run the following command:

**https://<LoadMasterIPAddress>/access/showldapendpoint?name=<LDAPEndpointName>**

### 3.12.8 Intrusion Detection Options (IPS/IDS)

The Intrusion Detection Rules can be updated using the following command:

**https://<LoadMasterIPAddress>/access/updatedetect**

There are a number of methods of using this command for example, using a CURL command on Linux would look like the following:

```
curl –X POST --data-binary “@<Detection Rules File>” –k
https://<LoadMasterIPAddress>/access/updatedetect
```

The above example would install new detection rules (<Detection Rules File>) on the system.

Related parameters that can be managed using **get** and **set** commands are detailed in the following table. Refer to the **Using get and set commands** section for the **get** and **set** commands.

| Name | Type | Range | Description |
|---|---|---|---|
| paranoia | I | 0 = Low<br>1 = Default<br>2 = High<br>3 = Paranoid | Sets the sensitivity of the Intrusion Detection System (IDS) detection. |

## 3.13 Interfaces

### 3.13.1 Get Interface Details

Obtain interface details by using the following command:

**https://<LoadMasterIPAddress>/access/showiface?interface=<InterfaceID>**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

To view the interface ID for each of the interfaces, run the **stats** command. The interface IDs are displayed as the **ifaceID** in the XML output. For further information on the **stats** command, refer to the **Statistics** section.

Running the **showiface** command without using the **interface** parameter displays details for all existing interfaces.

### 3.13.2 Modify Interface Details

Interface parameters can be changed using the following command:

```
https://<LoadMasterIPAddress>/access/modiface?interface=<InterfaceID>&<parameter>=<value>
```

> Only one parameter can be changed on each call. The parameters are checked in the order below.

| Name | Type | Description | Additional Information |
|---|---|---|---|
| interface | I | The number of the interface to modify | To view the interface ID for each of the interfaces, run the **stats** command. The interface IDs are displayed as the **ifaceID** in the XML output. For further information on the **stats** command, refer to the **Statistics** section. |
| addr | S | IP address | Specify the internet address of this interface. |
| mtu | I | MTU size<br>Range: 512-9216 | Change the maximum size of the Ethernet frame that will be sent from this interface. |
| hacheck | B | 0 – Not used for HA/cluster checks<br>1 – Used for HA/cluster checks | This parameter is only relevant in a HA/cluster configuration. Specify whether or not to use this interface for HA/cluster checks.<br>The default interface used for checking is eth0. When this option is enabled for an interface, you are prevented from disabling it on that interface. To switch to another interface, specify hacheck=yes/1 for a different interface. You cannot disable this parameter by specifying hacheck=no/0. |
| clupdate | B | Use this interface for cluster | There must be exactly one interface that is configured for cluster updates. The default interface used for updates is eth0. When this option is enabled for an interface, you are prevented from |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | synchronization operations. | disabling it on that interface. To switch to another interface, specify clupdate=yes/1 for a different interface. You cannot disable this parameter by specifying clupdate=no/0. |
| gwiface | B | Use this interface as the default gateway<br><br>0 - Disabled<br><br>1 - Enabled | Specifies if this is a network gateway interface.<br><br>If enabling this option, you must then run the following command:<br><br>**https://<LoadMasterIPAddress>/access/set?param=dfltgw&value=<NewIPAddress>** |
| bondmode | I | 1 = active-backup<br><br>4 = 802.3ad | The bondmode determines the way in which traffic sent out of the bonded interface is actually dispersed over the real interfaces. |
| partner | A | IP address of the partner machine (HA only) | This parameter is only relevant for LoadMasters in HA mode |
| shared | A | IP address of the shared address (HA only) | This parameter is only relevant for LoadMasters in HA mode |
| adminwuienable | B | This option can only be set to yes (1) if the **multihomedwui** parameter is set to yes. | When both of the **adminwuienable** and **multihomedwui** parameters are enabled, the WUI can be accessed from the IP address of the relevant interface, and any Additional addresses set up for that interface.<br><br>Refer to the **Remote Access** section for further information on the **multihomedwui** parameter. |
| geotraffic | B | 0 – Do not use for GEO requests | Specify whether or not to use this interface for GEO responses and requests. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | |
|---|---|
| | and responses |
| | 1 – Use for GEO requests and responses |

### 3.13.3 Additional Addresses

Additional Addresses can be added to an interface by using the command

**https://<LoadMasterIPAddress>/access/addadditional?interface=<InterfaceID>&addr=<AdditionalAdressIP/prefix>**

Additional Addresses can be deleted from an interface by using the command

**https://<LoadMasterIPAddress>/access/deladditional?interface=<InterfaceID>&addr=<AdditionalAdressIP/prefix>**

### 3.13.4 Bonded Interfaces

A bonded interface can be created by using the following command:

**https://<LoadMasterIPAddress>/access/createbond?interface=<InterfaceID>**

An interface can be added to a bonded interface by using the following command:

**https://<LoadMasterIPAddress>/access/addbond?interface=<InterfaceID>&bond=<BondID>**

An interface can be removed from a bonded interface by using the following command:

**https://<LoadMasterIPAddress>/access/delbond?interface=<InterfaceID>&bond=<BondID>**

A bond can be converted back to a port by using the following command:

**https://<LoadMasterIPAddress>/access/unbond?interface=<InterfaceID>**

To view the interface ID for each of the interfaces, run the **stats** command. The interface IDs are displayed as the **ifaceID** in the XML output. For further information on the **stats** command, refer to the **Statistics** section.

The BondID is the number of the bond in the **Interfaces** section of the main menu in the WUI. For example, **bnd2** will have a BondID of **2**.

### 3.13.5 VLANs

A new VLAN can be added to an interface using the following command:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

**https://<LoadMasterIPAddress>/access/addvlan?interface=<InterfaceID>&vlanid=<ID>**

A VLAN can be removed from an interface using the following command:

**https://<LoadMasterIPAddress>/access/delvlan?interface=<InterfaceID>&vlanid=<ID>**

### 3.13.6 VXLANs

A VXLAN can be added by running one of the following commands:

**https://<LoadMasterIPAddress>/access/addvxlan?interface=<InterfaceID>&vni=<VXLANNetworkIdentifier>&group=<GroupMulticastIP>**
**https://<LoadMasterIPAddress>/access/addvxlan?interface=<InterfaceID>&vni=<VXLANNetworkIdentifier>&remote=<RemoteVTEPIPAddress>**

A VXLAN can be deleted by running the following command:

**https://<LoadMasterIPAddress>/access/delvxlan?interface=<InterfaceID>**

To modify VXLAN details (for example set the IP address) please use the **modiface** command. For more information, refer to the **Running the showiface command without using the interface parameter displays details for all existing interfaces.Modify Interface Details** section.

To retrieve VXLAN details, use the **showiface** command. For more information, refer to the **Get Interface Details** section.

## 3.14 Host & DNS Configuration

Some parameters relating to Host & DNS Configuration can be managed using the **get** and **set** commands, for example:

**https://<LoadMasterIPAddress>/access/get?param=hostname**

| Name | Type | Additional Information |
|---|---|---|
| Hostname | S | Set the hostname of the local machine. |
| ha1hostname | S | Set the hostname for the active LoadMaster |
| ha2hostname | S | Set the hostname for the standby LoadMaster |
| namserver | A | The IP address of a DNS server which is to be used to resolve names locally on the LoadMaster. Setting this parameter to an empty string will delete the name servers. The last remaining name server cannot be deleted if the **dnssecclient** parameter is enabled.<br><br>This parameter has been deprecated and replaced with the nameserver parameter. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| nameserver | A | The IP address of a DNS server which is to be used to resolve names locally on the LoadMaster. Setting this parameter to an empty string will delete the name servers. The last remaining name server cannot be deleted if the **dnssecclient** parameter is enabled. |
| searchlist | S | Specify the domain name that is to be prepended to requests to the DNS name server. |
| dnssecclient | B | Enable or disable DNSSEC client capabilities on the LoadMaster. At least one name server must be configured before DNSSEC can be enabled. After changing this setting, the LoadMaster must be rebooted for the change to be applied. Once the setting is changed, it cannot be changed again until the LoadMaster has been rebooted. If using HA, please set the parameter on both devices separately.<br>0 - Disabled<br>1 – Enabled |
| DNSNamesEnable | B | When this option is enabled, the LoadMaster automatically attempts to update any changedDNS names (based on the update interval)::<br>• If the address is not found, or if it is the same as before – nothing is done (except a log entry is generated).<br>• If the address is different, the Real Server entry will be updated with the new address, if possible.<br>• If the new address is invalid for some reason, for example if it is a non-local address and the nonlocalrs option has been disabled, no changes are made and a log is generated. |
| dnsupdateinterval | I | Set the update interval for DNS entries. Valid values range from 1 to 60 (minutes). The default value is 60. |
| dnsreloadonerror | B | If this parameter is enabled, DNS entries are reloaded when health checks have errors and an FQDN is associated with the Real Server IP address. |

### 3.14.1 Resolve DNS Names Now

To force a new resolution of DNS names, run the **resolvenow** command, for example:

**`https://<LoadMasterIPAddress>/access/resolvenow`**

The LoadMaster will try to resolve the DNS names:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- If the address is not found or if it is the same as before – nothing is done (except a log entry is generated).
- If the address is different, the Real Server entry will be updated with the new address, if possible.
- If the new address is invalid for some reason, for example if it is a non-local address and the **nonlocalrs** parameter has been disabled, no changes are made and a log is generated. The log is found in the normal syslog messages. The message "DNS update failed" appears and includes the reason why. It is a descriptive error message based on what is incorrect.

### 3.14.2 Hosts for Local Resolution

To list the existing hosts for local resolution, run the **gethosts** command, for example:

**https://<LoadMasterIPAddress>/access/gethosts**

To add a host IP address and host FQDN, run the **addhostsentry** command, using the following format:

**https://<LoadMasterIPAddress>/access/addhostsentry?hostip=<HostIPAddress>&hostfqdn=<HostFQDN>**

To delete a host IP address and host FQDN, run the **delhostsentry** command, using the following format:

**https://<LoadMasterIPAddress>/access/delhostsentry?hostip=<HostIPAddress>**

## 3.15 Route Management

### 3.15.1 Default Gateway

Parameters relating to Route Management that can be managed using **get** and **set** commands, for example:

**https://<LoadMasterIPAddress>/access/get?param=dfltgw**

Before setting the default gateway, the network interface addresses must be configured, for example:

**https://<LoadMasterIPAddress>/access/modiface?interface=<ifaceID>&gwiface=1**

| Name | Type | Default | Additional Information |
|---|---|---|---|
| dfltgw | A (IPv4) | <unset> | Specify the IPv4 default gateway that is to be used for communicating with the internet. |
| dfltgwv6 | A | <unset> | Specify the IPv6 default gateway that is to be used for |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | |
|---|---|
| (IPv6) | communicating with the internet. |

### 3.15.2 Additional Routes

Existing Additional Routes can be listed by running the following command:

**https://<LoadMasterIPAddress>/access/showroute**

Additional Routes can be added or deleted with the following commands:

**https://<LoadMasterIPAddress>/access/addroute?dest=<DestIPAddress>&gateway=<GatewayIPAddress>**
**https://<LoadMasterIPAddress>/access/delroute?dest=<DestIPAddress>**

### 3.15.3 Packet Routing Filter

The commands in this section relate to the global packet routing filter option. Packet filtering is enabled by default. It is not possible to disable the packet routing filter if GEO is enabled. Refer to the **Enable/Disable GEO** section for commands on enabling and disabling GEO.

To check if the packet routing filter is enabled or not, run the following command:

**https://<LoadMasterIPAddress>/access/aclcontrol?isenabled**

To enable/disable the packet routing filter, run the following command:

**https://<LoadMasterIPAddress>/access/aclcontrol?enable=<0/1>**

> It is not possible to disable the packet routing filter if GEO is enabled. If you try to disable the packet routing filter with GEO enabled, you get the following error:
> **Cannot disable aclcontrol while GSLB is enabled**

The following parameters can only be set if the packet filter is enabled.

Check if the connection is dropped or rejected when it is on the block list:

**https://<LoadMasterIPAddress>/access/aclcontrol?isdrop**

Enable dropping of block list entries:

**https://<LoadMasterIPAddress>/access/aclcontrol?drop=1**

Disable dropping of block list entries:

**https://<LoadMasterIPAddress>/access/aclcontrol?drop=0**

When the **Restrict traffic to Interfaces** option is enabled, restrictions are enforced upon routing between attached subnets. To check if the **Restrict traffic to Interfaces** option is enabled or disabled, run the following command:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

**https://<LoadMasterIPAddress>/access/aclcontrol?isifblock**

- **Block** - enabled
- **Free** - disabled

To enable the **Restrict traffic to Interfaces** option:

**https://<LoadMasterIPAddress>/access/aclcontrol?ifblock=1**

To disable the **Restrict traffic to Interfaces** option:

**https://<LoadMasterIPAddress>/access/aclcontrol?ifblock=0**

If the **Include WUI in IP Access Lists** option is enabled, access to the WUI is also controlled by the packet filter. In this case, the client that enabled the **Include WUI in IP Access Lists** option will still have access. If this option is disabled, access to the WUI is not affected by the packet filter.

To check if **Include WUI in IP Access Lists** is enabled or disabled, run the following command:

**https://<LoadMasterIPAddress>/access/aclcontrol?iswuiblock**

To enable the **Include WUI in IP Access Lists** option, run the following command:

**https://<LoadMasterIPAddress>/access/aclcontrol?wuiblock=1**

To disable the **Include WUI in IP Access Lists** option, run the following command:

**https://<LoadMasterIPAddress>/access/aclcontrol?wuiblock=0**

To check the IP address of the last client that changed the packet filter (that is, the host that is allowed in), run the following command:

**https://<LoadMasterIPAddress>/access/aclcontrol?wuiaddr**

> The **wuiaddr** command is only relevant if the **Include WUI in IP Access Lists** option is enabled.

### 3.15.4 VPN Management

#### 3.15.4.1 Create a New VPN Connection

To create a new Virtual Private Network (VPN) connection, run the following command:

**https://<LoadMasterIPAddress>/access/createvpncon?name=<VPNname>**

#### 3.15.4.2 Delete an Existing IPsec Connection

An existing IPsec connection can be deleted by running the following command:

**https://<LoadMasterIPAddress>/access/deletevpncon?name=<VPNname>**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.15.4.3 Set the VPN Addresses

The VPN addresses can all be set at the same time by running the following command:

```
https://<LoadMasterIPAddress>/access/setvpnaddr?name=<VPNname>&localip=<
LocalIPAddress>&localsubnets=<LocalSubnetAddress
(es)>&remoteip=<RemoteIPAddress>&remotesubnets=<RemoteSubnetAddress(es)>
```

All of the parameters listed below are required when running the **setvpnaddr** command:

| Name | Type | Default | Additional Information |
|---|---|---|---|
| localip | String | See additional information | In non-HA mode, the default is the LoadMaster IP address, that is, the IP address of the default gateway interface.<br><br>In HA-mode, the default is the shared IP address. |
| localsubnets | String | See additional information | Set the subnet for the local side of the connection. The local IP can be the only participant if applicable, given the /32 CIDR. When the **localip** is set, the **localsubnet** is automatically populated. Multiple local subnets can be specified using a comma-separated list. Up to 10 IP addresses can be specified. |
| remoteip | String | <unset> | Set the IP address for the remote side of the connection. |
| remotesubnets | String | <unset> | Set the subnet for the remote side of the connection. Multiple remote subnets can be specified using a comma-separated list. Up to 10 IP addresses can be specified. |

These parameters can also be set individually by running the commands listed below.

To set the **Local IP Address**, run the command below:

```
https://<LoadMasterIPAddress>/access/setvpnlocalip?name=<VPNname>&localip=<Lo
calIPAddress>
```

To set the **Local Subnet Address**, run the command below:

```
https://<LoadMasterIPAddress>/access/setvpnlocalsubnet
s?name=<VPNname>&localsubnets=<LocalSubnetAddress(es)>
```

To set the **Remote IP Address**, run the command below:

```
https://<LoadMasterIPAddress>/access/setvpnremoteip?name=<VPNname>&remoteip=<
RemoteIPAddress>
```

To set the **Remote Subnet Address**, run the command below:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

**https://<LoadMasterIPAddress>/access/setvpnremotesubnets?name=<VPNname>&remotesubnets=<RemoteSubnetAddress(es)>**

#### 3.15.4.4 Set the Perfect Forward Secrecy Option

To enable the **Perfect Forward Secrecy** option on a particular connection, run the command below:

**https://<LoadMasterIPAddress>/access/setvpnpfsenable?name=<ConnectionName>**

To disable the **Perfect Forward Secrecy** option on a particular connection, run the command below:

**https://<LoadMasterIPAddress>/access/setvpnpfsdisable?name=<ConnectionName>**

#### 3.15.4.5 Set the Connection Secret

To set the connection secret details, run the command below:

**https://<LoadMasterIPAddress>/access/setvpnsecret?name=<VPNname>&localid=<LocalID>&remoteid=<RemoteID>&key=<PreSharedKey>**

All of the parameters are required for this command to work.

| Name | Type | Default | Additional Information |
|---|---|---|---|
| localid | String | Same as the **localip** | Identification for the local side of the connection |
| remoteid | String | <unset> | Identification for the remote side of the connection. This can be the **remoteip**. |
| key | String | <unset> | The Pre Shared Key (PSK) string. This is the **Shared key** which is generated and managed on the Azure side. The key length should be at least 16 and at most 64 characters. |

#### 3.15.4.6 Start the Connection

To start the connection, run the command below:

**https://<LoadMasterIPAddress>/access/startvpncon?name=<VPNname>**

#### 3.15.4.7 Stop the Connection

To stop the connection, run the command below:

**https://<LoadMasterIPAddress>/access/stopvpncon?name=<VPNname>**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.15.4.8 Get the Connection Status

To view the status of the connection, run the command below:

**https://<LoadMasterIPAddress>/access/getvpnstatus?name=<VPNname>**

#### 3.15.4.9 List All Existing Connections

To list the details about all of the existing VPN connections, run the command below:

**https://<LoadMasterIPAddress>/access/listvpns**

#### 3.15.4.10 Stop the IKE Daemon

To stop the Internet Key Exchange (IKE) daemon, run the command below:

**https://<LoadMasterIPAddress>/access/stopikedaemon**

#### 3.15.4.11 Start the IKE Daemon

To start the IKE daemon, run the command below:

**https://<LoadMasterIPAddress>/access/startikedaemon**

#### 3.15.4.12 Get the IKE Daemon Status

To view the status of the IKE daemon, run the command below:

**https://<LoadMasterIPAddress>/access/statusikedaemon**

## 3.16 Access Lists

The Access Control List (ACL) commands allow you to switch on or off the ACL and set or get the related parameters. When running an ACL command without a specified Virtual Service IP address, the command is run for the global ACL. If a Virtual Service IP address is set, the command is only run for the ACL for that specific Virtual Service.

Only users with 'All Permissions' can run the global commands.

Users with 'All Permissions' and 'Virtual Service' permissions can run the Virtual Service-specific commands.

Show the addresses on the global block or allow list:

**https://<LoadMasterIPAddress>/access/aclcontrol?list=<ListType>**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| List Type |
| --- |
| block |
| allow |

Add/remove an address to/from the global block or allow list:

```
https://<LoadMasterIPAddress>/access/aclcontrol?add=<ListType>&addr=<IPAddress/CIDR>
https://<LoadMasterIPAddress>/access/aclcontrol?del=<ListType>&addr=<IPAddress/CIDR>
```

> The **addr** can be an IPv4 or an IPv6 address. If the CIDR is not specified, the system uses a default of /32.

For the three commands below, you can either use the socket information (the IP address, port, and protocol of the Virtual Service) or the Virtual Service index to specify the Virtual Service to run the command on.

To retrieve the Virtual Service index, run the **listvs** command, for example:

```
https://<LoadMasterIPAddress>/access/listvs
```

List the block or allow list for a specific Virtual Service:

```
https://<LoadMasterIPAddress>/access/aclcontrol?listvs=<ListType>&vsip=<VirtualServerIPAddress>&vsprot=<VirtualServerProtocol>&vsport=<VirtualServerPort>
```

| Virtual Server Protocol |
| --- |
| tcp |
| udp |

> If the CIDR is not specified, the system will use its own default value which is /32.

You can also use the Virtual Service index to specify the Virtual Service, for example:

```
https://<LoadMasterIPAddress>/access/aclcontrol?listvs=<ListType>&vs=<VirtualServiceIndex>
```

Add/remove an address to/from a Virtual Service block or allow list:

```
https://<LoadMasterIPAddress>/access/aclcontrol?addvs=<ListType>&vsip=<VirtualServerIPAddress>&vsprot=<VirtualServerProtocol>&vsport=<VirtualServerPort>&addr=<IPAddressToAdd/CIDR>&comment=<Comment>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

You can also use the Virtual Service index to specify the Virtual Service, for example:

**https://<LoadMasterIPAddress>/access/aclcontrol?addvs=<ListType>&vs=<VirtualServiceIndex>&addr=<IPAddressToAdd/CIDR>&comment=<Comment>**

The **comment** parameter is optional. The **comment** parameter accepts a maximum of 127 characters.

**https://<LoadMasterIPAddress>/access/aclcontrol?delvs=<ListType>&vsip=<VirtualServerIPAddress>&vsprot=<VirtualServerProtocol>&vsport=<VirtualServerPort>&addr=<IPAddressToRemove/CIDR>**

You can also use the Virtual Service index to specify the Virtual Service, for example:

**https://<LoadMasterIPAddress>/access/aclcontrol?delvs=<ListType>&vs=<VirtualServiceIndex>&addr=<IPAddressToAdd/CIDR>&comment=<Comment>**

## 3.17 Cluster Control

Clustering can be configured using API commands. For details on each of the commands that can be used, refer to the sections below.

> The clustering API commands are only available on LoadMasters which have a clustering license. To add the clustering feature to your license, please contact a Kemp representative. For further information on clustering, refer to the LoadMaster Clustering, Feature Description.

### 3.17.1 Clustering API Commands

The sections below provide details on each of the RESTful API commands relating to clustering. For step-by-step instructions on how to configure clustering using the RESTful API, refer to the **RESTful API Clustering Example** section.

#### 3.17.1.1 Get the Status of the Cluster

To retrieve the status of the cluster, run the command below:

**https://<LoadMasterIPAddress>/access/cluster/status**

The details for all nodes in the cluster is returned. It lists all the enabled nodes in the cluster in XML format, for example:

```
<Response stat="200" code="ok">
<Success>
<Data>
<Status>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
<SharedAddress>10.35.47.100</SharedAddress>
<Node>
<Id>1</Id>
<Address>10.35.47.7</Address>
<Enabled>1</Enabled>
<Status>5</Status>
</Node>
<Node>
<Id>2</Id>
<Address>10.35.47.8</Address>
<Enabled>0</Enabled>
<Status>2</Status>
</Node>
</Status>
</Data>
</Success>
</Response>
```

If the LoadMaster is not in a cluster an error message will be returned using the WUI.

The status is represented by a number, as follows:

- 0 – The node is down
- 1 – The node is up
- 2 – The node is disabled - connections will not be sent to that node. If there are no Virtual Services in the node, the node will be in a Disabled state.
- 3 – The node has been disabled and the connections are being shut down in an orderly fashion. Drain stopping lasts for 10 seconds by default.
- 4 – The node is starting
- 5 – The node is the primary control node.

#### 3.17.1.2 Create a Cluster

If a LoadMaster is not in currently in cluster mode, it can be converted to cluster mode by running the command below:

**https://<LoadMasterIPAddress>/access/cluster/create?SharedAddress=<SharedIPAddress>**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.17.1.3 Initiate a Node Joining a Cluster

To initiate a node joining a cluster, run the following command on the LoadMaster:

**https://<LoadMasterIPAddress>/access/cluster/joincluster**

> Running this command will make the LoadMaster available to be added to the cluster. To finish adding the node, please run the **addnode** command. Refer to the **Add a Node to the Cluster** section for further information.

#### 3.17.1.4 Add a Node to the Cluster

Before running this command, the node LoadMaster needs to be available to be added. To make the node LoadMaster available, run the **joincluster** command on the node LoadMaster. Refer to the **Initiate a Node Joining a Cluster** section for further information on the **joincluster** command.

> If the **addnode** command is run when the node LoadMaster is not available to be added, an error will be returned which says that the machine could not be contacted.

To add a node to the cluster (while the node LoadMaster is available to be added), run the following command on the shared IP address:

**https://<LoadMasterIPAddress>/access/cluster/addnode?Address=<NodeIPAddress>**

#### 3.17.1.5 Enable a Node

When a node is first added to the cluster it is disabled by default. To enable a node, run the following command:

**https://<LoadMasterIPAddress>/access/cluster/enablenode?nodeid=<NodeID>**

The ID of the node can be found in the **ID** column in the **Cluster Control** screen in the LoadMaster WUI, or by running the **status** command (refer to the **Get the Status of the Cluster** section for further details).

#### 3.17.1.6 Disable a Node

To disable a node, run the following command:

**https://<LoadMasterIPAddress>/access/cluster/disablenode?nodeid=<NodeID>**

The ID of the node can be found in the **ID** column in the **Cluster Control** screen in the LoadMaster WUI, or by running the **status** command (refer to the **Get the Status of the Cluster** section for further details).


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.17.1.7 Delete a Node

To delete a node from a cluster, run the command below:

**https://<LoadMasterIPAddress>/access/cluster/deletenode?NodeId=<NodeID>**

The ID of the node can be found in the **ID** column in the **Cluster Control** screen in the LoadMaster WUI, or by running the **status** command (refer to the **Get the Status of the Cluster** section for further details).

### 3.17.2 RESTful API Clustering Example

The sections above provide details relating to each of the clustering RESTful API commands. This section provides step-by-step instructions on how to create a cluster and add a node to it, using these API commands. The example IP addresses which are used in the example commands are below:

- LoadMaster 1: **10.154.11.10**
- LoadMaster 2: **10.154.11.20**
- Shared IP Address: **10.154.11.30**
- Node ID: **2**

Follow the steps below in sequential order to create a cluster and add a node to it:

1. Create a cluster. Run this command on LoadMaster 1:

**https://10.154.11.10/access/cluster/create?SharedAddress=10.154.11.30**

2. Initiate the node (LoadMaster 2) joining a cluster. Run this command on LoadMaster 2:

**https://10.154.11.20/access/cluster/joincluster**

3. Add the node (LoadMaster 2) to the cluster. Run this command on LoadMaster 1:

**https://10.154.11.10/access/cluster/addnode?Address=10.154.11.20**

> The **addnode** command must be run while the node LoadMaster is available to join the cluster. This command should be run immediately after the **joincluster** command.

> If the **addnode** command is run when the node LoadMaster is not available to be added, an error will be returned which says that the machine could not be contacted.

4. Enable the node. Run this command on LoadMaster 1:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
https://10.154.11.10/access/cluster/enablenode?nodeid=2
```

## 3.18 QoS/Limiting

This section contains details about the QoS/Limiting API commands and parameters. You can retrieve or configure each of these parameters using the **get** or **set** RESTful API commands.

Here is an example of a **get** command to retrieve the **MaxConnsLimit** parameter value:

```
/access/get?param=MaxConnsLimit
```

Here is an example of a set command to set the **MaxConnsLimit** to **80000**:

```
/access/set?param=MaxConnsLimit&value=80000
```

The following limiting parameters can be retrieved or configured using the **get** or **set** commands:

- **MaxConnsLimit:** The maximum number of simultaneous connections (TCP and UDP).
- **MaxCPSLimit:** The global connection limit (per second).
- **MaxRPSLimit:** The global request limit (per second).
- **MaxBandwidthLimit:** The global bandwidth limit (kilobits per second)
- **SendRateLimitError:** This parameter accepts the following values:
  - 0 - no error response (the connection is simply dropped)
  - 1 - **Send 429 Too Many Requests** error response
  - 2 - **Send 503 Service Unavailable** error response
- **RateLimitFail:** Fail on rate limit. This parameter accepts the following values:
  - 0 - disabled the LoadMasterttempts to select a different RS or SubVS to use for the connection)
  - 1 - enabled (forces an error)
- **LimitLogging:** Generate a summary log entry every 5 seconds. This parameter accepts the following values:
  - 0 - disabled
  - 1 - enabled
- **ClientRepeatDelay:** Set the minimum time after a client is no longer limited before a new message is generated. If a client generates a message and continues to be blocked for


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

continuously hitting the limit, no new message is generated. Only if the client goes quiet for the delay period will a new message be generated. Valid values range from 10 - 86400 seconds.

- **ClientMaxConnsLimit:** This limits the default maximum number of concurrent connection attempts (per second) from a specific host. Setting the limit to 0 disables this option. Valid values range from 0 - 1000000.
- **ClientCPSLimit:** The global client connection limit.
- **ClientRPSLimit:** The global client request limit.
- **ClientMaxBandwidthLimit:** The global client maximum bandwidth limit.

### 3.18.1 Maximum Client Concurrent Connection Limit

To list the existing client concurrent connection limits, run the **clientmaxclimitlist** command, for example:

```
/access/clientmaxclimitlist
```

To add a new client concurrent connection limit, run the **clientmaxclimitadd** command, for example:

```
/access/clientmaxclimitadd?l7addr=<Address>&l7limit=<Limit>
```

To delete an existing client concurrent connection limit, run the **clientmaxclimitdel** command, for example:

```
/access/clientmaxclimitdel?l7addr=<Address>
```

### 3.18.2 Client CPS Limit

To list the existing Connections Per Second (CPS) limits, run the **clientcpslimitlist** command, for example:

```
/access/clientcpslimitlist
```

To add a new CPS limit, run the **clientcpslimitadd** command, for example:

```
/access/clientcpslimitadd?l7addr=<Address>&l7limit=<Limit>
```

To delete an existing CPS limit, run the **clientcpslimitdel** command, for example:

```
/access/clientcpslimitdel?l7addr=<Address>
```

### 3.18.3 Legacy Client CPS Limit Commands

Before the rate limiting functionality was improved in LoadMaster version 7.2.52, you could run the following commands relating to client CPS limits.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> Although these commands still work - Kemp recommends using the new commands outlined in the **Client CPS Limit** section above.

Client limiting can be used to limit the default maximum number of connection attempts (per second) from a specified host. The limit can be set using the **set** parameter, for example:

```
https://<LoadMasterIPAddress>/access/set?param=l7limitinput&value=25
```

Setting the limit to zero disables the option.

A number of addresses or networks can be specified to be limited. To add an address, run the command below:

```
https://<LoadMasterIPAddress>/access/afeclientlimitadd?l7addr=<L7Address>&l7limit=<L7Limit>
```

To delete an address, run the command below:

```
https://<LoadMasterIPAddress>/access/afeclientlimitdel?l7addr=<L7Address>
```

To list the addresses and their limits, run the command below:

```
https://<LoadMasterIPAddress>/access/afeclientlimitlist?
```

### 3.18.4 Client RPS Limit

To list the existing RPS limits, run the **clientrpslimitlist** command, for example:

```
/access/clientrpslimitlist
```

To add a new RPS limit, run the **clientrpslimitadd** command, for example:

```
/access/clientrpslimitadd?l7addr=<Address>&l7limit=<Limit>
```

To delete an existing RPS limit, run the **clientrpslimitdel** command, for example:

```
/access/clientrpslimitdel?l7addr=<Address>
```

### 3.18.5 Client Bandwidth Limit

To list the existing client bandwidth limits, run the **clientbandwidthlimitlist** command, for example:

```
/access/clientbandwidthlimitlist
```

To add a new client bandwidth limit, run the **clientbandwidthlimitadd** command, for example:

```
/access/clientbandwidthlimitadd?l7addr=<Address>&l7limit=<Limit>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> The global client maximum bandwidth limit (**ClientMaxBandwidthLimit**) must be set before you add a specific client bandwidth limit.

To delete an existing client bandwidth limit, run the **clientbandwidthlimitdel** command, for example:

```
/access/clientbandwidthlimitdel?l7addr=<Address>
```

### 3.18.6 Per-Virtual Service Limits

To add a new Virtual Service with limits, run the **addvs** command, for example:

```
/access/addvs?vs=<VirtualServiceAddress>&port=<VirtualServicePort>&prot=<tcp/udp>&ConnsPerSecLimit=<Limit>&RequestsPerSecLimit=<Limit>&MaxConnsLimit=<Limit>&bandwidth=<Limit>
```

To modify the limits for an existing Virtual Service, run the **modvs** command, for example:

```
/access/modvs?vs=<VirtualServiceAddress>&port=<VirtualServicePort>&prot=<tcp/udp>&ConnsPerSecLimit=<Limit>&RequestsPerSecLimit=<Limit>&MaxConnsLimit=<Limit>&bandwidth=<Limit>
```

To modify the limits for an existing SubVS, run the **modvs** command, for example:

```
/access/modvs?vs=<SubVSIndex>&ConnsPerSecLimit=<Limit>&RequestsPerSecLimit=<Limit>&MaxConnsLimit=<Limit>&bandwidth=<Limit>
```

You can retrieve the SubVS **Index** by running the **listvs** command or by checking the **Id** at the top of the SubVS modify screen.

### 3.18.7 URL-Based Limiting Rules

You can list the existing URL-based limiting rules by running the **listlimitrules** command, for example:

```
/access/listlimitrules
```

You can add a new URL-based limiting rule by running the **addlimitrule** command, for example:

```
/access/addlimitrule?name=ExampleRule&pattern=/test/a.html&limit=5&match=0
```

You can modify an existing URL-based limiting rule by running the **modlimitrule** command, for example:

```
/access/modlimitrule?name=ExampleRule&pattern=/test/b.html&limit=5&match=0
```

Valid values for the **match** parameter are as follows:

- 0 - Request
- 1 - Host


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- 2 - User Agent
- 64 - !Request
- 65 - !Host
- 66 - !UserAgent

> The values with an exclamation mark (**!**) before them matches the inverse, for example, not a specific request or not a specific user agent.

You can delete an existing URL-based limiting rule by running the **dellimitrule** command, for example:

```
/access/dellimitrule?name=ExampleRule
```

You can move the position of an existing URL-based limiting rule by running the **movelimitrule** command, for example:

```
/access/movelimitrule?name=ExampleRule3&position=1
```

Setting the **position** parameter to a value larger than the size of the list will move the rule to the end of the list.

## 3.19 System Administration

Various system administration tasks can be completed using the RESTful API.

### 3.19.1 User Management

#### 3.19.1.1 Change the System Password

To change the password of the default **bal** user, run the command below:

```
https://<LoadMasterIPAddress>/access/usersetsyspassword?currpassword=<Current Password>&password=<NewPassword>
```

#### 3.19.1.2 Set the Minimum Password Length

To set the minimum password length for local users, run the command below:

```
https://<LoadMasterIPAddress>/access/set?param=minpassword&value=<8-16>
```

#### 3.19.1.3 List All Local Users

To list all local users and their permissions, run the command below:

```
https://<LoadMasterIPAddress>/access/userlist
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.19.1.4 Display Permissions for a Particular Local User

To display permissions for a particular local user, run the command below:

**https://<LoadMasterIPAddress>/access/usershow?user=<Username>**

#### 3.19.1.5 Add a New Local User

To add a new local user, run the command below:

**https://<LoadMasterIPAddress>/access/useraddlocal?user=<Username>&password=<UserPassword>**

| Name | Type | Description | Mandatory |
|---|---|---|---|
| user | String | The username of the new user. | Yes |
| password | String | The password of the new user. | Yes – unless **nopass** or **radius** is set to yes. |
| radius | Boolean | Determines whether the user will use RADIUS server authentication or not when logging in to the LoadMaster. The RADIUS server details must be set up before this option can be enabled. | No |
| nopass | Boolean | This option is only valid if session management is enabled. Set this option to yes to create a user with no password. This can be used to allow certificate-based access. For further information, please refer to the **Local Certificate Management** section. | No |

#### 3.19.1.6 Delete a Local User

To delete a local user, run the command below:

**https://<LoadMasterIPAddress>/access/userdellocal?user=<Username>**

#### 3.19.1.7 Change the Password of a Local User

To change the password of a local user, run the command below:

**https://<LoadMasterIPAddress>/access/userchangelocpass?user=<Username>&password=<NewPassword>&radius=<0/1>**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> The username is case sensitive - ensure to enter the username exactly as it has been set.

All parameters are required. The **radius** parameter determines whether the user will use RADIUS server authentication or not when logging in to the LoadMaster. The RADIUS server details must be set up before this option can be used.

#### 3.19.1.8 Set Permissions for a Local User

To set permissions for a local user, run the command below:

```
https://<LoadMasterIPAddress>/access/usersetperms?user=<Username>&perms=<CommaSeparatedListOfPermissions>
```

Multiple permissions can be set at the same time by separating the values with a comma, for example:

```
https://<LoadMasterIPAddress>/access/usersetperms?user=<Username>&perms=real,vs
```

> Running this command will overwrite any previous permissions for this user. For example, if a user had the **rules** permission and you ran the command listed above, the user would no longer have the **rules** permission but would have the **real** and **vs** permission.

Valid values for the perms parameter are listed and described in the table below.

| Value | Description |
|---|---|
| real | This role permits enabling and disabling Real Servers. Users with the Real Servers permission cannot add SubVSs. |
| vs | This role relates to managing Virtual Services. This includes SubVSs. Virtual Service actions permitted vary depending on whether or not the **extendedperms** parameter is enabled. For further information, refer to the **User Management Feature Description** on the Kemp Documentation Page. |
| rules | This role permits managing Rules. Rule modifications permitted include add, delete and modify. |
| backup | This role permits performing system backups. |
| certs | This role permits managing SSL Certificates. Certificate management includes adding, deleting and modifying SSL Certificates. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | |
|---|---|
| cert3 | This role permits managing intermediate Certificates. Certificate management includes the ability to add and delete intermediate certificates. |
| certbackup | This role permits the ability to export and import certificates. |
| users | This role is allowed access to all functionality within the **System Configuration > System Administration > User Management** WUI screen. |
| root | This role gives users all permissions except the permission to change the bal password and the permission to create or delete other users. |
| geo | This role is used only with the LoadMaster GEO product. For more information on GEO and the Global Server Load Balancing (GSLB) Feature Pack, refer to the **GEO, Feature Description** on the Kemp Documentation Page. |
| addvs | This parameter can only be enabled if the **extendedperms** parameter is enabled. This role relates to managing Virtual Services. This includes SubVSs. Refer to the **User Management Feature Description** on the Kemp Documentation Page for further details on the permissions provided by this option. |
| | To set the permissions to none, leave the parameter blank, for example **&perms=** |

#### 3.19.1.9 Local Certificate Management

To return a previously generated certificate for a user, run the **userreadcert** command, in the following format:

**https://<LoadMasterIPAddress>/access/userreadcert?user=<Username>**

To download a previously generated certificate for a user, run the **userdownloadcert** command:

**https://<LoadMasterIPAddress>/access/userdownloadcert?user=<Username>**

To generate a new certificate for a user, run the **usernewcert** command, in the following format:

**https://<LoadMasterIPAddress>/access/usernewcert?user=<Username>&passphrase=<Passphrase>**

> The passphrase is optional. If entered, it will be used to encrypt the private key.

To delete an existing user certificate, run the **userdelcert** command, in the following format:

**https://<LoadMasterIPAddress>/access/userdelcert?user=<Username>**

#### 3.19.1.10 Remote User Group Management

To return a list of existing groups and their associated permissions, run the **grouplist** command:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

**https://<LoadMasterIPAddress>/access/grouplist**

To display permissions for a specific user group, run the **groupshow** command:

**https://<LoadMasterIPAddress>/access/groupshow?group=<GroupName>**

To add a new group, run the **groupaddremote** command:

**https://<LoadMasterIPAddress>/access/groupaddremote?group=<GroupName>**

> The following characters are permitted in the group name: alphanumeric characters, spaces, or the following special symbols: **=~^._+#,@/-**.

To configure permissions for a group, run the **groupsetperms** command:

**https://<LoadMasterIPAddress>/access/groupsetperms?group=<GroupName>&perms=<Permissions>**

Enter a comma-separated list of permissions in the **perms** parameter. The valid values for the **perms** parameter are the same as the ones for the **usersetperms** command, as outlined in the **Set Permissions for a Local User** section.

To delete an existing group, run the **groupdelremote** command:

**https://<LoadMasterIPAddress>/access/groupdelremote?group=<GroupName>**

#### 3.19.1.11 Extended Permissions Management

The Virtual Service operations permitted vary depending on whether or not the **extendedperms** parameter is enabled. For further information, refer to the **User Management Feature Description** on the Kemp Documentation Page.

The **extendedperms** parameter can be managed using the **get** and **set** commands. Refer to the **Using get and set commands** for further information on how to use these commands. For example, to display the value of the parameter, run the following command:

**https://<LoadMasterIPAddress>/access/get?param=extendedperms**

The **extendedperms** parameter is Boolean - set it to **1** to enable extended permissions, or **0** to disable extended permissions.

### 3.19.2 Licensing

Similar to when initially licensing a LoadMaster, a license may be updated using the online or offline method.

Offline licensing requires a Binary Large OBject (BLOB) file which is provided by Kemp.

When updating online, only a Kemp ID and password are needed.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

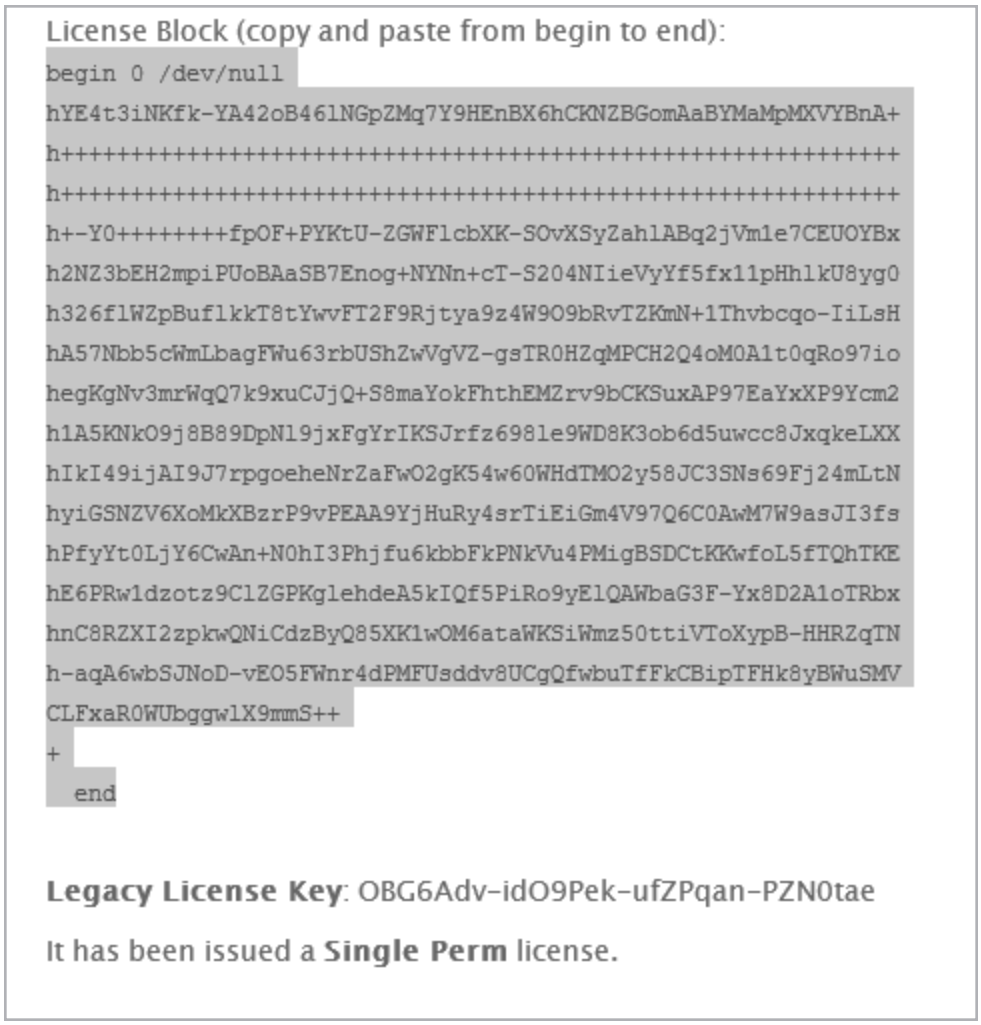
For further information on licensing, refer to the Licensing, Feature Description.

#### 3.19.2.1 License

The LoadMaster's licence can be updated offline by using the **license** command.

The License BLOB is emailed to the customer when requested. Each time a license is updated a new BLOB is needed.

The following is an example of a BLOB:




The BLOB is the body of text from the word begin to the word end, as is highlighted in the example in the screenshot above. The BLOB must be copied and pasted into a text file (in the following example the file is called license.txt). For more information on licensing (including details on how to retrieve a BLOB), please refer to the Licensing, Feature Description.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

There are a number of methods of using the license command for example, using a CURL command on Linux would look like the following:

```
curl –X POST --data-binary “@license.txt” –k
https://<LoadMasterIPAddress>/access/license
```

This command uploads the BLOB file to the LoadMaster. The example command above assumes that the license.txt file is in the current directory. If the license.txt file is stored elsewhere, specify the path to the file after the @ symbol.

#### 3.19.2.2 AlsiLicense

The **AlsiLicense** command updates the LoadMaster's license online. To cause the LoadMaster to query the Kemp licensing system for an updated licence, and update the license if one is available, run the following command:

```
https://<LoadMasterIPAddress>/access/alsilicense?kempid=<KempID>&password=<Ke
mpIDPassword>&lic_type_id=<LicenseTypeID>&orderid=<OrderID>
```

| Name | Type | Description | Mandatory |
|---|---|---|---|
| kempid | String | The email address used when registering for a Kemp ID. | Yes |
| password | String | The Kemp ID account password. | Yes |
| http_proxy | String | Specify the HTTP(S) proxy server and port, in the format **<ProxyAddress>:<Port>**. | No |
| lic_type_id | String | The license type ID. If you specify an order ID, the license type ID is not required.<br><br>To retrieve the license ID, run the **alsilicensetypes** command. Refer to the **Retrieve the Available License Types** section for further details. | No |
| orderid | String | Specify the order ID received from Kemp. The order ID is usually provided by Kemp after purchasing the license in the **Kemp VLM Activation Instructions** document. | Yes |

#### 3.19.2.3 Accesskey

The access key can be obtained by the following command:

```
https://<LoadMasterIPAddress>/access/accesskey?
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.19.2.4 KillASLInstance

If the Activation Server Lite (ASL) functionality was used to license a LoadMaster, the **KillASLInstance** command can be run to deactivate the client LoadMaster license:

```
https://<LoadMasterIPAddress>/access/KillASLInstance
```

> Kemp strongly recommends deregistering a LoadMaster using the Kemp 360 Central WUI/API, rather than the LoadMaster WUI/API. Deregistering a LoadMaster from the LoadMaster UI/API can lead to the LoadMaster having an unknown state in Kemp 360 Central. In these cases, it is not easy to remove the LoadMaster from Kemp 360 Central and the unknown LoadMaster is still taking up an available license.

#### 3.19.2.5 Deactivate a non-SPLA License

To deactivate a non-SPLA (Service Provider License Agreement) client LoadMaster license, run the **kill_instance** command:

```
https://<LoadMasterIPAddress>/access/kill_
instance?name=<KempID>&passwd=<KempIDPassword>&kill=1
```

> Do not run this command unless instructed to by Kemp Support.

### 3.19.3 System Reboot

The LoadMaster can be shut down or rebooted using the following commands:

```
https://<LoadMasterIPAddress>/access/shutdown?
https://<LoadMasterIPAddress>/access/reboot?
```

### 3.19.4 Update Software

#### 3.19.4.1 Upgrade to a Newer Version of Software

The LoadMaster can be upgraded to a new version of software by using the **installpatch** command. There are a number of methods of using this command for example, using a CURL command on Linux would look like the following:

```
curl -X POST --data-binary "@<LM Patch File>" -k
https://<LoadMasterIPAddress>/access/installpatch
```

This cURL command would install a patch (<LM Patch File>) on the system.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> The file being uploaded must be a valid patch file. If the file does not work in the WUI it will not work using a RESTful API command.

#### 3.19.4.2 Check the Previously Installed Firmware Version

You may want to check the previously installed LoadMaster firmware version in certain situations, for example, before you roll back to a previous firmware version. To check the previously installed firmware version, run the following command:

**https://<LoadMasterIPAddress>/access/getpreviousversion**

#### 3.19.4.3 Restore to a Previously Installed Version of Software

The previous version of firmware on the LoadMaster can be restored by using the following command:

**https://<LoadMasterIPAddress>/access/restorepatch**

The machine needs to be rebooted for the change to take place.

#### 3.19.4.4 List the Installed Add-On Packs

A list of any add-on packages that are installed on the LoadMaster can be displayed by running the following command:

**https://<LoadMasterIPAddress>/access/listaddon**

#### 3.19.4.5 Upload or Update an Add-On Pack

Add-on packs can be uploaded by running the following POST command:

```
curl -X POST --data-binary "@<Path To Add-On Pack File>" -k
https://<LoadMasterIPAddress>/access/addaddon
```

> If the add-on pack already exists, the add-on pack will be updated to the version being uploaded.

#### 3.19.4.6 Delete Add-On Pack

Add-on packs can be deleted by running the following command:

**https://<LoadMasterIPAddress>/access/deladdon?name=<AddOnPackName>**

The name of the existing add-on packs can be displayed by running the **listaddon** command.

### 3.19.5 Backup/Restore

LoadMaster configurations can be backed up or restored using the following commands:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
curl -k  "https://bal:<Password>@<LoadMasterIPAddress>/access/backup" -o
attemptbackup
```

If you run this command using cURL the file will be downloaded to your working directory in Linux.

Below is an example of a cURL command to restore a LoadMaster configuration:

```
curl -X POST --data-binary "@<Path To Backup File>" -k
https://<LoadMasterIPAddress>/access/restore?type=<RestoreTypeNumber>
```

**type** takes the integer range from 1 to 15:

| Name | Type | Range | Additional Information |
|---|---|---|---|
| type | Integer | 1-15 | 1 = LoadMaster Base configuration<br>2 = Virtual Service configuration<br>3 = Base and Virtual Service configuration<br>4 = GEO configuration<br>5 = Base and GEO configuration<br>6 = Virtual Service and GEO configuration<br>7 = Base, Virtual Service and GEO configuration<br>8 = ESP SSO configuration<br>9 = ESP SSO and base configuration<br>10 = ESP SSO and Virtual Service configuration<br>11 = ESP SSO, Virtual Service and base configuration<br>12 = ESP SSO and GEO configuration<br>13 = ESP SSO, GEO and base configuration<br>14 = ESP SSO, GEO and Virtual Service configuration<br>15 = ESP SSO, GEO, Virtual Service and Base configuration |

#### 3.19.5.1 Automated Backups

Parameters relating to automated backups that can be managed using **get** and **set** commands are detailed in the following table. Refer to the **Using get and set commands** section for the **get** and **set** commands.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| Name | Type | Default | Range | Additional Information |
|---|---|---|---|---|
| backupday | Integer | Daily | 0-7 | Specify which day to perform the automated backup (or daily):<br>0 = Daily<br>1 = Monday<br>2 = Tuesday<br>3 = Wednesday<br>4 = Thursday<br>5 = Friday<br>6 = Saturday<br>7 = Sunday |
| backupenable | Boolean | N | | Enable automated timed backups (using FTP, SCP, or SFTP). |
| backuphost | String | | | Set the IP address or hostname of the remote host to which you want the backup archives sent, optionally followed by a colon and the port number. If no port is specified, the default port for the selected protocol is used. |
| backuphour | Integer | 0 | 0-23 | The hour to perform the automated backup.<br>0 = Midnight<br>23 = 11pm |
| backupminute | Integer | 0 | 0-59 | The minute to perform the automated backup.<br>Note the range values are full minutes |
| backupsecure | Boolean | 0 - ftp | 0 – ftp (insecure)<br>1 – scp | Specify the file transfer method for automated backups. This is a legacy parameter. You cannot specify **sftp** |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | (secure) | **(secure)** if using this parameter. To set the **Backup Method** to **sftp (secure)** use the **backupmethod** parameter. |
| backupmethod | String | wput | | Specify the file transfer method for automated backups. Takes a string that can be either **wput**, **scp**, or **sftp**. Setting the backupmethod to **wput** sets the **Backup Method** field to **Ftp (insecure)**. |
| backuppassword | String | | | The password of the remote user. This parameter is used when the **backupsecure** method is set to **0** (**Ftp (insecure)**). |
| backupident | File | | | If using **scp** or **sftp** as the **backupmethod**, the remote identity value must be provided. This is the SSH private key generated using ssh-keygen on the remote scp server.<br><br>The key file must be encoded in base64 before uploading.<br><br>This parameter can only be set – running a get on this parameter returns some asterisks. |
| backuppath | String | | | Specify the remote path name. |
| backupuser | String | | | Specify the remote username. |

> You cannot use the **Test Automated Backups** functionality using the API. You can do this using the WUI if needed.

### 3.19.6 Date/Time Settings

Parameters relating to the date and time that can be managed using **get** and **set** commands are detailed in the following table. Refer to the **Using get and set commands** section for the **get** and **set** commands.

| Name | Type | Additional Information |
|---|---|---|
| ntphost | S | Specify the host from which the LoadMaster will set the time. Multiple |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| | | hosts can be specified in a space-separated list. Please escape the spaces using %20. The time will be set from the first host to return a valid answer. |
| time | I | The time in hours, minutes and seconds. |
| timezone | S | The timezone where the LoadMaster is located |
| ntpkeyid | I | The NTP key ID. Valid values range from 1 to 99. |
| ntpkeysecret | S | The NTP shared secret string. The NTP secret can be a maximum of 40 characters long. If the secret is more than 20 characters long, it is treated as a hex string. Setting this value to an empty string will disable the NTPv4 feature. |
| ntpkeytype | S | Specify the NTP Key Type. The valid values are SHA-1 (**SHA1**), legacy SHA (**SHA**), and MD5 (**M**). Note that the values are case sensitive and must be in uppercase. |

It is not possible to set the time using a RESTful API command.

## 3.20 Logging Options

### 3.20.1 Manage System Logs

To list the existing system log files, run the following command:

**https://<LoadMasterIPAddress>/access/logging/listsyslogfiles**

To clear all the system log files, run the following command:

**https://<LoadMasterIPAddress>/access/logging/clearlogs**

The legacy command before **clearlogs** was **resetlogs**.

To clear a specific log file, run the following command:

**https://<LoadMasterIPAddress>/access/logging/clearlogs?fsel=<FileToClear>**

To save all the system log files, run the following command:

**https://<LoadMasterIPAddress>/access/logging/savelogs**

The legacy command before **savelogs** was **downloadlogs**.

To save a specific log file, run the following command:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

**https://<LoadMasterIPAddress>/access/logging/savelogs?fsel=<FileTodownload>**

When using cURL, successful output of the required log file is compressed into .tar and .gzip format and the downloaded filename can be provided using the **-o** parameter. To print the response code in the filename provided in the cURL request, use the following syntax: **-w"%{http_code}\n"**. If the output fails, it is saved as text in the provided file. For example:

```
curl -o syslogs.tar.gz -s -w "%{http_code}\n" -k
"https://<Username>:<Password>@<LoadMasterIPAddress>/access/logging/savelogs?
fsel=messages"
```

### 3.20.2 Ping Host

To perform a ping, run the following command:

**https://<LoadMasterIPAddress>/access/logging/ping?addr=<Address>&intf=<Interf aceID>**

| Parameter | Parameter Type | Parameter Description | Mandatory |
|---|---|---|---|
| addr | Address | Specify the host to perform the ping on. This parameter accepts an IPv4 address, IPv6 address, FQDN, or hostname. | Yes |
| intf | Integer | Specify the ID of the interface from which the ping should be sent from. If the interface is not specified here, the correct interface to ping an address on a particular network will be automatically selected. | No |

The LoadMaster will try to auto-detect what type of ping to use (ping for IPv4 and ping6 for IPv6). However, it is also possible to force a ping6 on an IPv6 address by running the **ping6** command:

**https://<LoadMasterIPAddress>/access/logging/ping6?addr=<Address>&intf=<Inter faceID>**

> The ping command returns a **200 OK** success message even if an incorrect or non-existing interface is provided.

### 3.20.3 Run a Traceroute

To perform a traceroute, run the following command:

**https://<LoadMasterIPAddress>/access/logging/traceroute?addr=<Address>**

The **addr** parameter accepts an IPv4 address, IPv6 address, FQDN, or hostname.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

### 3.20.4 Debug Options

#### 3.20.4.1 Get/Set Debug Options

Parameters relating to Debug Options that can be managed using **get** and **set** commands are detailed in the table below. Refer to the **Using get and set commands** section for the **get** and **set** commands. For example, to display the value of the irqbalance parameter, run the following command:

```
https://<LoadMasterIPAddress>/access/get?param=irqbalance
```

| Name | Type | Parameter Description |
|---|---|---|
| irqpinning | B | You can use this parameter to enable or disable Interrupt Request Line (IRQ) pinning. This is disabled by default.<br>Only enable this option in consultation with Kemp Support.<br>When you change the IRQ pinning option from off to on, IRQ pinning is enabled on all network interfaces that are assigned an IP address. When IRQ pinning is enabled and you add an IP address to an unconfigured interface, that interface will not have IRQ pinning enabled until you either toggle the IRQ pinning off and back on again, or the system is rebooted. |
| irqbalance | B | The purpose of IRQBalance is distribute hardware interrupts across processors on a multiprocessor system. This should only be enabled after consultation with Kemp technical support. |
| tcpsack | B | Use this parameter to enable or disable TCP SACK (Selective ACKnowledgement) processing. This is a global setting that affects all Layer 7 Virtual Services. It only works if TCP SACK is enabled on a Virtual Service client and the LoadMaster. |
| IPV6forwarding | B | Enable this parameter to enable Layer 4 IPv6 forwarding. Disable this option for full IPv6 conformance. |
| EnableISetupCli | B | Enable or disable the Command Line Interface (CLI) Service |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| | | Management function. |
| linearesplogs | B | By default, the LoadMaster deletes older log files. If this parameter is enabled, older log files will no longer be deleted. If the filesystem fills up, further access using the LoadMaster is blocked. |
| dhcpv6 | B | When this parameter is enabled, the DHCPv6 client will run on the primary interface. This provides the capability to obtain an IPv6 address on boot. If you want DHCPv6 to be run on every boot, keep this option enabled. However, this is a long running process and it keeps running in the background when it is enabled so if you only need an IPv6 address to be assigned and you do not need to renew and release the IPv6 address you should disable this option after the IPv6 address is assigned. |

#### 3.20.4.2 Retrieve RAID Information

Display the Redundant Array of Independent Disks (RAID) controller details, including the model name, serial number, capacity, state, status, level, and total members in the RAID, by running this command:

**https://<LoadMasterIPAddress>/access/logging/getraidinfo**

#### 3.20.4.3 Retrieve RAID Disk Information

Display details about the RAID disks, including the model name, serial number, firmware version, capacity, type, and speed, by running this command:

**https://<LoadMasterIPAddress>/access/logging/getraiddisksinfo**

#### 3.20.4.4 Reset Statistics

Reset the statistics by running the following command:

**https://<LoadMasterIPAddress>/access/logging/resetstats**

#### 3.20.4.5 Flush SSO Authentication Cache

The SSO authentication cache can be flushed by running the **ssoflush** command:

**https://<LoadMasterIPAddress>/access/logging/ssoflush**

### 3.20.5 Extended Log Files

#### 3.20.5.1 List the Extended Log Files

To list the existing extended log files, run the **listextlogfiles** command:

**https://<LoadMasterIPAddress>/access/listextlogfiles**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.20.5.2 Clear Extended Log Files

To clear the extended log files, run the **clearextlogs** command. To clear all the ESP log files, run the command without the **fsel** parameter:

```
https://<LoadMasterIPAddress>/access/logging/clearextlogs
```

To clear a specific extended log file, enter the log file to clear in the **fsel** parameter:

```
https://<LoadMasterIPAddress>/access/logging/clearextlogs?fsel=connection
```

#### 3.20.5.3 Save Extended Log Files

To save (download) the extended log files, run the **saveextlogs** command.

To save a specific extended log file, enter the log file to save in the **fsel** parameter:

```
https://<LoadMasterIPAddress>/access/logging/saveextlogs?fsel=connection
```

When using cURL, successful output of the required log files is compressed into .tar and .gzip format and the downloaded filename can be provided using the **-o** parameter. To print the response code in the filename provided in the cURL request, use the following syntax: **-w"%{http_code}\n"**. If the output fails, it is saved as text in the provided file. For example:

```
curl -o extlogs.tar.gz -s -w "%{http_code}\n" -k
"https://<Username>:<Password>@<LoadMasterIPAddress>/access/logging/saveetxlo
gs?fsel=user"
```

#### 3.20.5.4 Enable/Disable Extended ESP Logging

To check if the **Disable Local Extended ESP Logs** option is currently enabled/disabled, run the **isextesplogenabled** command:

```
https://<LoadMasterIPAddress>/access/logging/isextesplogenabled
```

To disable extended ESP logging, run the **disableextesplog** command:

```
https://<LoadMasterIPAddress>/access/logging/disableextesplog
```

To enable extended ESP logging, run the **enableextesplog** command:

```
https://<LoadMasterIPAddress>/access/logging/enableextesplog
```

If **Disable Local Extended ESP Logs** is disabled (the default option), messages are written to the extended ESP logs expediently and are not sent to any remote syslog servers that are defined.

If **Disable Local Extended ESP Logs** is enabled, no messages are written to the extended ESP logs and messages are only sent to the remote logger (if one is defined). If a remote logger is not defined, no logs are recorded.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

You can no longer configure the system to both populate the local extended ESP logs and send the same messages to remote syslog servers, as it was in previous releases.

### 3.20.6 Syslog Options

Parameters relating to Syslog Options that can be managed using **get** and **set** commands are detailed in the table below. Refer to the **Using get and set commands** section for the **get** and **set** commands.

| Name (*SyslogLevelParam*) | Type | Parameter Description |
|---|---|---|
| syslogemergency | A | Use this option to set the host(s) which will receive **Emergency** events only. Entries must be comma-separated. Up to 10 entries are supported in total for all levels. |
| syslogcritical | A | Use this option to set the host(s) which will receive **Emergency** and **Critica**l events. Entries must be comma-separated. Up to 10 entries are supported in total for all levels. |
| syslogerror | A | Use this option to set the host(s) which will receive **Emergency, Critical** and **Error** events. Entries must be comma-separated. Up to 10 entries are supported in total for all levels. |
| syslogwarn | A | Use this option to set the host(s) which will receive **Emergency**, **Critical**, **Error** and **Warning** events. Entries must be comma-separated. Up to 10 entries are supported in total for all levels. |
| syslognotice | A | Use this option to set the host(s) which will receive **Emergency**, **Critical**, **Error**, **Warning** and **Notice** events. Entries must be comma-separated. Up to 10 entries are supported in total for all levels. |
| sysloginfo | A | Use this option to set the host(s) which will receive **All** events. Entries must be comma-separated. Up to 10 entries are supported in total for all levels. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| syslognone | A | Use this option to delete a host, or hosts, from any syslog level. Because you can only assign a specific host to one level, you do not need to specify the syslog level to remove the host from. Entries must be comma-separated. Up to 10 entries can be deleted at once.<br><br>The **get** command does not retrieve anything for this parameter. |
| syslogport | I | Specify the port that syslog messages are sent to on the receiving hosts. |
| syslogprot | S | Specify what protocol to use for the connection to a remote syslog server. Valid values are **tcp**, **udp**, and **tls**. |
| syslogcert | B | This parameter is only relevant when **tls** is specified as the **syslogprot**. When **syslogcert** is enabled, it ensures that the host name or IP address that was used to initiate the secure connection resides in the Certificate Subject or Subject Alternative Names (SAN) of the certificate. |

Up to 10 individual IP addresses and/or hostnames can be specified for each of the Syslog fields. Multiple IP addresses/hostnames must be differentiated using a comma-separated list.

> You cannot configure the same host for multiple levels.

To delete all hosts for a syslog level, set the value of the syslog level to an empty string, for example:

**`https://<LoadMasterIPAddress>/access/set?param=<SyslogLevelParam>&value=`**

For example:

**`https://<LoadMasterIPAddress>/access/set?param=syslognotice&value=`**

### 3.20.7 SNMP Options

Parameters relating to SNMP Logging Options that can be managed using **get** and **set** commands are detailed in the following table. Refer to the **Using get and set commands** section for the **get** and **set** commands.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| Name | Type | Additional Information |
|---|---|---|
| snmpcommunity | S | Specify the SNMP community string. |
| snmpcontact | S | Specify the contact address that is sent in SNMP responses. |
| snmpenable | B | 0 - Disabled<br>1 - Enabled |
| snmptrapenable | B | Enable the generation of SNMP events whenever a significant event occurs. |
| snmpv1sink | A | Specify the sink address for SNMP type 1 traps. |
| snmpv2sink | A | Specify the sink address for SNMP type 2 traps. |
| snmpV3enable | B | Enable/disable SNMP V3.<br>0 - Disabled<br>1 - Enabled |
| snmpv3user | A | Specify the username. |
| snmpv3userpasswd | A | Specify the user password. |
| snmplocation | S | Specify the location that is sent in SNMP responses. |
| snmpclient | S | Specify the list of machines that can access the SNMP subsystem. If no clients are specified, anyone can access SNMP. |
| snmpHATrap | B | Send SNMP traps from the shared IP address. This option is only available when the LoadMaster is in HA mode. |
| snmpAuthProt | S | Specify the relevant authentication protocol:<br>MD5<br>SHA<br>SHA is a more secure protocol.<br>**Note:** These values are case sensitive - please enter them in uppercase. |
| snmpV3Privenable | B | Enable the SNMP V3 private password. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| | | 0 - Disabled<br>1 - Enabled |
| snmpv3privpasswd | A | Specify the private password. |
| snmpPrivProt | S | Specify the relevant privacy protocol:<br>**DES**or **AES**<br>AES is a more secure protocol.<br>**Note:** These values are case sensitive - please enter them in uppercase. |

### 3.20.8 Email Options

Parameters relating to Email Logging Options that can be managed using **get** and **set** commands are detailed in the following table. Refer to the **Using get and set commands** section for the **get** and **set** commands.

| Name | Type | Range | Additional Information |
|---|---|---|---|
| emailcritical | S | | The email address to receive critical messages. |
| emaildomain | S | | The domain, if required, for the user account authentication. |
| emailemergency | S | | The email address to receive emergency messages. |
| emailenable | B | | Enables or disables the email logging options. |
| emailerror | S | | The email address to receive error messages. |
| emailinfo | S | | The email address to receive informational messages. |
| emailnotice | S | | The email address to receive notices. |
| emailpassword | S | | The email user's password. |
| emailport | I | 0-65535 | The TCP port on which your mail server accepts connections (usually 25). |
| emailserver | S | | The host name or address of the SMTP server to send mail messages through. |
| emailsslmode | I | 0-3 | Specify the type of security protocol that should be used on the connection:<br>0 = None |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| | | 1 = STARTTLS, if available<br>2 = STARTTLS<br>3 = SSL/TLS |
| emailuser | S | The user account with access to send email messages. |
| emailwarn | S | The email address to receive warnings. |

### 3.20.9 SDN Log Files

#### 3.20.9.1 Debug Options

There are two modes that can be used to gather the SDN statistics.

The modes are described below:

- **Mode 1:** When set to mode 1, the statistics are taken from the switch port that is connected to the server and the statistics are relayed back to the LoadMaster.
- **Mode 2:** When set to mode 2, the information is taken from all of the switch ports along the path.

The SDN statistics mode can be managed using the **get** and **set** commands by using the parameter **sdnstatsmode** with a value of 1 or 2, for example:

**`https://<LoadMasterIPAddress>/access/set?param=sdnstatsmode&value=2`**

## 3.21 Troubleshooting

### 3.21.1 Get/Set Debug Options

Parameters relating to Troubleshooting that can be managed using **get** and **set** commands are detailed in the table below. Refer to the **Using get and set commands** section for the **get** and **set** commands.

| Name | Type | Parameter Description |
|---|---|---|
| backupnetstat | B | By default, the LoadMaster includes a Netstat output in backups taken. When this is included, backups take longer to complete. You can stop the Netstat output from being included by disabling this parameter. |
| netconsole | A | Netconsole is a kernel module which logs kernel printk messages over UDP allowing debugging of problems where disk logging fails. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | |
|---|---|---|
| | | If this parameter is populated, the syslog daemon on a specific host will receive all critical kernel messages. This can help in understanding why a LoadMaster is rebooting. Netconsole is mainly used for capturing kernel panic output.<br><br>To unset this, set the value to an empty string. |
| netconsoleinterface | I | The interface which hosts the Netconsole. |

### 3.21.2 Run a Top

Performing a top displays memory, CPU, and I/O usage for the LoadMaster. You can specify the number of samples and an interval between them (the default is 10 samples and a 1 second interval). You can also show threads and/or sort by memory usage by selecting the appropriate check boxes.

Perform a top by running the following command:

**`https://<LoadMasterIPAddress>/access/logging/top`**

| Name | Type | Parameter Description |
|---|---|---|
| iterations | I | Specify the number of samples (the default is 10 samples).<br><br>Range: 1-30 |
| interval | I | Specify the interval between them (the default is a 1 second interval).<br><br>Range: 1-30 |
| threads | B | Enable this option to show process threads (disabled by default).<br><br>0 - Disabled<br><br>1 - Enabled |
| mem | B | By default, the results are sorted by CPU usage (so the **mem** parameter is defaulted at 0 - Disabled). Enable the **mem** parameter to sort by memory usage instead.<br><br>0 - Disabled<br><br>1 - Enabled |

Here is an example with each of the optional parameters set:

**`https://<LoadMasterIPAddress>/access/logging/top?iterations=4&interval=3&threads=1&mem=1`**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

By default, the LoadMaster does not include **top** command output in LoadMaster system backups. To include it, enable the **backuptop** parameter using the **set** command:

```
https://<LoadMasterIPAddress>/access/set?param=backuptop&value=1
```

When included in LoadMaster system backups, **top** is run using the default parameters (regardless of what is configured in the WUI) and is sorted by memory usage.

### 3.21.3 Run the Other Debug Options

These other debug options commands can be run using the API:

- /logging/ps

  > The **ps** command does not work when run in a browser. Use a cURL command to run a **ps**.

- /logging/meminfo
- /logging/ifconfig
- /listifconfig
- /logging/netstat
- /logging/interrupts
- /logging/partitions
- /logging/cpuinfo
- /logging/df
- /logging/lspci
- /logging/lsmod
- /logging/slabinfo

For example:

```
https://<LoadMasterIPAddress>/access/logging/meminfo
```

### 3.21.4 Run a TCP Dump

Run a TCP dump using the following command:

```
https://<LoadMasterIPAddress>/access/tcpdump?maxpackets=<MaximumNumberOfPackets>&maxtime=<MaximumTime>&interface=<InterfaceID>&port=<Port>&address=<Address>&tcpoptions=<OptionalParameters>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

All parameters are optional.

| Name | Type | Parameter Description | Mandatory |
|---|---|---|---|
| maxpackets | I | The maximum number of packets to capture. The default value for this parameter is 10000. Valid values range from 1 to 200000. | N |
| maxtime | I | The maximum number of seconds to capture. The default value for this parameter is 10. Valid values range from 1 to 600. | N |
| interface | I | The interface(s) to monitor. The default interface is eth0. A TCP dump can be captured either by one or all Ethernet ports. | N |
| port | I | The port to be monitored. | N |
| address | I | The (optional) address to be monitored. | N |
| tcpoptions | S | Any optional parameters needed. The maximum number of characters permitted is 255. You can use any options that you can have in a tcp dump command. For example, if you do not set the port parameter, you could set the port in the **tcpoptions** parameter. You could also set the protocol to udp. You can enter multiple options. | N |

The output of a TCP dump is a .pcap file, which is downloaded. You can use an application such as Wireshark to view the output.

## 3.22 Miscellaneous Options

### 3.22.1 WUI Settings

Parameters relating to WUI Settings that can be managed using **get** and **set** commands are detailed in the following table. Refer to the **Using get and set commands** section for the **get** and **set** commands.

| Name | Type | Range | Description |
|---|---|---|---|
| hoverhelp | B | 0 – Disable<br>1 - | This option allows the display of descriptive text when a cursor rests on a clickable option in the WUI screen. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | Enable | |
| autosave | B | 0 – Disable<br>1 - Enable | Disabling auto-save is currently a beta feature. Auto-save is enabled by default. If it is disabled, this option modifies the several default WUI behaviors. For further details refer to the Web User Interface (WUI) Configuration Guide. |
| motd | S | | This is the Message of the Day (MOTD). Either plain text or a text file can be used.<br>The maximum number of characters is 5,000.<br>An error will be displayed if the MOTD is greater than 5,000 characters. |
| wuidisplaylines | I | 10-100 | Set the maximum number of lines which can be displayed on a single statistics page. |

> If the Message Of The Day (MOTD) is specified using the **set** command as above, the maximum number of characters that can be entered is 5,000.

You can view the third-party acknowledgements file applicable to the LoadMaster release you are running by using the **notice** command. For example:

**`access/notice`**

### 3.22.2 L7 Configuration

Parameters relating to L7 Configuration that can be managed using **get** and **set** commands are detailed in the following table. Refer to the **Using get and set commands** section for the **get** and **set** commands.

| Name | Type | Range | Description |
|---|---|---|---|
| addcookieport | B | 0 - Disabled<br>1 - Enabled | When using the LoadMaster behind a NATing gateway, all client addresses are the same. To create individual cookies the remote port can also be added to the cookie. Enabling this option when not needed wastes resources. |
| addvia | B | 0 - Disabled | When enabled, a VIA header field will be added |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | 1 - Enabled | to all cache responses. The Virtual Service address will be the address used. |
| allowemptyposts | B | 0 - Disabled<br>1 - Enabled | By default the LoadMaster blocks POSTs that do not contain a Content-Length or Transfer-Encoding header to indicate the length of the requests payload. When this parameter is set to true, such requests are assumed to have no payload data and are therefore not rejected. |
| forcefullrsmatch | B | 0 – Disabled<br>1 – Enabled | By default, when the LoadMaster is trying to locate a Real Server for use with content switching, it tries to use the same Real Server as currently selected, even if the port is not the same. Enabling this parameter forces the port to also be compared. |
| alwayspersist | S | 0 = Only check persist on the first request of a HTTP/1.1 connection<br>1 = Check the persist on every request<br>2 = All persistent changes will be saved, even in the middle of a connection | This parameter also accepts **no** and **yes** as valid values. **No** and **yes** correspond to 0 and 1 respectively. |
| closeonerror | B | 0 - Disabled<br>1 - Enabled | When enabled, the LoadMaster will always close the client connection when it sends back an error response. For Example, this changes the behaviour of the LoadMaster when sending back a 304 File not changed message after receiving an If-Modified-Since HTTP header. |
| dropatdrainend | B | 0 - Disabled<br>1 - Enabled | If enabled, all open connections to disabled Real Servers will be dropped at the end of the Real |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | Servers Drain Stop Time OR immediately if there are no Persist entries associated with the Real Server. |
| droponfail | B | 0 - Disabled<br>1 - Enabled | By default, existing connections are not closed if a Real Server fails. Enabling this feature causes all connections to be immediately dropped on Real Server failure |
| expect100 | I | 0 - RFC-2616 Compliant<br>1 - Require 100-Continue<br>2 - RFC-7231 Compliant | Determines how 100-Continue Handling messages are handled. The available options are:<br>- RFC-2616 Compliant (**0**): conforms with the behavior as outlined in RFC-2616<br>- Require 100-Continue (**1**): forces the LoadMaster to wait for the 100-Continue message<br>- RFC-7231 Compliant (**2**): ensures the LoadMaster does not wait for 100-Continue messages. This is the default value.<br>Modifying how 100 Continue messages are handled by the system requires an understanding of the relevant technologies as described in the RFCs listed above. It is recommended that you speak with a Kemp Technical Support engineer before making changes to these settings. |
| rfcconform | B | 0 - Disabled<br>1 - Enabled | By default, the LoadMaster conforms to the RFC when parsing HTTP headers. Disabling this will allow interworking with some broken browsers. |
| rsarelocal | B | 0 - Disabled<br>1 - Enabled | When checking to see if a client is on the local subnet, also check to see if the client is actually a Real Server. |
| localbind | B | 0 - Disabled<br>1 - Enabled | In very high load situations, local port exhaustion can occur. Enabling this option |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | allows the setting of alternate source addresses. This can be used to expand the number of available local ports. |
| transparent | B | 0 - Disabled<br>1 - Enabled | Globally enable or disable the transparent handling of connections using the L7 subsystem. L4 connections are ALWAYS handled transparently. |
| slowstart | I | 0-600 | When using the Least Connection (or Weighted Least Connection) scheduling method, specify the time (in seconds) over which the load to a Real Server which has just come online will be throttled. |
| addforwardheader | I | 0 - X-ClientSide<br>1 - X-Forwarded-For<br>2 - None | This option (which is only available when **L7 Transparency** is disabled) allows the addition of either **X-ClientSide** or **X-Forwarded For** to the HTTP header. The default value is **X-Forwarded-For**. |
| logsplitinterval | I | 1-100 | When using Log Insight Scheduling this is the number of messages which are received on a connection before the stream is rescheduled. The default value is 10. |
| authtimeout | I | 30 – 300 | The duration (in seconds) that a connection remains open for while authentication is ongoing. This value can be between 30 and 300. |
| authpostwait | I | 1-2000 | When using KCD backend authentication, the length of time to wait for a 401 response from a POST before sending the remainder of the POST body. |
| clienttokentimeout | I | 60-300 | The duration (in seconds) to wait for the client token while the process of authentication is ongoing (used for RSA SecurID and RADIUS authentication). The default value for this parameter is 120. |
| ShareSubVSPersist | I | 0 – Disabled | By default, each SubVS has an independent persistence table. Enabling this parameter will |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | 1 – Enabled | allow the SubVS to share this information. |
| loguseragent | B | 0 - Disabled<br>1 - Enabled | When enabled, the User Agent header field is added to the User Logs. |
| CEFmsgFormat | B | 0 - Disabled<br>1 - Enabled | When enabled, the ESP logs are generated in Common Event Format (CEF). CEF log format is easily consumable for Security Information and Event Management (SIEM) tools, such as; Splunk, SolarWinds, LogRhythm, AlienVault, and so on.<br>This option is disabled by default. |
| SameSite | I | 0 – SameSite Option Not Added<br>1 – SameSite=None<br>2 - SameSite=LAX<br>3 - SameSite=Strict | Set the default value for SameSite option for cookies sent by the LoadMaster during ESP processing. The default value is SameSite option not added. |
| L7NTLMProxy | B | 0 - Disabled<br>1 - Enabled | When **L7NTLMProxy** is enabled, NTLM authorization works against the Real Servers. If **L7NTLMProxy** is disabled, the old insecure NTLM processing is performed.<br>Kemp highly recommends ensuring that **L7NTLMProxy** is enabled. |

### 3.22.3 Network Options

Parameters relating to Network Options that can be managed using **get** and **set** commands are detailed in the following table. Refer to the **Using get and set commands** section for the **get** and **set** commands.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| Name | Type | Range | Additional Information |
|---|---|---|---|
| snat | B | 0 - Disabled<br>1 - Enabled | Enabling this option allows the LoadMaster to NAT connections from the Real Servers to the internet. |
| allowupload | B | 0 - Disabled<br>1 - Enabled | The LoadMaster has been optimized with HTTP workloads in mind. Enabling this option allows non HTTP uploads to work correctly. |
| conntimeout | I | 0-86400 | Specify (in seconds) the time a connection can be idle before it is closed. This is independent of Persistency Timeout. Setting a value of 0 resets to the default value of 660 seconds. |
| keepalive | B | 0 - Disabled<br>1 - Enabled | By default, the system uses TCP keepalives to check for failed clients. Enabling this option improves the reliability of older TCP connections (SSH sessions). This is not normally required for normal HTTP/HTTPS services. |
| multigw | B | 0 - Disabled<br>1 - Enabled | Use this option to enable the ability to move the default gateway to a different interface.<br>Alternate default gateway support is not permitted in a cloud environment. |
| nonlocalrs | B | 0 - Disabled<br>1 - Enabled | Enable this option to permit non-local Real Servers to be assigned to Virtual Services.<br>This option is enabled by default. |
| onlydefaultroutes | B | 0 - Disabled<br>1 - Enabled | Enable this option to force traffic from Virtual Services, which have default route entries set, to be routed to the interface where the Virtual Service's default route is located. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| resetclose | B | 0 - Disabled<br>1 - Enabled | When enabled, the LoadMaster will close its connection to the Real Servers by using TCP RESET instead of the normal close handshake. |
| subnetorigin | B | 0 - Disabled<br>1 - Enabled | When transparency is disabled for a Virtual Service, the source IP address of connections to Real Servers is the Virtual Service. When enabled, the source IP address is the local address of the LoadMaster. If the Real Server is on a subnet, the subnet address of the LoadMaster will be used. |
| subnetoriginating | B | 0 - Disabled<br>1 - Enabled | When transparency is disabled for a Virtual Service, the source IP address of connections to Real Servers is the Virtual Service. When enabled, the source IP address is the local address of the LoadMaster. If the Real Server is on a subnet, the subnet address of the LoadMaster will be used. |
| tcptimestamp | B | 0 - Disabled<br>1 - Enabled | The LoadMaster can include a timestamp in the SYN when connecting to Real Servers. Only enable this only on request from Kemp Support. |
| routefilter | B | 0 - Disabled<br>1 - Enabled | When enabled, this option only accepts IP frames from a host over the interface where the routing algorithm would route frames to the host. This is known as strict source route validation. |
| sslforceserververify | B | 0 – Disabled<br>1 – Enabled | By default, when re-encrypting traffic the LoadMaster does not check the certificate provided by the Real Server. Enabling this option forces the LoadMaster to verify that the certificate on the Real Server is valid, that is, the certificate authority and expiration are OK. This includes all intermediate certificates. |
| http_proxy | S | | This option allows clients to specify the HTTP(S) proxy server and port the LoadMaster will use to access the internet. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| tcpnorecycle | B | 0 - Disabled<br>1 - Enabled | This option is disabled by default. Enable this option to revert to the legacy mode of reusing TCP timewait connections.<br>Only enable this after consulting with Kemp Support. |

### 3.22.4 HA Management

If using the LoadMaster for Azure product, please refer to the next section.

Parameters relating to HA Parameters that can be managed using **get** and **set** commands are detailed in the following table. Refer to the **Using get and set commands** section for the **get** and **set** commands.

| Name | Type | Range | Description |
|---|---|---|---|
| hastatus | S | Normal HA:<br>Active, Standby, Passive (all as expected).<br>Cloud HA:<br>Active, Standby, Passive (if status not yet set).<br>Cluster:<br>Active (if master), Standby (if slave), Passive (if disabled). For clusters, there is one master and all of the others are standby. | Retrieve the status of a HA or cluster unit. This is a read only parameter and cannot be set. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | If HA is not configured, **HA not configured** is returned. | |
| haif | I | | The network interface used when synchronising the configuration between the members of the HA cluster |
| hainitial | B | 0 – Disabled<br>1 – Enabled | Perform extra network checks at boot time. This may cause instability and should not be used. |
| macglobal | B | 0 - Disabled<br>1 - Enabled | By default, the LoadMaster uses an IP multicast address when sending CARP packets. Enabling this option forces the use of the IP broadcast address instead. |
| haprefered | I | 0 = No preferred host<br>1 = Prefer First HA<br>2 = Prefer Second HA | By default, neither partner in a HA cluster has priority. When a machine restarts after a switchover that machine becomes a standby. Specifying a preferred host means that when this machine restarts it will always become the active and the partner will revert to standby mode. |
| hastyle | B | 0 = legacy heart beat<br>1 = carp | By default, the system uses a version of VRRP (carp) to check the status of the partner. The system can also support the legacy Heartbeat program. This option only takes effect when both machines are rebooted |
| hatimeout | I | 1 = 3 seconds<br>2 = 6 seconds<br>3 = 9 second<br>4 = 12 seconds<br>5 = 15 seconds | The time the active must be unavailable before a switchover occurs. |
| havhid | I | 1-255 | When using multiple HA LoadMasters on the same network, this value identifies each cluster so that there are no potential unwanted |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | | interactions. |
| hawait | I | 0-200 | This is how long (in seconds) after the initial boot, before the LoadMaster becomes active. If the partner machine is running this value is ignored. This value can be changed to mitigate the time taken for some intelligent switches to detect that the LoadMaster has started and to bring up the link. |
| mcast | I | | The network interface used for multicast traffic which is used to synchronize Layer 4 and Layer 7 traffic when Inter HA Updates are enabled. |
| vmac | B | | This option creates a shared MAC address for both units. When failover occurs, the LoadMaster handles the MAC address handover too. This allows the switches to keep the MAC address and not worry about ARP caches or stale records. |
| Tcpfailover | B | 0 – Disable<br>1 – Enable | When using L4 services, enabling updates allows L4 connection maintenance across a HA switchover. This option is ignored for L7 services.<br>This parameter is now deprecated and has been replaced with the **hal4update** parameter. |
| hal4update | B | 0 – Disable<br>1 – Enable | When using L4 services, enabling updates allows L4 connection maintenance across a HA switchover. This option is ignored for L7 services. |
| cookieupdate | B | 0 – Disable<br>1 – Enable | When using L7 services, enabling this option allows sharing of persistency information between HA partners. If a HA switchover occurs, the persistency information will then not be lost. Enabling this option can have a significant performance impact.<br>This parameter is now deprecated and has been replaced with the **hal7update** parameter. |
| hal7update | B | 0 – Disable | When using L7 services, enabling this option |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | 1 – Enable | allows sharing of persistency information between HA partners. If a HA switchover occurs, the persistency information will then not be lost. Enabling this option can have a significant performance impact. |
| finalpersist | I | 0, 60-86400 | When a Real Server is disabled, the sessions persisting on that Real Server continue to be served until the Drain Time has expired or until no more sessions are being handled by the Real Server. No new sessions will be handled by the Real Server. |
| hamode | I | 0 – HA mode disabled<br>1 – HA 1 mode<br>2 – HA 2 mode<br>3 – System is using cloud HA<br>4 – System is in a cluster | Specify the HA mode. If only using a single LoadMaster, use Non-HA Mode. In non-cloud HA mode, one LoadMaster must be specified as the first and another as second. HA will not work if both LoadMasters are specified the same.<br>HA enables two physical or virtual LoadMasters to become one logical device. Only one of these units is active and handling traffic at any one time (HA 1 mode) while the other is a hot standby (passive - HA 2 mode). |
| hacheck | B | 0 - Disable<br>1 - Enable | Enable HA health checking. At least one interface must be enabled. |
| halinkfailreboot | B | 0 - Disable<br>1 - Enable | Enables LoadMaster to reboot if there is a link failure. |

Simply changing the HA mode does not switch between non-HA and HA. The partner and Virtual IP (VIP) Addresses also need to be set and a reboot is needed before the system is fully switched over. For instructions on how to set up HA using the RESTful API, refer to the **Azure HA Parameters** section.

After changing the **hastyle** or **hamode** a reboot is required for the changes to take effect.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

### 3.22.5 Cloud HA Parameters

You can retrieve the HA parameters for a cloud LoadMaster by running the **getCloudHaParams** command:

**https://<LoadMasterIPAddress>/access/getCloudHaParams**

You can set the cloud HA mode by running the following command:

**https://<LoadMasterIPAddress>/access/setcloudhamode?hamode=<first/second/single>**

Setting the **hamode** to **single**, disables HA (the LoadMaster is treated as a single unit).

You can set the cloud HA parameters by running the following command:

**https://<LoadMasterIPAddress>/access/setcloudhaparam?partner=<PartnerHostNameOrIPAddress>**

| Name | Type | Range | Additional Information |
|---|---|---|---|
| partner | S | Must be a valid IP address | Specify the host name or IP address of the HA partner unit. |
| hcp | I | Must be a valid port value | Set the port to run the health check over. The port must be the same on both the active and standby unit for HA to function correctly. |
| haprefered | B | 0 – No Preferred Host<br>1 – Prefer First | There are two possible values to set:<br>0 - No Preferred Host: Each unit takes over when the other unit fails. No switchover is performed when the partner is restarted.<br>1 - Prefer First: The active unit always takes over. This is the default option. |
| hcai | B | 0 - Disabled<br>1 - Enabled | When this option is enabled, the health check listens on all interfaces. This is required when using a multi-arm configuration. If this is disabled, the health check listens on the primary eth0 address (this is the default behavior). |

For details on API commands specific to different cloud platforms, refer to the sections below.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

#### 3.22.5.1 Azure HA Parameters

> These commands are only relevant to the LoadMasters running in Azure.

The Azure HA mode can be set by running the following command:

**https://<LoadMasterIPAddress>/access/azurehamode?hamode=<first/second/single>**

The Azure HA parameters can be set by running the following command:

**https://<LoadMasterIPAddress>/access/azurehaparam?partner=<PartnerHostNameOrIPAddress>&hcp=<HealthCheckPort>**

The parameters that can be set using the **azurehaparam** command are the same as those set using the **setcloudhaparam** command. For details about these parameters, refer to the **Cloud HA Parameters** section.

The Azure HA parameters can be retrieved by using the following command:

**https://<LoadMasterIPAddress>/access/getazurehaparams?**

#### 3.22.5.2 AWS HA Parameters

> These commands are only relevant to LoadMasters running in AWS.

The AWS HA mode can be set by running the following command:

**https://<LoadMasterIPAddress>/access/awshamode?hamode=<first/second/single>**

The AWS HA parameters can be set by running the following command:

**https://<LoadMasterIPAddress>/access/awshaparam?partner=<PartnerHostNameOrIPAddress>&hcp=<HealthCheckPort>**

| Name | Type | Range | Additional Information |
|---|---|---|---|
| partner | S | Must be a valid IP address | Specify the host name or IP address of the HA partner unit. |
| hcp | I | Must be a valid port value | Set the port over which the health check will be run. The port must be the same on both the active and standby unit for HA to function correctly. |
| haprefered | B | 0 – No Preferred | There are two possible values to set:<br>0 - No Preferred Host: Each unit takes over when the other unit |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | |
|---|---|---|---|
| | | Host | fails. No switchover is performed when the partner is restarted. |
| | | 1 – Prefer First | 1 - Prefer First: The HA1 (active) unit always takes over. This is the default option. |
| hcai | B | 0 - Disabled<br>1 - Enabled | When this option is enabled, the health check listens on all interfaces. This is required when using a multi-arm configuration. If this is disabled, the health check listens on the primary eth0 address (this is the default behavior). |

The AWS HA parameters can be retrieved by using the following command:

**https://<LoadMasterIPAddress>/access/getawshaparams?**

Example output for the **getawshaparams** command is below:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<Response stat="200" code="ok">
<Success><Data><AwsHA>
<HaMode>master</HaMode>
<HaPrefered>0</HaPrefered>
<Partner>172.18.0.5</Partner>
<Port>8444</Port>
</AwsHA>
</Data>
</Success>
</Response>
```

### 3.22.6 SDN Configuration

#### 3.22.6.1 Add an SDN Controller

To add a new SDN controller to the LoadMaster, run the command below:

**https://<LoadMasterIPAddress>/access/addsdncontroller?ipv4=<IPv4Address>&port=<SDNControllerPort>&https=<0/1>&user=<UserToAccessSDNControllerAPI>&password=<PasswordForSDNUser>&clid=<ClusterID>**

The parameters used in this command are described below:

| Name | Mandatory | Type | Default | Range | Additional Information |
|---|---|---|---|---|---|
| ipv4 | Yes | S | <unset> | Valid IPv4 | The IPv4 address of the SDN controller. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | | |
|---|---|---|---|---|---|
| | | | | address range | |
| port | Yes | I | <unset> | Valid port range | The port of the SDN controller. |
| https | No | B | 0 - HTTP | 0 - HTTP<br>1 - HTTPS | The HTTP method to use. |
| user | No | S | <unset> | | The username to be used to access the SDN controller RESTful API. |
| password | No | S | <unset> | | The password to be used to access the SDN controller RESTful API. |
| clid | No | I | <unset> | 1 - 6 | The cluster ID for the new SDN controller. If a number is specified, the SDN controller will be added to the cluster with the relevant ID number. The cluster with the ID number specified must already exist.<br>If a number is not specified, the SDN controller will be added to a new cluster. |

**Expected Output**

```
<Response stat="200" code="ok">
<Success>Command completed ok</Success>
</Response>
```

### 3.22.6.2 Modify an SDN Controller

To modify an existing SDN controller, run the command below:

**https://<LoadMasterIPAddress>/access/modsdncontroller?cid=<ControllerID>&ipv4=<IPv4Address>&port=<SDNControllerPort>&https=<0/1>&user=<UserToAccessSDNControllerAPI>&password=<PasswordForSDNUser>&clid=<ClusterID>**

The parameters used in this command are described below:

| Name | Mandatory | Type | Default | Range | Additional Information |
|---|---|---|---|---|---|


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | | |
|---|---|---|---|---|---|
| cid | Yes | I | Auto incrementing number | | The ID of the controller to be modified. To get the controller ID, run the **getsdncontroller** command. |
| ipv4 | No | S | <unset> | Valid IPv4 address range | The IPv4 address of the SDN controller. |
| port | No | I | <unset> | Valid port range | The port of the SDN controller. |
| https | No | B | 0 - HTTP | 0 - HTTP<br>1 - HTTPS | The HTTP method to use. |
| user | No | S | <unset> | | The username to be used to access the SDN controller RESTful API. |
| password | No | S | <unset> | | The password to be used to access the SDN controller RESTful API. |
| clid | No | I | <unset> | 1 - 6 | The cluster ID for the new SDN controller. If a number is specified, the SDN controller will be added to the cluster with the relevant ID number. The cluster with the ID number specified must already exist.<br>If a number is not specified, the SDN controller will be added to a new cluster. |

**Expected Output**

```
<Response stat="200" code="ok">
<Success>
<Data>
<controllers>
<cluster id="2"/>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
<cluster id="3"/>
<cluster id="5"/>
<cluster id="6"/>
<cluster id="7"/>
<cluster id="8"/>
<cluster id="9"/>
<cluster id="10"/>
<cluster id="11"/>
<cluster id="12"/>
<cluster id="13"/>
<cluster id="14"/>
<cluster id="15"/>
<cluster id="16"/>
<cluster id="17"/>
<cluster id="18">
<controller id="30">
<ipv4>172.16.0.6</ipv4>
<port>8443</port>
<https>yes</https>
<user>sdn</user>
<password>*****</password>
</controller>
</cluster>
<cluster id="19">
<controller id="31">
<ipv4>172.16.0.8</ipv4>
<port>8443</port>
<https>yes</https>
<user>sdn</user>
<password>*****</password>
</controller>
</cluster>
<cluster id="20">
<controller id="32">
<ipv4>172.16.0.8</ipv4>
<port>8443</port>
<https>no</https>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
<user/>
<password/>
</controller>
</cluster>
</controllers>
</Data>
</Success>
</Response>
```

#### 3.22.6.3 Delete an SDN Controller

To delete an SDN controller, run the command below:

**https://<LoadMasterIPAddress>/access/delsdncontroller?cid=<ControllerID>&clid=<ClusterID>**

Either the Controller ID or the Cluster ID must be specified. The Controller ID and Cluster ID can be found by running the **getsdncontroller** command. For more information, refer to the **Show the Existing SDN Controllers** section.

**Expected Output**

```
<Response stat="200" code="ok">
<Success>Command completed ok</Success>
</Response>
```

#### 3.22.6.4 Show the Existing SDN Controllers

To display a list of the SDN controllers that currently exist on the LoadMaster, run the command below:

**https://<LoadMasterIPAddress>/access/getsdncontroller**

An example of the returned output is below:

```
<Response stat="200" code="ok">
<Success>
<Data>
<controllers>
<cluster id="2">
<controller id="29">
<ipv4>172.16.0.6</ipv4>
<port>8443</port>
<https>yes</https>
<user>sdn</user>
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

```
<password>*****</password>
</controller>
</cluster>
<cluster id="3"/>
<cluster id="5"/>
<cluster id="6"/>
<cluster id="7"/>
<cluster id="8"/>
<cluster id="9"/>
<cluster id="10"/>
<cluster id="11"/>
<cluster id="12"/>
<cluster id="13"/>
<cluster id="14"/>
<cluster id="15"/>
<cluster id="16"/>
<cluster id="17"/>
</controllers>
</Data>
</Success>
</Response>
```

The parameters that appear in the output are explained below:

- **Cluster ID:** The unique ID of the cluster that the SDN controller is a member of.

  > Any empty cluster parameter sections relate to clusters that were previously added but were later removed. Each time a new cluster is added it gets assigned a new ID number.

- **Controller ID:** The ID of the SDN controller.
- **IPv4:** The IPv4 address of the SDN controller.
- **Port:** The port of the SDN controller WUI.
- **HTTPS:** Displays whether HTTPS (**yes**) or HTTP (**no**) is used to access the SDN controller.
- **User:** The username to be used to access the SDN controller.
- **Password:** The password of the user to be used to access the SDN controller.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

## 3.23 Network Telemetry

A number of parameters relating to network telemetry can be retrieved and configured using the **get** and **set** commands. Refer to the table below for details about these parameters:

| Name | Type | Default | Range | Additional Information |
|---|---|---|---|---|
| TelemetryServer | S | <unset> | | Define the destination IP address or Fully Qualified Domain Name (FQDN) and port number of your IPFIX collector (for example, **1.1.1.1:2055** or **collector.local:3000**). The IPFIX export runs over the UDP protocol and you must ensure that the collector is reachable over the network from the LoadMaster. |
| TelemetryActiveTimeout | I | 300 | 10 - 6000 | The global active timeout value. |
| TelemetryInactiveTimeout | I | 30 | 1 - 59 | The global inactive timeout value. |
| TelemetryOptArp | B | 1 - Enabled | 0 - Disabled<br>1 - Enabled | Specify whether or not to collect ARP values. |
| TelemetryOptDhcp | B | 1 - Enabled | 0 - Disabled<br>1 - Enabled | Specify whether or not to collect DHCP values. |
| TelemetryOptDns | B | 1 - Enabled | 0 - Disabled | Specify whether or not to collect DNS values. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | 1 - Enabled | |
| TelemetryOptHttp | B | 1 - Enabled | 0 - Disabled<br>1 - Enabled | Specify whether or not to collect HTTP values. |
| TelemetryOptMail | B | 1 - Enabled | 0 - Disabled<br>1 - Enabled | Specify whether or not to collect email values. |
| TelemetryOptNbar2 | B | 1 - Enabled | 0 - Disabled<br>1 - Enabled | Specify whether or not to collect NBAR2 values. |
| TelemetryOptSamba | B | 1 - Enabled | 0 - Disabled<br>1 - Enabled | Specify whether or not to collect Samba values. |
| TelemetryOptExtendedVoip | B | 1 - Enabled | 0 - Disabled<br>1 - Enabled | Specify whether or not to collect VoIP values. |
| TelemetryOptMsSql | B | 1 - Enabled | 0 - Disabled<br>1 - Enabled | Specify whether or not to collect MSSQL values. |
| TelemetryOptPostgres | B | 1 - Enabled | 0 - Disabled<br>1 - Enabled | Specify whether or not to collect PostgresSQL values. |
| TelemetryOptMySql | B | 1 - | 0 - | Specify whether or not |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | Enabled | Disabled<br>1 - Enabled | to collect MySQL values. |
| TelemetryOptNpm | B | 1 - Enabled | 0 - Disabled<br>1 - Enabled | Specify whether or not to collect NPM values. |
| TelemetryOptExtendedNpm | B | 1 - Enabled | 0 - Disabled<br>1 - Enabled | Specify whether or not to collect Extended NPM values. |
| TelemetryOptVxlan | B | 1 - Enabled | 0 - Disabled<br>1 - Enabled | Specify whether or not to collect VXLAN values. |

To check if network telemetry monitoring is enabled or disabled on all interfaces, run the **showtelemetry** command with no parameters. For example:

**/access/showtelemetry?**

To check if network telemetry monitoring is enabled or disabled on a specific interface, run the **showtelemetry** command with the **interface** parameter. For example:

**/access/showtelemetry?interface=0**

To enable or disable network telemetry monitoring on a particular interface, run the **enabletelemetry** command. For example:

**/access/enabletelemetry?interface=<InterfaceID>&enable=<0/1>**

Valid values for **enable** are:

- 0 - Disabled
- 1 - Enabled


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

## 3.24 Setting Up HA using the RESTful API

The two sections below provide step-by-step instructions on how to set up HA using the RESTful API on a regular LoadMaster, and a LoadMaster for Azure:

### 3.24.1 Set up HA on a Regular LoadMaster using RESTful API

The example commands that are needed to set up HA using the RESTful API on a regular LoadMaster are below:

1. Set device 1 to HA1:

**https://192.168.1.1/access/set?param=hamode&value=1**

2. Reboot HA1:

**https://192.168.1.1/access/reboot?**

3. Set HA1's partner's address (HA2 address):

**https://192.168.1.1/access/modiface?interface=0&PartnerIPAddress=192.168.1.2**

4. Set the shared IP address for the HA pair:

**https://192.168.1.1/access/modiface?interface=0&SharedIPAddress=192.168.1.10**

5. Set HA2 to secondary:

**https://192.168.1.2/access/set?param=hamode&value=2**

6. Reboot HA2:

**https://192.168.1.2/access/reboot?**

7. Set HA2's partner's address (HA1's address):

**https://192.168.1.2/access/modiface?interface=0&partner=192.168.1.1**

8. Set the shared IP address for the HA pair:

**https://192.168.1.2/access/modiface?interface=0&shared=192.168.1.10**

> Commands such as **reboot** take several seconds for the LoadMaster to complete. If scripting, please allow for a proper delay after the **reboot** command.

To remove HA, use the commands below:

1. Set to non-HA:

**https://192.168.1.1/access/set?param=hamode&value=0**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2. Reboot:

**https://192.168.1.1/access/reboot?**

### 3.24.2 Set up HA on a LoadMaster for Azure using RESTful API

The example commands that can be used to set up HA on a LoadMaster for Azure using RESTful API are below:

Set the active unit to first HA mode:

**https://192.168.1.1/access/azurehamode?hamode=first**

Set the HA parameters (partner address and health check port) for the active unit:

**https://192.168.1.1/access/azurehaparam?partner=192.168.1.2&hcp=8444**

Set the standby unit to second HA mode:

**https://192.168.1.2/access/azurehamode?hamode=second**

Set the HA parameters (partner address and health check port) for the standby:

**https://192.168.1.2/access/azurehaparam?partner=192.168.1.1&hcp=8444**

To remove HA, use the commands below:

**https://192.168.1.1/access/azurehamode?hamode=single**
**https://192.168.1.2/access/azurehamode?hamode=single**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# 4 Scripting Examples with the LoadMaster RESTful API

The LoadMaster RESTful API can be used in conjunction with many scripting methods and applications to allow users and applications to directly access the LoadMaster.

Refer to the RESTful API Programmers Guide, Technical Note for some detailed examples of how the RESTful API can be used.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# 5 List All API Commands and get/set Parameters

A number of parameters can be retrieved and set using the **get** and **set** commands. For more details on how to get the list of parameters, refer to the section **List All API Commands and get/set Parameters**.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# References

Unless otherwise specified, the following documents can be found at http://kemptechnologies.com/documentation.

**WUI, Configuration Guide**

**Kemp LoadMaster, Product Overview**

**SSL Accelerated Services, Feature Description**

**GEO, Feature Description**

**RESTful API Programmers Guide, Technical Note**

**Licensing, Feature Description**

**CLI, Interface Description**

**LoadMaster Clustering, Feature Description**

**Custom Authentication Form, Technical Note**

**User Management, Feature Description**

**Content Rules, Feature Description**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# Last Updated Date

This document was last updated on 27 July 2023.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.