SLAnalyzer User Guide

9.0.1.15

Copyright 2014-2023 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Table of Contents

Description 18

Supported Platforms 18

Prerequisites 18

Installation 20

- Download manager 20
- Manual Installation 20

Uninstalling SLAnalyzer 22

AutoUpdate 23

Log File Types 24

Command Line Parameters 25

Support for compressed files (ZIP) 26

Support for large log files 27

Support for open log files 30

File Menu 31

- Open 32
  - Log File Features 32
    - Colorization 32
    - Column Move/Re-order 33
    - Column Sort 34
    - Comments 35
    - Context Menu for XML and JSON windows 37
      - Copy 37
      - Find 38
      - Expand All 39
      - Collapse All 39
      - View Line 40
    - Context Menu for reports/logs window 41
      - Copy 41
      - Find 44
      - Jumping to a specific entry/line 46
      - Show 47

View Line 48
Filters 49
Selecting a filter 50
Activating a Filter 51
Creating a filter 52
Manually entering a filter 55
Resetting the filter 57
Supported log/report file types 58
Opening a SLAnalyzer report 58
Opening a Novell Client credential provider log 58
Opening a Novell SecretStore client debug log 59
Opening a SecureLogin Debug log 59
Opening a Client Login Extension Emergency Access Debug Log 60
Opening a Desktop Automation Services debug log 60
Opening an NDS trace file 61
Opening a SSPR Support Bundle 61
Opening a AAF Database 64
Opening a AAF Debug Log 64
Opening a text file with the Generic log reader 65
Opening a Comma-Separated Values (CSV) file 66
Opening a JSON formatted file (JSON) 67
Opening an XML formatted file (XML) 67
Opening a HyperText Markup formatted file (HTM/HTML/URL) 68
Opening a ZEN message log 68
Opening a HAR log file 69
Save 75
Close 76
Exit 77
Analyze Menu 78
Configuration Report Window 79
Saving report information 80
Saving report as Report Format (*.txt) 81

Saving report as XML Format (*.xml) 81
XML report formatting 82
Available Reports 84
All 84
My Computer 85
ARP table 86
My Computer/Available Resources 86
My Computer/Debug Logging 87
My Computer/DNS Table 88
My Computer/Internet Browsers 88
My Computer/IP Configuration 89
My Computer/Group Policy 89
My Computer/TCP port table 90
My Computer/Registry 90
My Computer/Routing table 91
My Computer/Windows Event Logs 91
AAF 92
AD 93
CLE 94
LDAP 96
Novell Client 97
SecretStore 98
SecureLogin 99
Optional SecureLogin reports 100
Installation 100
TLaunch 100
Smart Card 101
Tools Menu 102
Debugging Options 105
Debug scope 105
User level debugging 106
Machine level debugging 107

Debug window components 108
Change button 108
Reset button 108
Debug Log Path 109
SecureLogin Debug module box 110
Additional Debugging options 111
LDAP Auth 111
Virtual Channel 111
Novell Client 111
Emergency Access 111
SecretStore 111
NMAS 111
DAS 111
AAF 112
SecureWorkstation 112
PCProx 112
Client Login Extension 112
Apply button 113
Rename existing logs checkbox 113
Debug Console 114
Filtering debug data 114
File Browser 115
View Registry Keys 116
Registry key detail 116
Registry Keys by Product 117
Registry Key by Product Details 117
Find 118
Select item Forward/Back 118
Group Policy 119
Generate HTML Report 120
Generate Report 121
Force Update 122

Common Appliance Framework 123
Reset Appliance Certificate 123
Get Registration/zypper Logs 123
Generate Support Config 123
Update Appliance 124
Verify Channel Connectivity 125
Registration 126
Check Registration 126
Clear Registration 127
New Registration 127
Get zypper Information 128
Capture packet trace 129
Self Service Password Reset 131
SSPR REST Client 132
REST Client Window components 132
REST URI 133
Authentication Credentials 133
REST Call Selection box 133
Parameters button 133
REST API Description 134
Request window 134
Reply window 134
Execute button 134
Links button 135
Exit button 135
Profile data 135
REST Calls 136
Forgotten Password 136
Get Challenge Questions 155
Post Challenge Answers 157
Post Verify Responses 161
Delete Challenge Answers 164

Post Check Password 166
Get Health 168
Get Profile 171
Post Profile 173
Parameters 173
Get Random Password 176
Post Random Password 178
Post Set Password 180
Get Statistics 183
Get Status 185
Post Verify OTP 187
SSPR Quick Links 194
Open with: 194
SSPR Rights Validator 195
Window components: 196
Data table: 196
Report window: 197
AD and eDirectory Data table menu: 198
LDAP and LDAPS Data table menu: 198
Data table menu items: 198
Read single attribute value 200
Read all attribute values 201
Write single attribute value: 202
Write all attributes: 204
Clear single attribute: 205
Get Effective Rights: 206
SSL Connection Failure 207
Get Server Info: 209
Change User Password: 210
Reset Password: 211
AD Validator (using Microsoft client) 212
eDirectory Validator (Using Novell/OES client) 213

LDAP/LDAPS validator 214
Command 215
Get App Version 215
Clear Local Responses 215
Lock Configuration 215
Unlock Configuration 216
Set Configuration Password 216
Delete Configuration 217
Advanced Authentication 218
REST Client 219
AAF REST Client Window components 219
REST URI 221
Tenant 221
Authentication Credentials 221
REST Call Selection box 221
Parameters button 223
Enable Profiling checkbox 223
Advanced checkbox 224
Request window 224
Reply window 224
Execute button 224
Links button 224
Exit button 226
Status Message 226
Profile data 226
Packet Data Window 227
View Line: 228
Copy/Paste: 228
Automated Processes: 229
Check Debug Logging State 230
Generate Support Bundle: 231
Enroll 235

Logon 247
Delete User(s) 251
Server Status 253
Lookup User 254
List of Users 255
Test Device Manager Plug-in 258
Build enrolled methods database 266
Manage OTP Tokens 269
Show Shared Template Info 272
Register Method for User 273
Show Override Auto Enrollment 275
Manage Radius Clients 276
Advanced 279
Assign User Template 281
Create Endpoint Session 283
Create Event 284
Create OTP Token 285
Create User Template with enroll data 286
Create User Template without enroll data 286
Delete All Records of OSLogon Data 286
Delete Event 287
Delete Login Session 288
Delete OTP Token 289
Delete Password Record Only 290
Delete User 291
Delete User Templatee 292
Destroy Endpoint 292
Destroy Endpoint Session 294
Destroy Enroll 295
Destroy Logon Process 296
Do Enroll 297
Do Logon 298

Do Method call 304
Enroll 306
Enroll new TOTP 307
Enroll OTP Token 308
Generate Cookie Value 309
Generate Ticket Value 310
Get Authentication Chains 311
Get Endpoint Session Info 314
Get Event by Event ID 315
Get Full Server Status 318
Get OTP Token 319
Get OTP Tokens with Pagenation 320
Get Server Status 321
Get User Templatee 322
List of Events 324
List of Users 325
Load Chain Image 326
Logon 327
Logon by Basic Auth 329
Logon Domains Lookup 330
Logon Next 331
Lookup User 332
Modify User Data 333
Read All Custom Messages for Category 334
Read All Records of OSLogon Data 335
Read Available Chains 336
Read Categories 337
Read Custom Messages for Category and Key 338
Read Effective Policies of User 339
Read Effective Policies of Endpoint 345
Read Endpoint Info 351
Read Info about Component of Endpont Policy 354

Read Info About Component of User Policy 356
Read Login Session Information 358
Register Logon Domains for the Current Tenant 359
Register New Endpoint 360
Packet Data 365
Remove Already Enrolled TOTP Template 366
Revoke OTP Token 367
Search for Endpoint 368
Update Endpoint Info 369
Update Event 371
Update User Template 372
Verify Cookie Value 373
Examples: 374
Create Session 375
Get Session Info 377
Get Server Status 377
Get Full Server Status 378
Delete Session 378
Get Authentication Chains 379
Logon 381
Read Login Session Information 382
Delete Login Session Information 382
Read User Data 383
Modify User Data 383
Delete User Data 383
Enroll 384
Delete Enroll 384
Get User Template 384
Create User Template 385
Assign User Template 385
Update User Template 385
Delete User Template 385

Risk Services 387
Remote Admin 391
Edit Chains 392
Edit Endpoints 393
Edit Events 394
Edit User Roles 395
View enrollment data 396
By User 397
By Method 398
View license data 399
User license consumption 400
Initialize default event/chains 401
Initialize default endpoints 402
Repair Cached Groups 403
Gather Server Stats 405
Monitor Server Performance 406
Find PostGres User 407
Add Root CA Certificate 408
Replace OSP Certificates 409
Reset Local Admin Pwd 412
OSP / OAuth2 413
Create OAuth2 Event 414
Enable OAuth services 418
SLAnalyzer OAuth2 settings 419
Navigating the SLAnalyzer OAuth2 Logon Test Page 421
Logon and obtaining an access token 424
Obtaining attribute data: 425
Refreshing the access token 426
Logon through Resource Owner Password Credentials Grant 428
Redirecting to an external resource 429
Get OpenId Config 430
Get SAML metadata 431

Check AAuth connectivity 432
SaaS 433
CBA 433
Gather CBA Stats 433
Start CBA 433
Stop CBA 433
Debug Settings 433
Get Install Log 434
Get Debug Logs 434
Azure 435
Prerequisites – Creating a service principal 436
Prerequisites – Granting access to a service principal for Azure access 439
Prerequisites – Granting access to a service principal for Azure AD access 442
Packet Data window 449
Gaining access to Azure 450
Azure AD Login 451
Azure OAuth2 Client Login 453
SecureLogin AE Login 455
Azure AD functions 457
Get AD Application Info 458
Azure functions 461
Get Subscriptions 462
Get Resources 463
Get Kubernetes Info 465
Get Kubernetes Name Space 467
Get Kubernetes Pods 468
Get Kubernetes Logs 469
Initalize for Kubernetes 470
KubeCtl terminal 471
Kubernetes Node Explorer 474
Options menu 476
View menu 476

Details view 477
Small Icons view 477
List view 478
Tile view (default view) 478
Node/Container/Directory functions 479
File functions 480
Get File 481
Send File 481
Send a Command 481
Send REST Get Request 481
Viewing Kubernetes Name Space Nodes 482
Nodes found in aks-command name space 483
Nodes found in kube-system name space 484
Product AKS Node (dogaafns) 485
Troubleshooting Azure connectivity 486
Login failure due to wrong client ID, secret, or tenant information. 486
Selecting a resource group and then selecting a cluster object not in that resource group 486
Selecting the resource group, cluster, but not the correct name space 486
Cannot get subscription information 487
Azure error during login to AD in Azure – No reply address 487
Azure error during login to AD in Azure – Misconfigured application 488
Identity Manager 489
Getting IDM information 489
Rest Client 490
Window components: 491
URI 491
User 491
API List 491
API Info button 491
Go button 491
API Description 491
Gather Support Bundle 492

LDAP Browser 493
LDAP Login Settings 494
LDAP Search Criteria 495
LDAP Connection Parameters 496
LDAP Object window 496
LDAP Attribute window 496
Profile data 496
Viewing LDAP attribute data 497
Building a list of LDAP users 498
LDAP Browser examples 499
Example 1: 499
Example 2: 501
JSON Console 502
SSH/SCP 504
Explorer 505
SSH Terminal 509
Download File 510
Upload File 511
Restart Host 512
SQL Browser 513
Server Type 514
SQL server list 514
Discover button 514
Server 514
Port 514
Database 514
Database User Credentials 514
Username 515
Password 515
Connect button 515
Status box 515
Query 515

Execute button 515
Profile data 515
MSSQL 516
Connecting to an MSSQL database 516
Connecting to an SSPR database on a non-standard port 517
MSSQL query examples 518
MySQL 520
Connecting to a MySQL server 520
MySQL Query example 522
PostgreSQL 523
Connecting to a PostgreSQL server 523
PostgreSQL command examples 526
Handling Bytea (Byte Array) fields. 529
Using Hex value 529
Using the escaped value 530
Steps to obtain PostgreSQL database user on AAF server 532
Web Browser 534
Developer tools 535
Configure SLAnalyzer 537
Changing the default report folder 538
Report Filter Type Definitions 539
Built-In Filters 540
User Defined Filters 541
Disabling a filter 542
Editing a filter 542
Deleting a Filter 543
Creating a new filter 544
Help Menu 545
Error and Return Codes 546
OpenText Internal Resources 547
3rd Party Tools 548
Product Links 549

About SLAnalyzer 550
Sample Reports 551
Sample Computer Information report 552
Sample Group Policy report 558
Sample Registry report 560
Sample Logging report 567
Sample SecureLogin report 568
Sample Installation report (SecureLogin) 579
Sample Tlaunch report 581
Sample eDirectory with Novell Client report 582
Sample LDAP report 584
Sample AD report 586
Sample LDAP SecretStore Report 587
Sample CLE report 588
Sample AAF report 599
Sample LDAP Server Information (Active Directory) 601
Sample LDAP Server Information (eDirectory) 603
Appendix - Figures 606

Description

SLAnalyzer is a tool developed by Open Text technical services to assist in the troubleshooting of support related issues. It includes a log reader which parses text-based log files. A tools menu that provides a REST client for SSPR and AAF, LDAP browser, a listing of registry keys used by several different products, and a growing number of other features. It also includes an analysis report engine for several different configurations and products.

Supported Platforms

SLAnalyzer has been tested on 32 bit and 64 bit systems. It should function on any windows platform supported by Microsoft. This would include:

- Windows Vista
- Windows 7
- Windows 8
- Windows 10
- Windows 2003
- Windows 2008
- Windows 2008 R2
- Windows 2012

Note: There is a special version of SLAnalyzer to generate analysis reports for Windows XP and SecureLogin 7 clients. Contact a support individual if this version is needed. The SecureLogin 7 version is not being updated to include newer features and is only being used to generate reports for support related issues.

Prerequisites

For SLAnalyzer to run you must install the Microsoft .Net 4.5 libraries.
https://www.microsoft.com/en-us/download/details.aspx?id=30653

Note: Executing SLAnalyzer on a workstation where the .Net 4.5 libraries are not installed will result in the below message being displayed to the user.

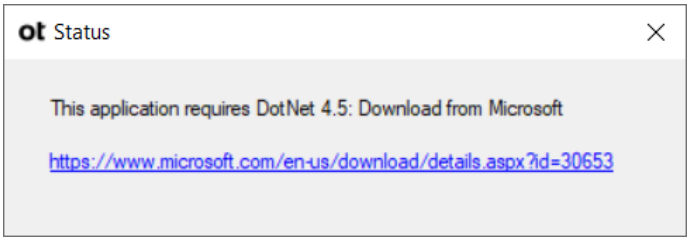
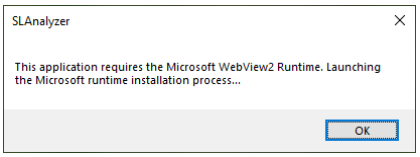
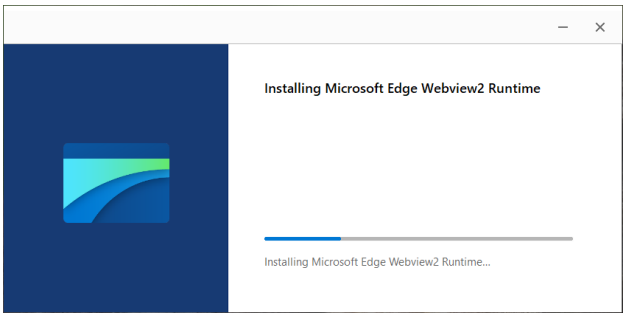
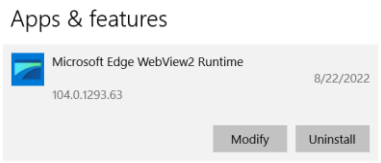


Figure 1 - Initialization error

Starting with SLAnalyzer version 9.0.1.0 the CEF open-source libraries have been replaced with the Microsoft WebView2 libraries. When the SLAnalyzer application is launched it will check for the presence of the WebView2 runtime libraries. If not present, then the user will be prompted to install.







Failure to install the Microsoft WebView2 runtime library will result in the embedded web browser not displaying web content. Only a blank web browser screen will be displayed.

The webview2 runtime library can be downloaded for offline installation of SLAnalyzer from:
[WebView2 - Microsoft Edge Developer]

Installation

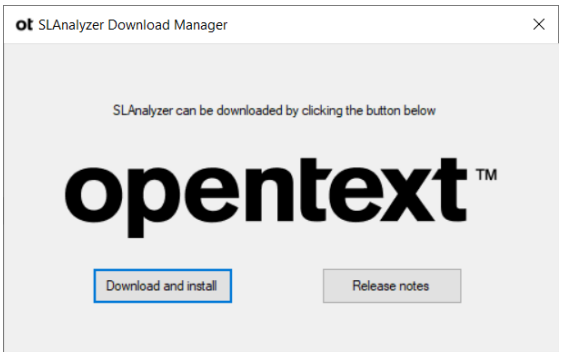
Prior to version 9.0 of SLAnalyzer, the complete tool was provided in a single binary. But with the inclusion of additional libraries and features it became necessary to implement an installation program.

SLAnalyzer now requires the application be installed through the Windows installer.

Download manager

A new download manager controls the download and installation of the SLAnalyzer application.

The SLAnalyzer download manager is located on the FTP server at:
https://ftp.novell.com/pub/SLAnalyzer/SLAnalyzer.exe



Click the Download and install button to install the latest version of SLAnalyzer. Click on the Release notes button to view the latest update information.

After clicking Download and install, the download manager will download the new version of the SLAnalyzer application. Once the download is completed it will then launch the installer.

Note that the downloaded application will be located in the users download folder. The file is extracted to a folder named <downloads>\SLAnalyzerInstall. Then the setup.exe program is executed to perform the installation.

Manual Installation

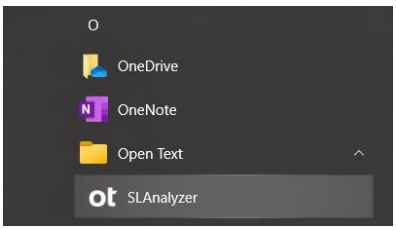
Download location: https://ftp.novell.com/pub/SLAnalyzer/SLAnalyzerChromium.new
After download, rename the file to .zip and extract to a temporary folder.
Run setup.exe from the temporary folder to install.

Note that to apply updates the SLAnalyzer application will need to be downloaded and installed from the same manual location. An attempt to apply updates to a different location will result in an error message indicating that the update cannot be installed. The error will show the location of the original installation folder. SLAnalyzer could also be uninstalled and then installed again from the desired location.

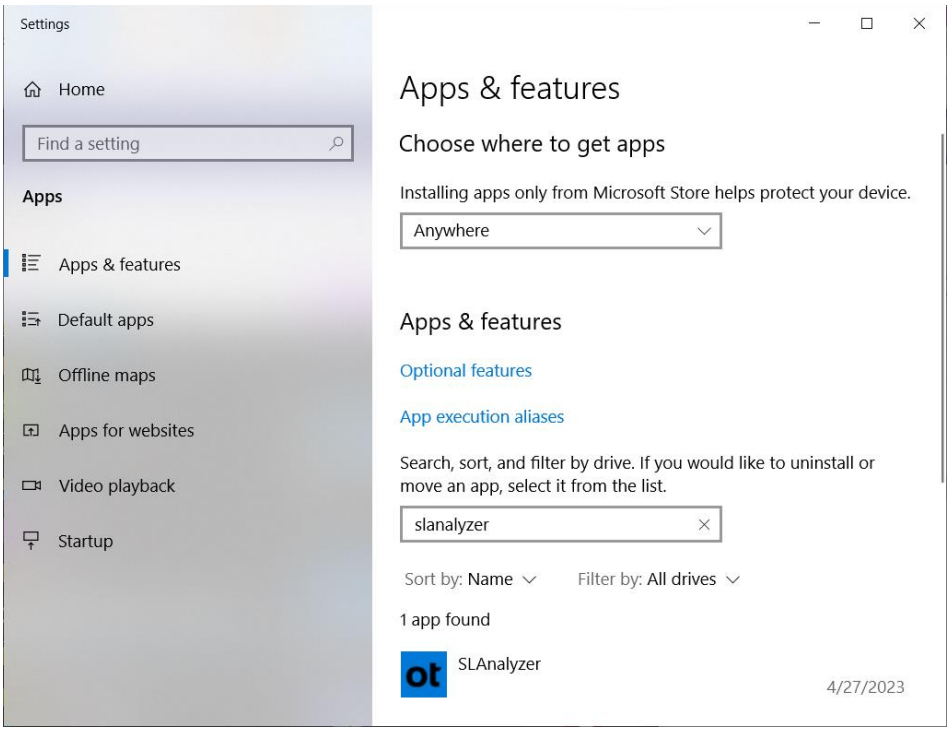
User documentation can be accessed from the help menu in the application or from:
https://ftp.novell.com/pub/SLAnalyzer/SLAnalyzer%20User%20Guide.pdf

Release notes can be viewed from the download manager or from:
https://ftp.novell.com/pub/SLAnalyzer/ReleaseNotes.rtf

After installation, the SLAnalyzer application will be launched and be ready for use.
The application can be found under Open Text -> SLAnalyzer



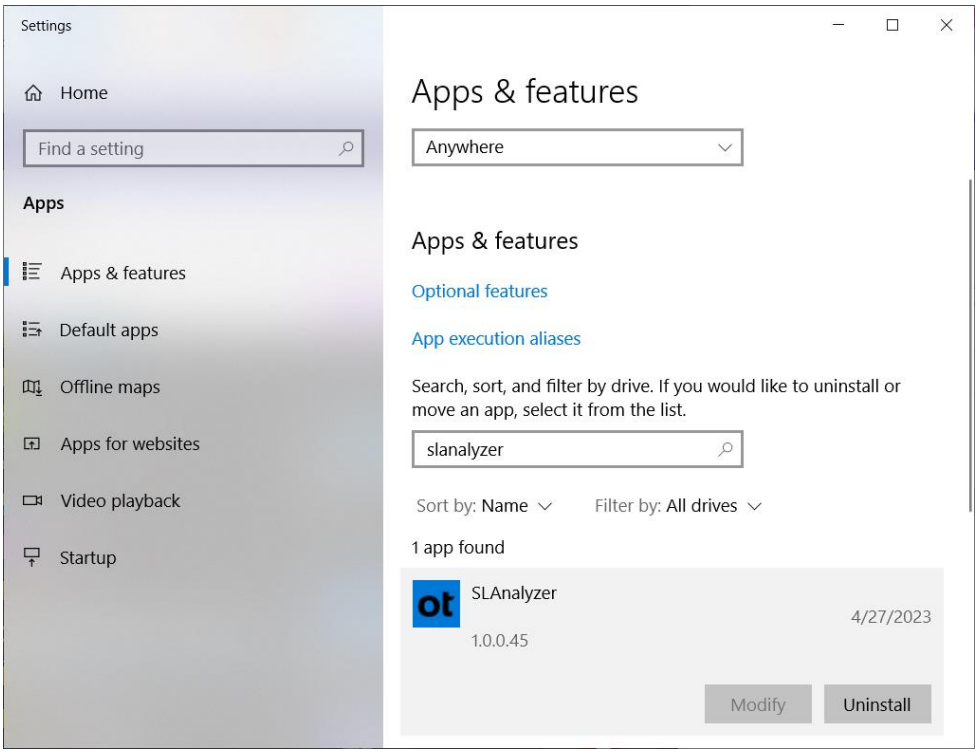
SLAnalyzer will now be seen under apps and features as an installed application.



Uninstalling SLAnalyzer

Open Apps and Features by clicking the left mouse button over the Windows Start button. Then select the top menu item “Apps and Features”.

Scroll through the list of applications and find SLAnalyzer or type in SLAnalyzer into the search bar. Click on SLAnalyzer and then choose the option Uninstall.



AutoUpdate

The first time SLAnalyzer is executed each day, the application will check for updates. If a newer version of SLAnalyzer is available for download, it will prompt the user if they would like to perform the update.

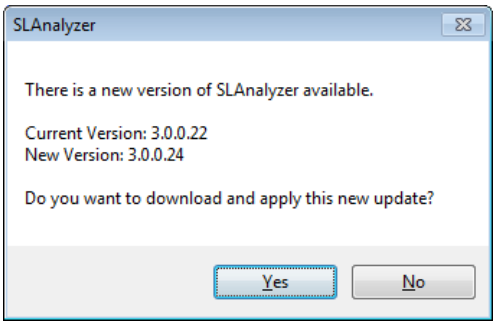


Figure 2 - Update prompt

If the user clicks the Yes button, then SLAnalyzer will download the the new SLAnalyzer download manager. After the download has completed it will exit and then launch the download manager to review the release notes or download the latest version.
If the user clicks the No button then SLAnalyzer will launch the current version of the binary. The next time the application is launched, it will again prompt the user for update. If the user wants to perform an update after clicking the No button then they can select the Check for Update option from the help menu.

During the update process the SLAnalyzer.exe binary is renamed to SLAnalyzer.backup. When the new SLAnalyzer binary loads it will attempt to delete the backup file. If SLAnalyzer has been loaded several times then this delete process may fail. At that point the user will need to close all instances of the SLAnalyzer binary and then delete the backup file.

The autoupdate process uses the following logic

1. Download file ftp.novell.com/pub/SLAnalyzer/slanalyzer.properties
2. Compare current running version to the version listed in the slanalyzer.properties file. (“version:”)
3. If current running version is older than the listed version then prompt user to download the file listed in the slanalyzer.properties file. (“url:”)

Structure of slanalyzer.properties file:
version:3.0.1.11
url:ftp://ftp.novell.com/pub/SLAnalyzer/SLAnalyzer.new

Log File Types

SLAnalyzer has built in log file parsers for a number of different log file types. The built in log file parser formats the data in a structured table format to allow for filtering and identification of issues and status. Starting in version 2.0.1.1 the user no longer needs to specify the log file type when opening. The user just opens the file through the command line or the file/open menu and SLAnalyzer will analyze the content to determine the log file type. If the type cannot be determined then SLAnalyzer will open the file as a generic text file.

Built in log file parsers:

- SLAnalyzer Report
- Novell Client Credential Provider Log
- SecretStore Debug Log
- SecureLogin Debug Log
- CLE EADebug Log
- DAS Log
- NDSTrace
- SSPR Support Bundle
- AAF Database
- AAF Debug Logs
- Generic Log Reader (TXT)
- Comma-Separated Values (CSV)
- JSON Formatted File (JSON)
- HyperText Markup Language (HTM/HTML/URL)
- XML Formatted File (XML)
- ZEN Message Logs
- HAR files

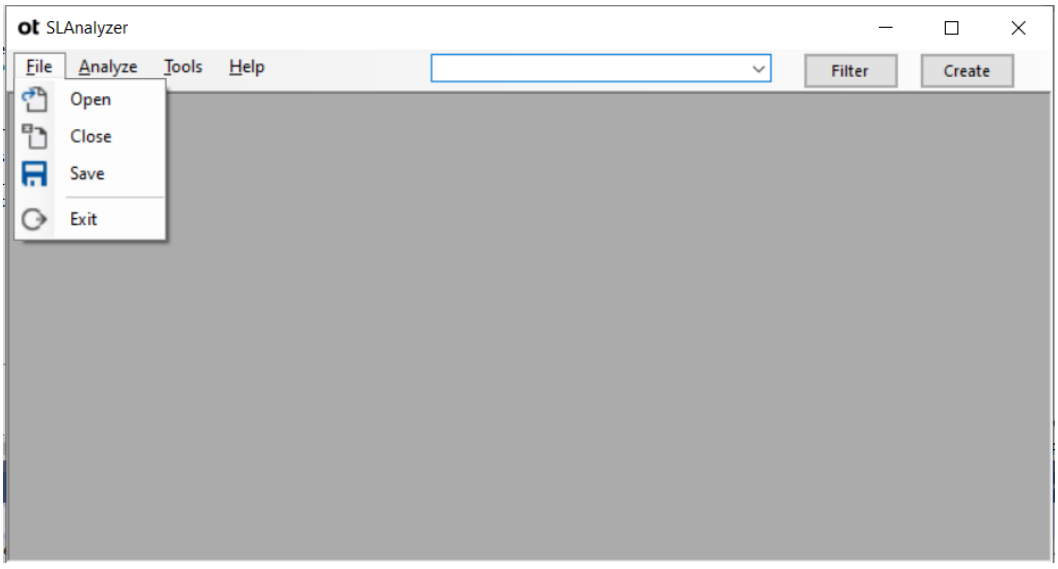


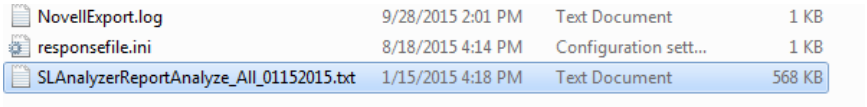
Figure 3 - File open menu

Command Line Parameters

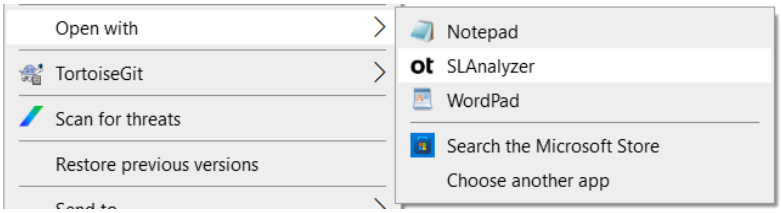
SLAnalyzer supports one command line parameter passed on execution.
C:\>SLAnalyzer logfile.log

Any filename passed to SLAnalyzer during load will be analyzed and an attempt will be made to open in the proper reader format. For example, when opening a text file, the data will be parsed in an attempt to identify if the content is a SLAnalyzer report, SSODebugLog, SSPR Debug log, etc. If SLAnalyzer is able to determine the content type then the appropriate reader will be used, otherwise SLAnalyzer will prompt the user if they would like to open the file with the generic text editor.

Open Windows explorer and navigate to the desired log.



Right click and select Open with



Choose SLAnalyzer or if it isn't listed in the menu then "Choose default program", browse for SLAnalyzer, and choose from there.

Support for compressed files (ZIP)

SLAnalyzer supports opening compressed files. This provides the ability to leave log files in zip file format and then to dynamically open with SLAnalyzer.

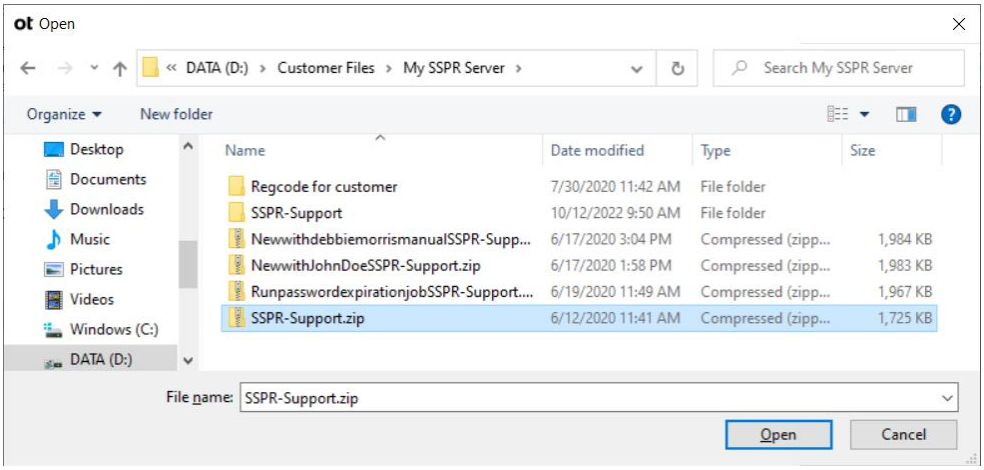


Figure 4 - Opening a compressed file

When opening zip files SLAnalyzer will extract the files to the temporary folder of the user. SLAnalyzer reads the defined DOS environment variable “TEMP” for the extract location.

```
TEMP=C:\Users\Greg\AppData\Local\Temp
```

SLAnalyzer then appends the path of SLAnalyzer followed by the name of the zip file.
For example: C:\Users\Greg\AppData\Local\Temp\SLAnalyzer\SSPR-Support
After the files are extracted the file browser window will be displayed again so that the desired log file can be opened.

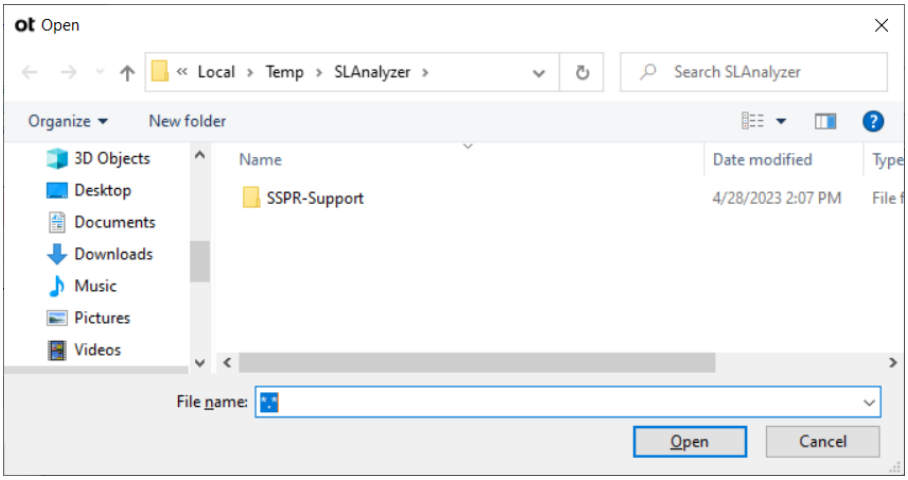


Figure 5 - Extracted content

When the user selects File/Close or exits SLAnalyzer, then the extracted files in this temporary folder are deleted.

Support for large log files

SLAnalyzer is designed to handle files of just about any size. But because of limitations of memory and other local resources, the open process will analyze the size of the file to determine if it is too large to be processed completely. If the log file contains more than 500,000 lines then a message will be displayed to the user indicating that the load times may be long.

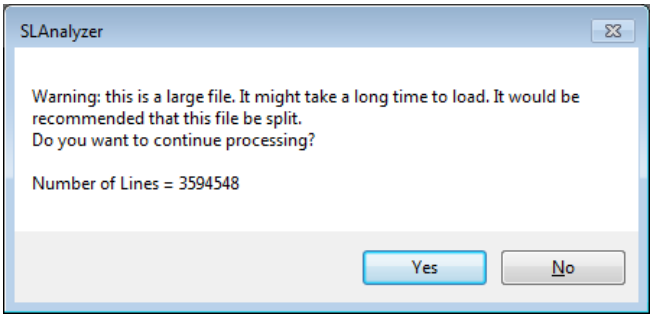


Figure 6 - Large file detected

- If the user selects no then the file will not be loaded.
- If the user selects yes, then the user will be presented with the option to split the file into more manageable pieces.

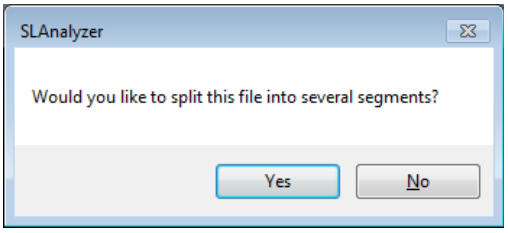


Figure 7 - Split file?

- If the user clicks no then the full file will be processed. Note that this could take a long time to complete. Also note that system resources could be reduced to a point where memory swaps to disk can cause the workstation to be slow or unresponsive. It is recommended that the file be split into smaller segments for easier analysis.
- If the user clicks yes then the file will be split into segments containing a maximum of 500,000 lines per segment.

SLAnalyzer will first validate if file segments are already found. If so, then the user is prompted to either abort the split or overwrite the existing files.

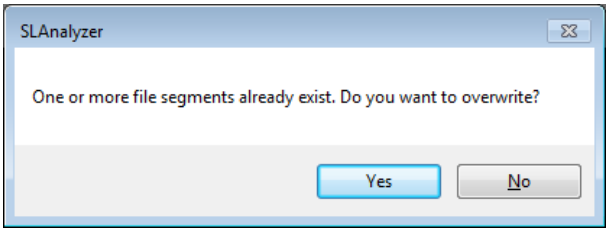


Figure 8 - Segments already found

A message is displayed to reflect the segment creation progress.

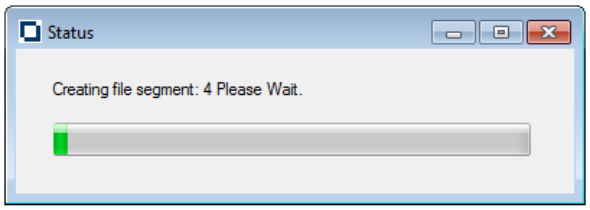
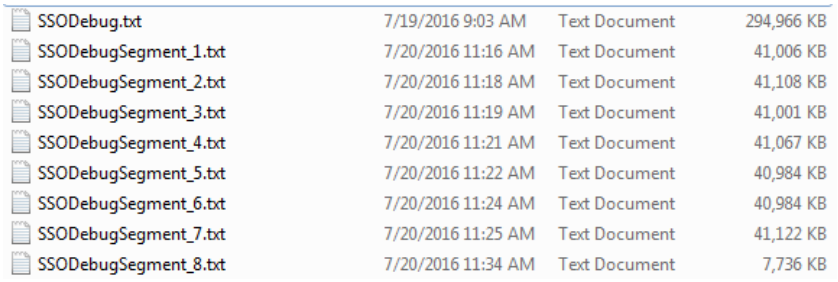


Figure 9 - Create segment progress

File segments are created in the same location as the original log file. Each file will be named with the original file name with Segment_x appended to the name. (where x is the actual segment number)



SSODebug.txt	7/19/2016 9:03 AM	Text Document	294,966 KB
SSODebugSegment_1.txt	7/20/2016 11:16 AM	Text Document	41,006 KB
SSODebugSegment_2.txt	7/20/2016 11:18 AM	Text Document	41,108 KB
SSODebugSegment_3.txt	7/20/2016 11:19 AM	Text Document	41,001 KB
SSODebugSegment_4.txt	7/20/2016 11:21 AM	Text Document	41,067 KB
SSODebugSegment_5.txt	7/20/2016 11:22 AM	Text Document	40,984 KB
SSODebugSegment_6.txt	7/20/2016 11:24 AM	Text Document	40,984 KB
SSODebugSegment_7.txt	7/20/2016 11:25 AM	Text Document	41,122 KB
SSODebugSegment_8.txt	7/20/2016 11:34 AM	Text Document	7,736 KB

Figure 10 - Segment list

After the file has been split, then SLAnalyzer notifies the user to open the desired segment file from the File/Open menu.

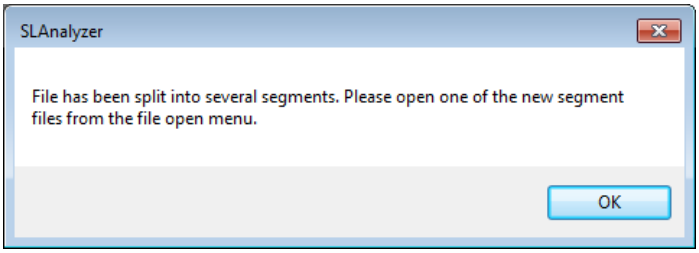
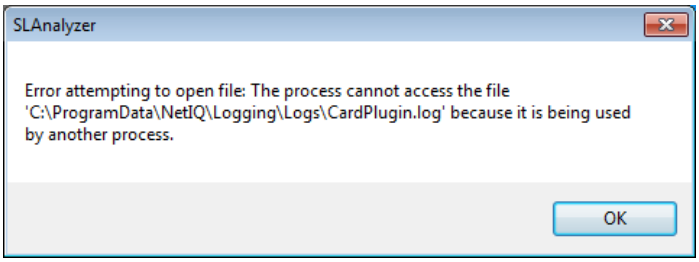


Figure 11 - Split completed

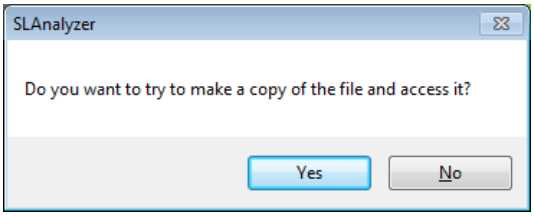
Note: If a compressed file is opened and then a file within that compressed file is split, the user can then open any of the split files from the temporary (extracted) file location. But if they close SLAnalyzer or click on File/Close, the split files will be removed and the process of extraction and splitting will need to be repeated.

Support for open log files

During the file open routine SLAnalyzer will detect if the file is currently being held open by some other process. If detected SLAnalyzer will display a message to the end user.



The user will then be prompted if they want to make a copy of the file for access.



If the user answers yes, then SLAnalyzer will make a copy of the file in the users temp folder location. Upon exiting SLAnalyzer the file will be deleted.

If the user answers no, then the file open attempt will be aborted and the user will be returned to the SLAnalyzer main window.

File Menu

The File menu consists of the following items.

- Open
- Save
- Close
- Exit

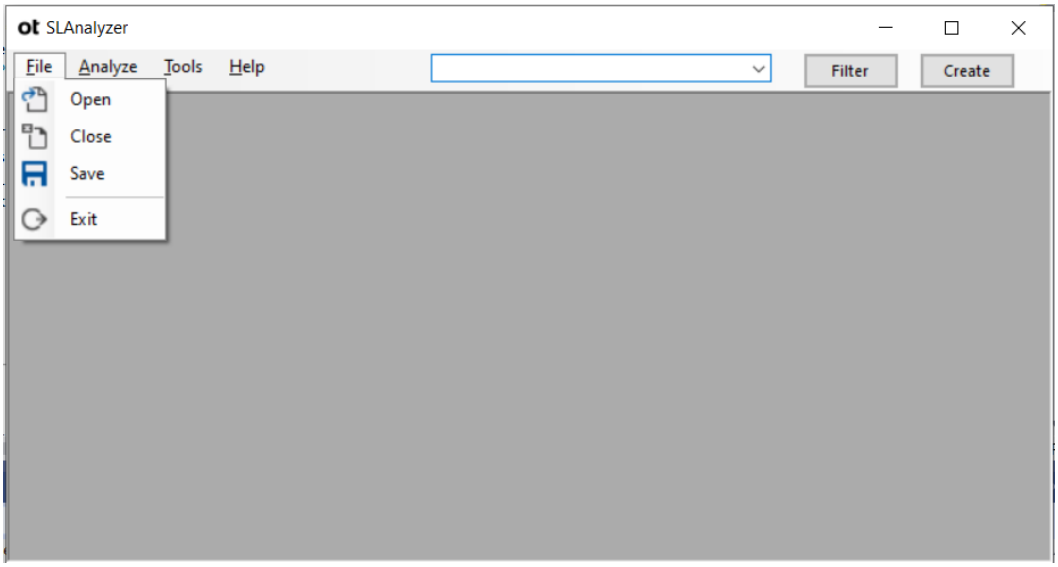


Figure 12 – File Menu

Open

SLAnalyzer supports a wide range of log files. There are specialized readers for some products and generic readers for most other log types. SLAnalyzer will also open media and office based files. If a built-in function cannot display the file type then the external program defined in Windows as the default for that type of file will be spawned. For example attempting to open a pdf file will actually launch the acrobat reader to display the pdf content.

Log File Features

When a log file is open the following features are available.

- Colorization
- Copying data
- Comments
- Column Sort
- Column Move/Re-order
- Finding data
- Jumping to a specific entry/line
- Filters

Colorization

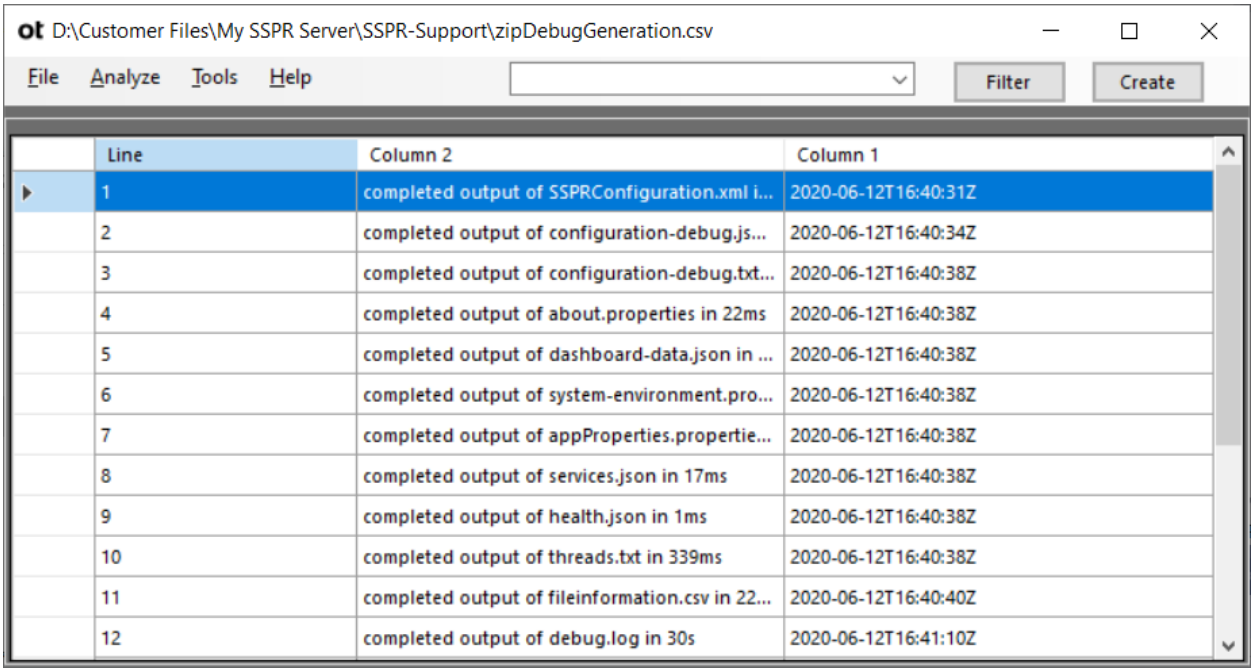
When a log file is opened, SLAnalyzer will parse each line of the file and colorize the information based upon the category defined for that logging type.

- None: No colorization
- Fatal: Orange/Red
- Error: Red
- Warning: Yellow
- Success: Green
- Information: Light Green
- Debug: Light Blue
- Trace – White
- Label – Cyan
- SectionMark – Gray

Column Move/Re-order

You can click on any column header and drag it left/right to move its position in the display. For example, the comments field is displayed as the last column. But it would be much easier to make comments if the field was adjacent to the field being commented on. So click on the column header for the comment field and drag it to the left to move it closer to the Message field.

Note that if the mouse is dragged outside of the column headers then the move will be aborted. You must keep the mouse within the column header line.

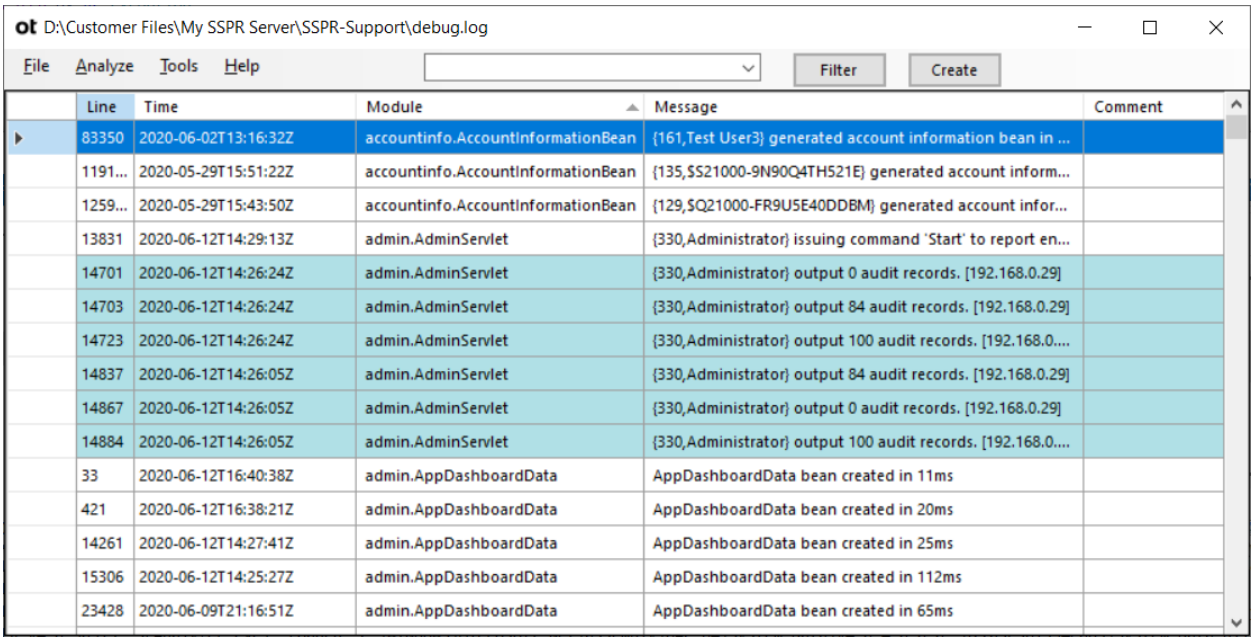


	Line	Column 2	Column 1
▶	1	completed output of SSPRConfiguration.xml i...	2020-06-12T16:40:31Z
	2	completed output of configuration-debug.js...	2020-06-12T16:40:34Z
	3	completed output of configuration-debug.txt...	2020-06-12T16:40:38Z
	4	completed output of about.properties in 22ms	2020-06-12T16:40:38Z
	5	completed output of dashboard-data.json in ...	2020-06-12T16:40:38Z
	6	completed output of system-environment.pro...	2020-06-12T16:40:38Z
	7	completed output of appProperties.propertie...	2020-06-12T16:40:38Z
	8	completed output of services.json in 17ms	2020-06-12T16:40:38Z
	9	completed output of health.json in 1ms	2020-06-12T16:40:38Z
	10	completed output of threads.txt in 339ms	2020-06-12T16:40:38Z
	11	completed output of fileinformation.csv in 22...	2020-06-12T16:40:40Z
	12	completed output of debug.log in 30s	2020-06-12T16:41:10Z

Figure 13 - Moved column

Column Sort

The user can click on a column header (I.E. Module) and the sort will occur on that column or reverse if it is already selected.



Line	Time	Module	Message	Comment
83350	2020-06-02T13:16:32Z	accountinfo.AccountInformationBean	{161,Test User3} generated account information bean in ...	
1191...	2020-05-29T15:51:22Z	accountinfo.AccountInformationBean	{135,$S21000-9N90Q4TH521E} generated account inform...	
1259...	2020-05-29T15:43:50Z	accountinfo.AccountInformationBean	{129,$Q21000-FR9U5E40DDBM} generated account infor...	
13831	2020-06-12T14:29:13Z	admin.AdminServlet	{330,Administrator} issuing command 'Start' to report en...	
14701	2020-06-12T14:26:24Z	admin.AdminServlet	{330,Administrator} output 0 audit records. [192.168.0.29]	
14703	2020-06-12T14:26:24Z	admin.AdminServlet	{330,Administrator} output 84 audit records. [192.168.0.29]	
14723	2020-06-12T14:26:24Z	admin.AdminServlet	{330,Administrator} output 100 audit records. [192.168.0....	
14837	2020-06-12T14:26:05Z	admin.AdminServlet	{330,Administrator} output 84 audit records. [192.168.0.29]	
14867	2020-06-12T14:26:05Z	admin.AdminServlet	{330,Administrator} output 0 audit records. [192.168.0.29]	
14884	2020-06-12T14:26:05Z	admin.AdminServlet	{330,Administrator} output 100 audit records. [192.168.0....	
33	2020-06-12T16:40:38Z	admin.AppDashboardData	AppDashboardData bean created in 11ms	
421	2020-06-12T16:38:21Z	admin.AppDashboardData	AppDashboardData bean created in 20ms	
14261	2020-06-12T14:27:41Z	admin.AppDashboardData	AppDashboardData bean created in 25ms	
15306	2020-06-12T14:25:27Z	admin.AppDashboardData	AppDashboardData bean created in 112ms	
23428	2020-06-09T21:16:51Z	admin.AppDashboardData	AppDashboardData bean created in 65ms	

Figure 14 - Sorted on Module column

Comments

SLAnalyzer will automatically create a comment field as the last column. This column allows the user to make comments on the specific line associated with the currently loaded log file.

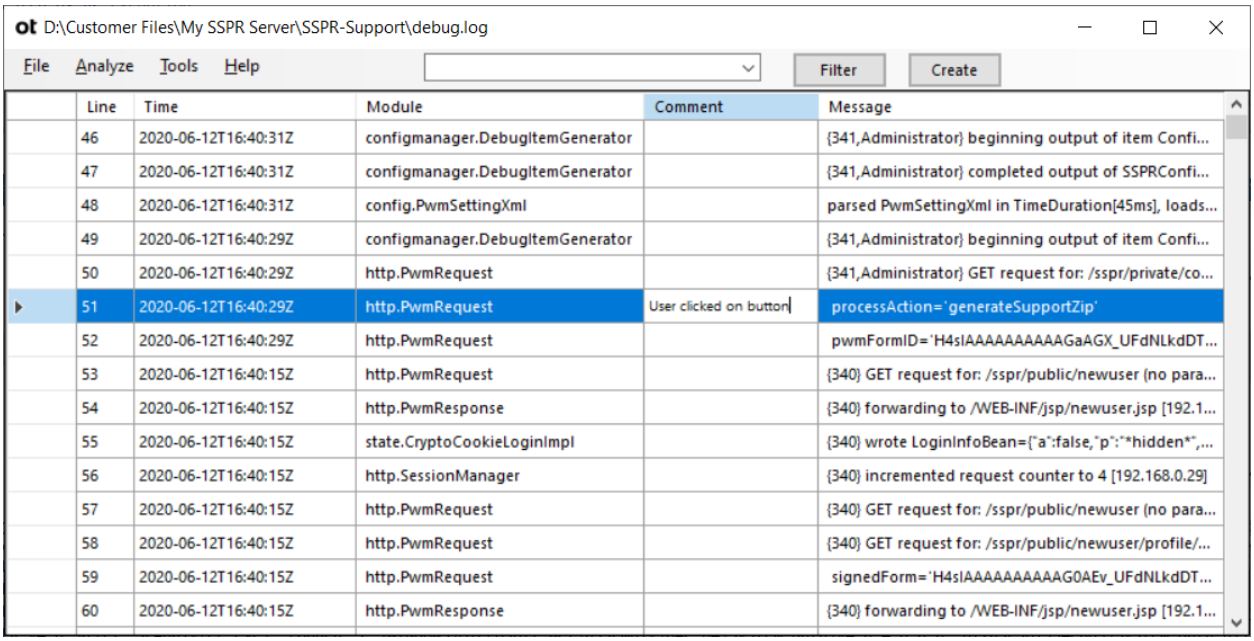


Figure 15 - Comments field

Double clicking in the Comment field allows the user to enter information. Comments are saved by clicking on the File/Save menu option.

Notes about comments:

- Comments are committed only after the user selects a different field. For example, of you entered a comment on line 1 and then immediately selected File/Save, the information entered into line 1 would not be saved. To save/commit the information then after entering new information into line 1, click on any other column. Then select File/Save to save the comments.
- Comments are not saved to the log file itself. A new file is created with the same name as the log file with a .comment file extension. For example if the log file was called customer.log then the comments file will be called customer.log.comments.
- If a compressed file is being commented then the comments file would be lost if the user were to click on File/Close or exit SLAnalyzer. For this reason the currently opened log file and the new comments file will be saved to the original folder of the compressed file. For example if the source zip file for the log customer.log was located on “c:\customers\12345” then the extracted log file and comments file would be automatically copied to this same location.
- When reopening the log file, the comments file will be parsed and the comments column will be populated with the information. If the comments file cannot be located in the same folder as the log file being opened, then the comments column will be blank.
- Because the comments column is inserted as the last column it might be difficult scrolling left and right to reference another column within the table data. For this reason it is much easier if the column is repositioned next to the column being referenced. See Moving Columns below.

- Attempting to close a log where comments have been made but not saved will result in a message being displayed to notify the user that the comments have not been saved.

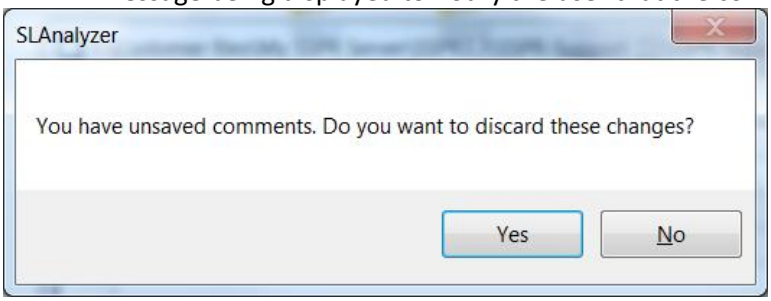


Figure 16 - Unsaved comments prompt

- Prior to saving the comments file, SLAnalyzer will attempt to make a backup of the original comments if they existed when the log file was loaded. It will first look for the presence of a file with the same name with the file extension of .bak. For example if there was a comments file named c:\customers\12345\customers.log.comments then SLAnalyzer will first rename this file to c:\customers\12345\customers.log.comments.bak and then save the new comments to the file c:\customers\12345\customers.log.comments. If an existing backup of the comments file already exists then SLAnalzyer will prompt the user if they would like to overwrite the existing backup.

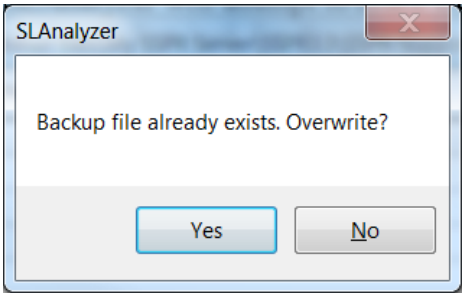
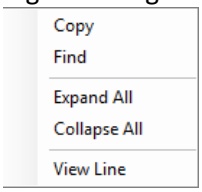


Figure 17 - Prompt to overwrite backup file

Context Menu for XML and JSON windows

Right clicking within the XML/JSON window will display the context menu.



Copy

When viewing data, you can right click on any of the elements displayed to copy the information to the system copy/paste buffer.

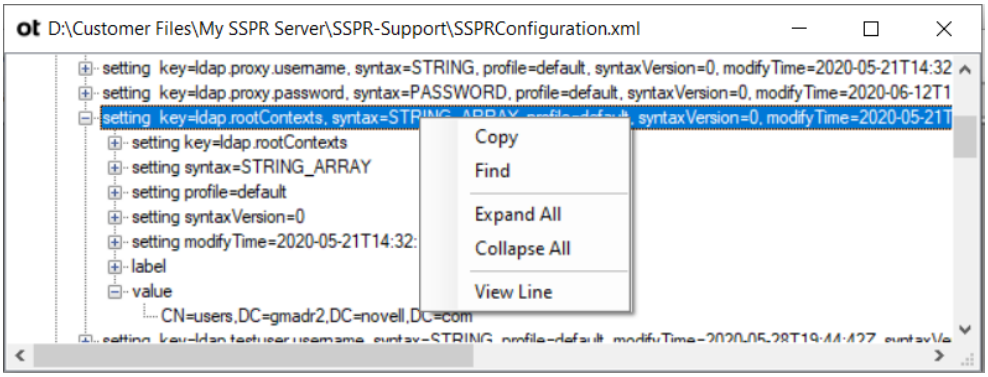


Figure 18 - Copying data from the XML data window

Alternatively, the window allows the user to perform a single left click on the line to select and then an additional single click to edit the information displayed. Once in edit mode for the line then copy and paste the desired information to the system copy/paste buffer.



Figure 19 - Copying data from the JSON data window

Find

Selecting find from the context menu will prompt for the desired search string.

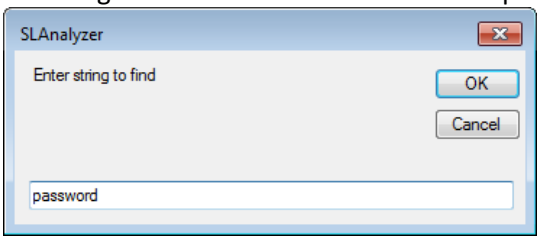


Figure 20 - Find XML/JSON text

SLAnalyzer will search the content of the XML/JSON tree, expand the items found and colorize them in yellow.

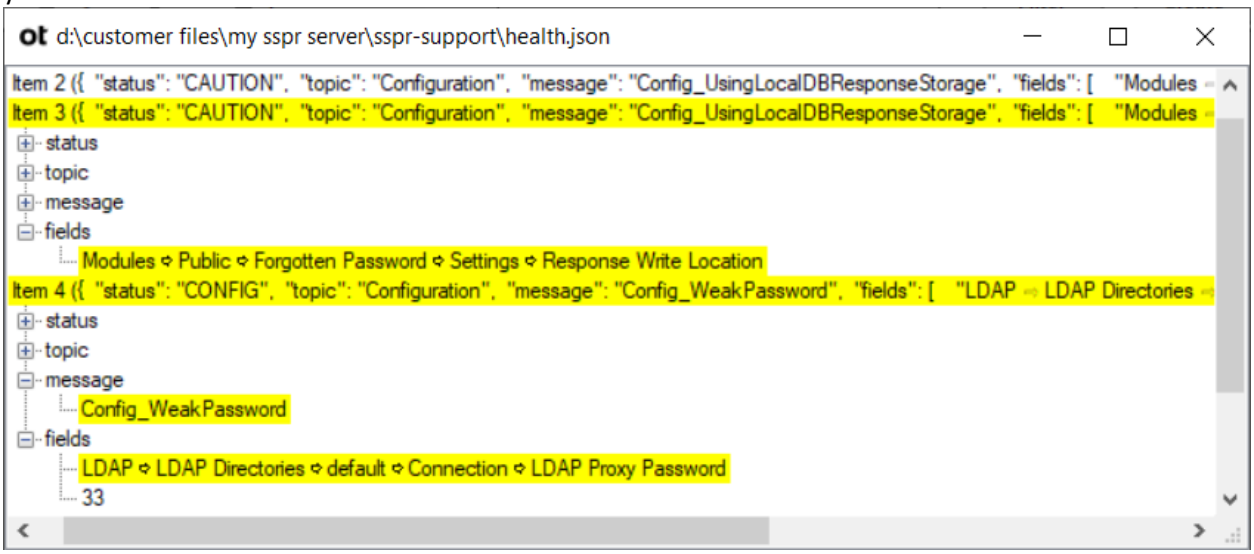


Figure 21 - Found XML/JSON data

Expand All

Selecting Expand All from the context menu will expand all of the sub-items of the selected item. If the root of the tree is selected, then all of the items will be expanded. If a sub-item is selected, then only those sub-items of the selected item will be expanded.

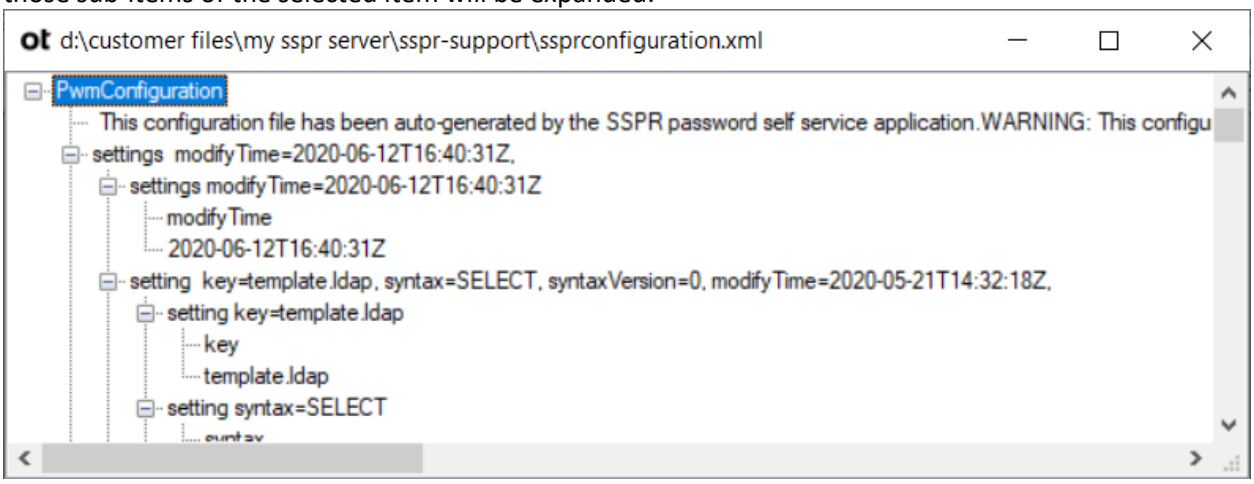


Figure 22 - Expand All

Collapse All

Selecting Collapse All from the context menu will collapse all of the sub-items of the selected item. If the root of the tree is selected, then all of the items will be collapsed. If a sub-item is selected, then only those sub-items of the selected item will be collapsed.



Figure 23 - Collapse All

View Line

When a line is bigger than the displayed window size then SLAnalyzer will display a tooltip of the data when the user positions the mouse pointer over the line. This data is sometimes difficult to read before the tooltip expires. By selecting View Line from the context menu, then users can display the data in a text window for closer examination.

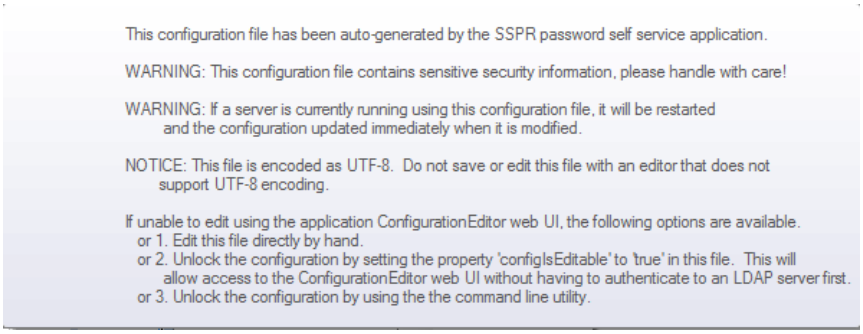


Figure 24 - Tooltip display

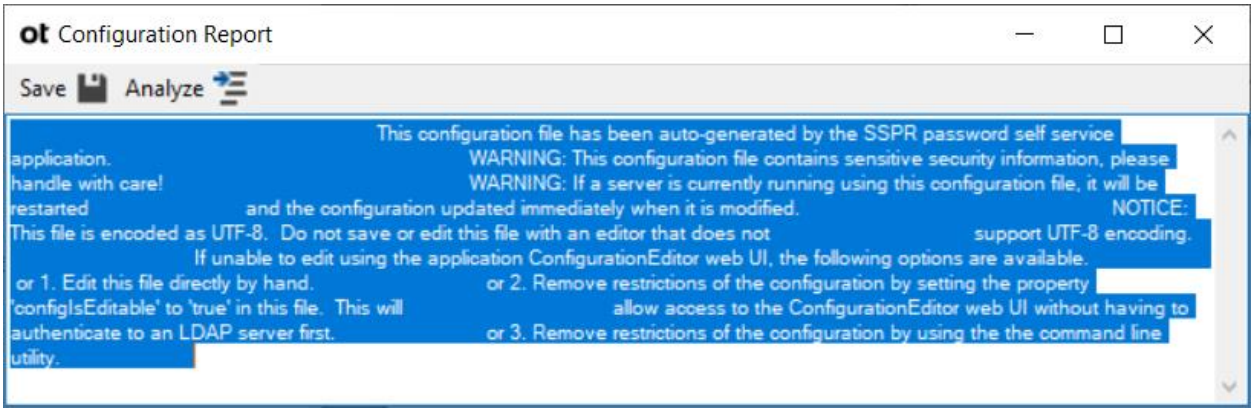
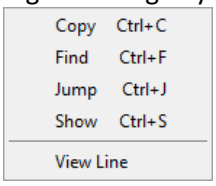


Figure 25 - View Line

Context Menu for reports/logs window

Right clicking anywhere within the report window will display a context menu.



Copy

While a log file is open you can copy the data being displayed in several ways.

Copying data from a log file

When a log file is open you can copy either the full line of the log which includes the data from all of the columns, or you can copy just the single column data.

Copying the full line

To copy the full line of a log file you simply click once on the desired line. The complete line is highlighted. Then right click and select the option (Copy) from the menu. You can also press Ctrl + C on the keyboard to perform the copy. The whole line will be copied to the system copy/paste buffer. You can now switch to email or another application and paste in the complete line of data.

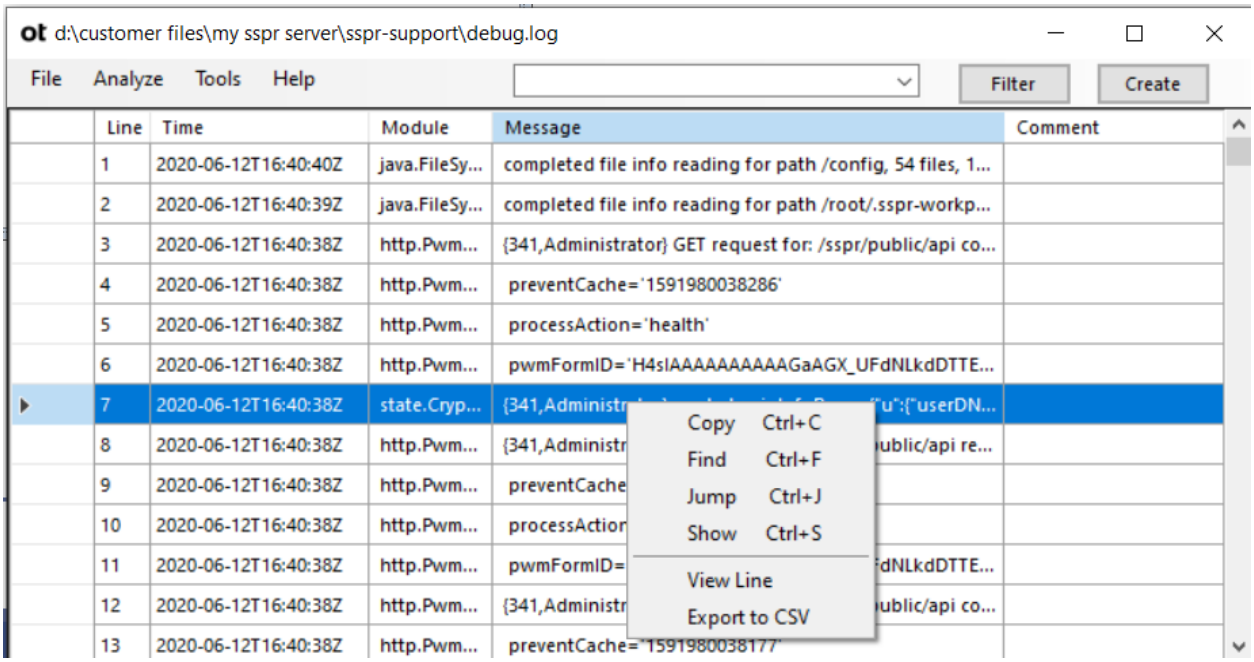


Figure 26 - Copying the full line from a log file

Copying a single column's data

To copy the data inside a single column entry, single click on the column entry to select the line. Then perform a single click again to enter edit mode. You can then mark the text you want to copy. Right click and select (Copy) to copy the column data to the system copy/paste buffer. You can now switch to email or another application and paste in the column entry data.

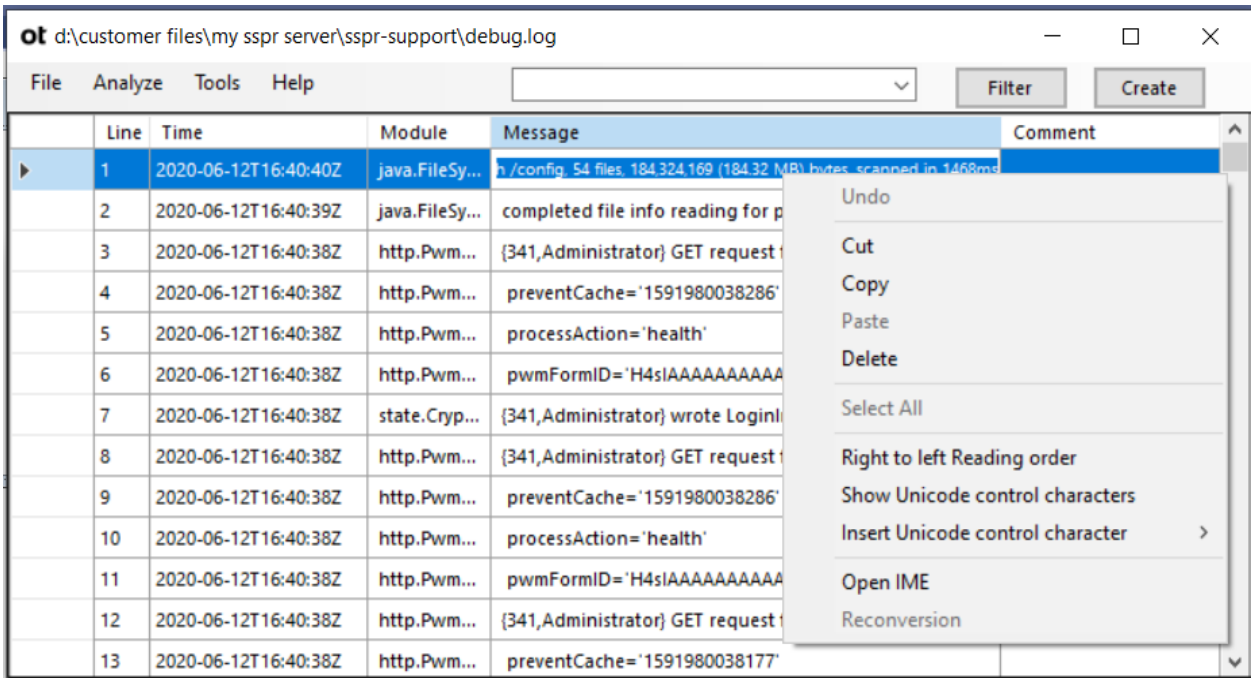


Figure 27 - Copying a single column's data

Copying multiple rows data

To copy multiple rows of data, highlight the first row, then hold the shift key down and click on the last row of the selection. Alternatively, you can hold down the control key and click on non-adjacent rows. The selected rows will be highlighted in blue. After making the desired selection, right click and select copy to copy the information to the system copy/paste buffer.

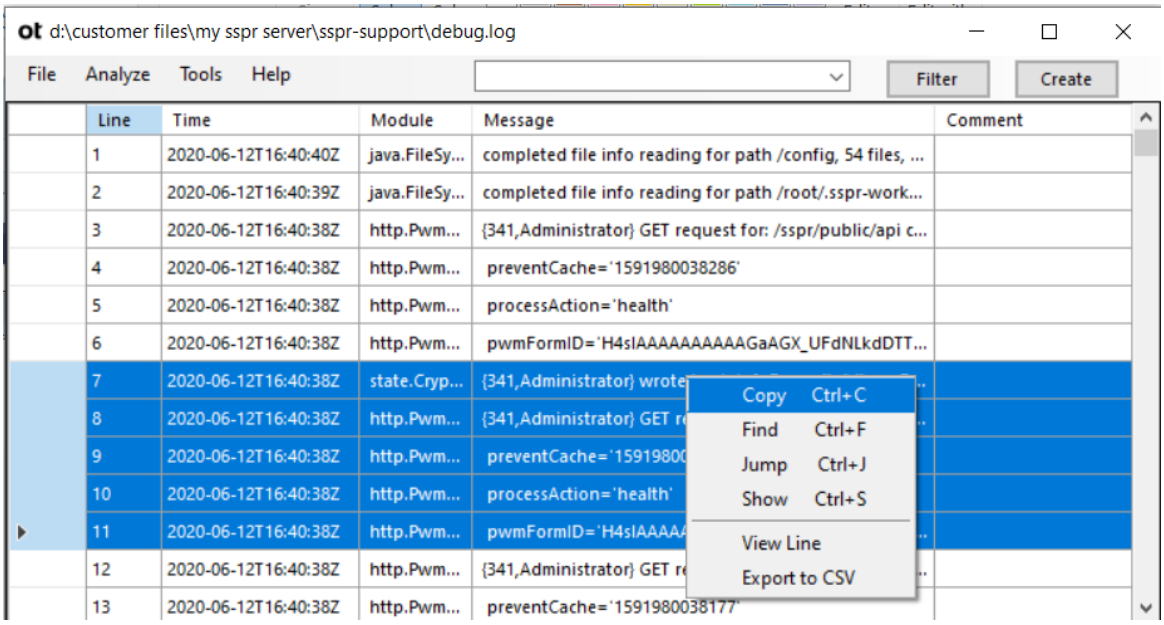


Figure 28 - Copying multiple rows of data

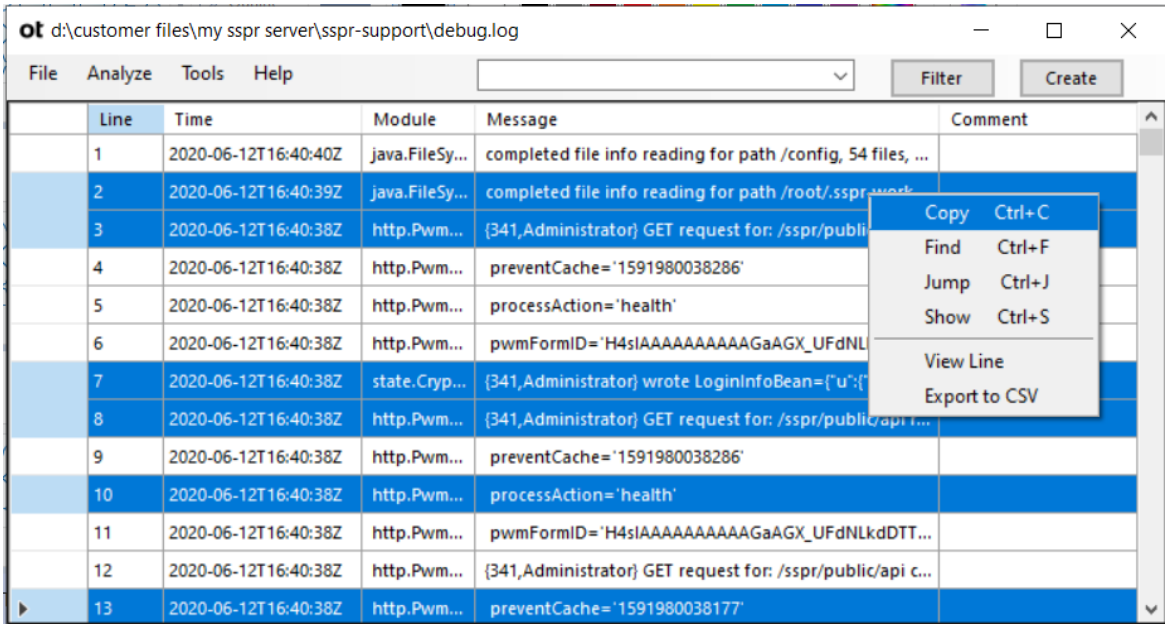


Figure 29 - Copy multiple rows non-adjacent

Find

To find data within an open log file, right click on the log file window and select (Find). You can also press Ctrl + F on the keyboard to execute the find operation.

When Find is selected the find window will be displayed.

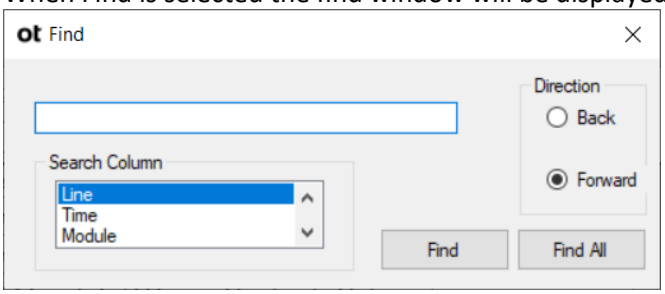


Figure 30 - Find window

The Find window allows the user to find data in one of two ways.

- Find – Will find the first/next occurrence of the specified string
- Find All – Will find all occurrences of the specified string

In the find window the user needs to specify the following information:

The text they would like to find
The direction they would like to search
The column in which to perform the search.

Find button:

After clicking the Find button, SLAnalyzer will attempt to locate the information. If the data is found, the line will be highlighted in the displayed log.

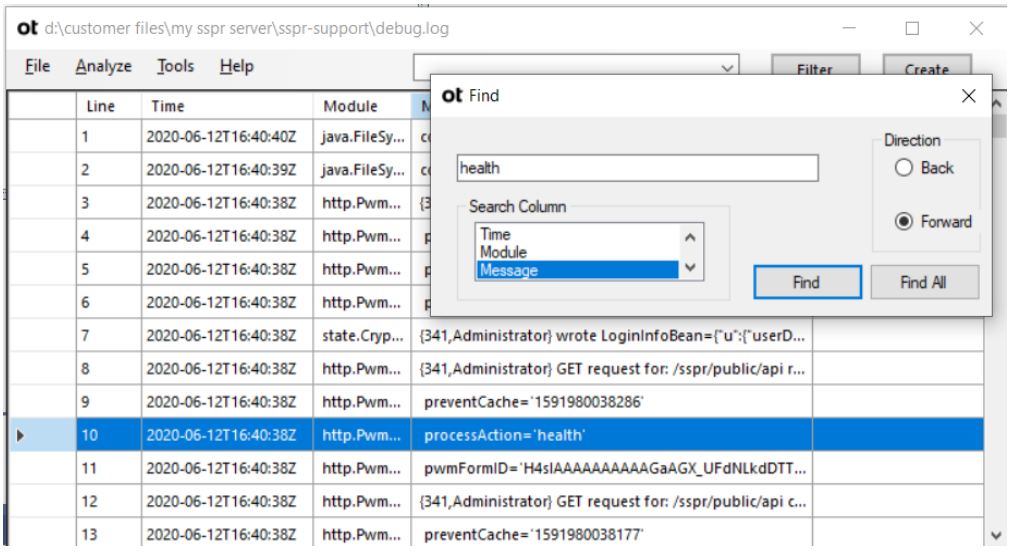


Figure 31 - Find

If the find string is not found, then a message will indicate that the search failed.

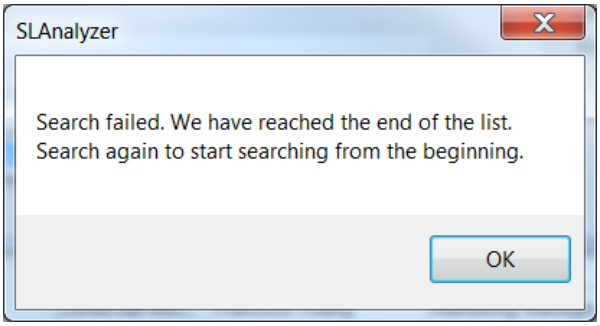


Figure 32 - Find failure

Find All button:

After clicking the Find All button, SLAnalyzer will locate all occurrences of the find string. A message will be displayed to indicate the number of items found. Items found will be marked by changing the color of the Line column (column 1) to Orange. If the find locates items, then the find window will close and the log will be displayed. If no items are found, then the find window will remain open.

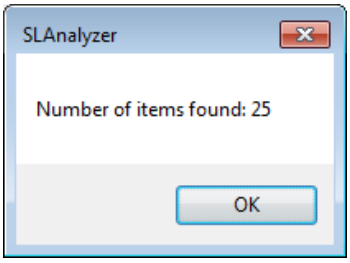


Figure 33 - Found items

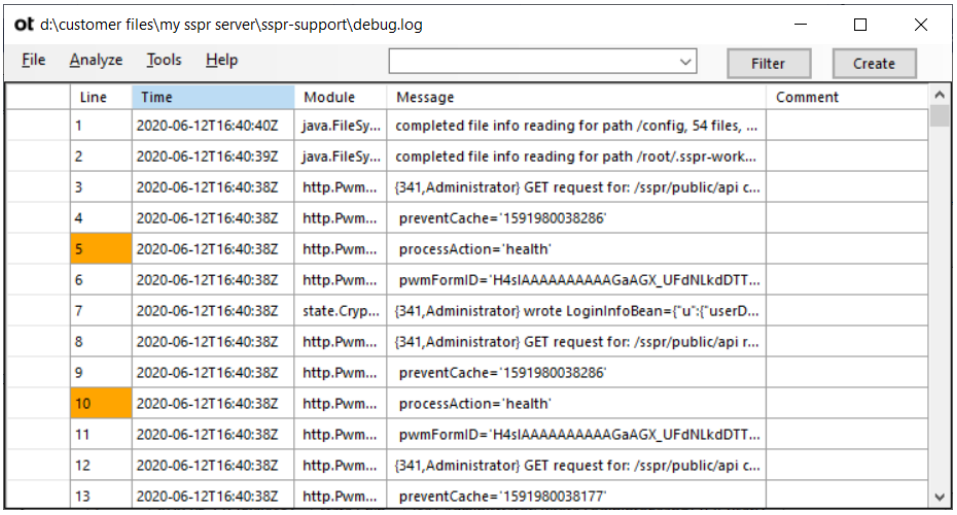


Figure 34- Find All

Jumping to a specific entry/line

When a log is open you can right click and select "Jump" or press Ctrl-J to set the position of the currently selected row within the log.

In the Jump to line window enter the line number of the log entry you want to jump to.

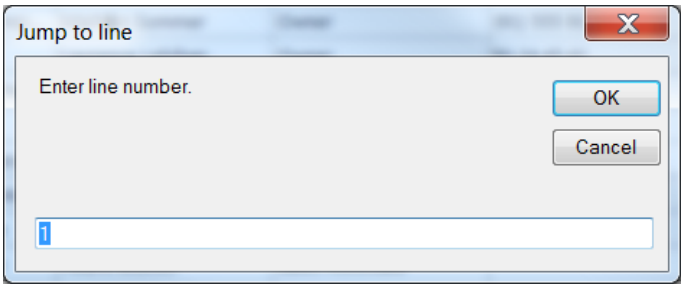


Figure 35 - Log file jump to line number

If the line number cannot be found, then a message is displayed to the user otherwise the line will be selected in the log window.

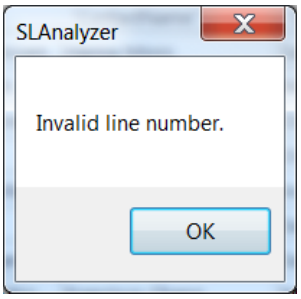
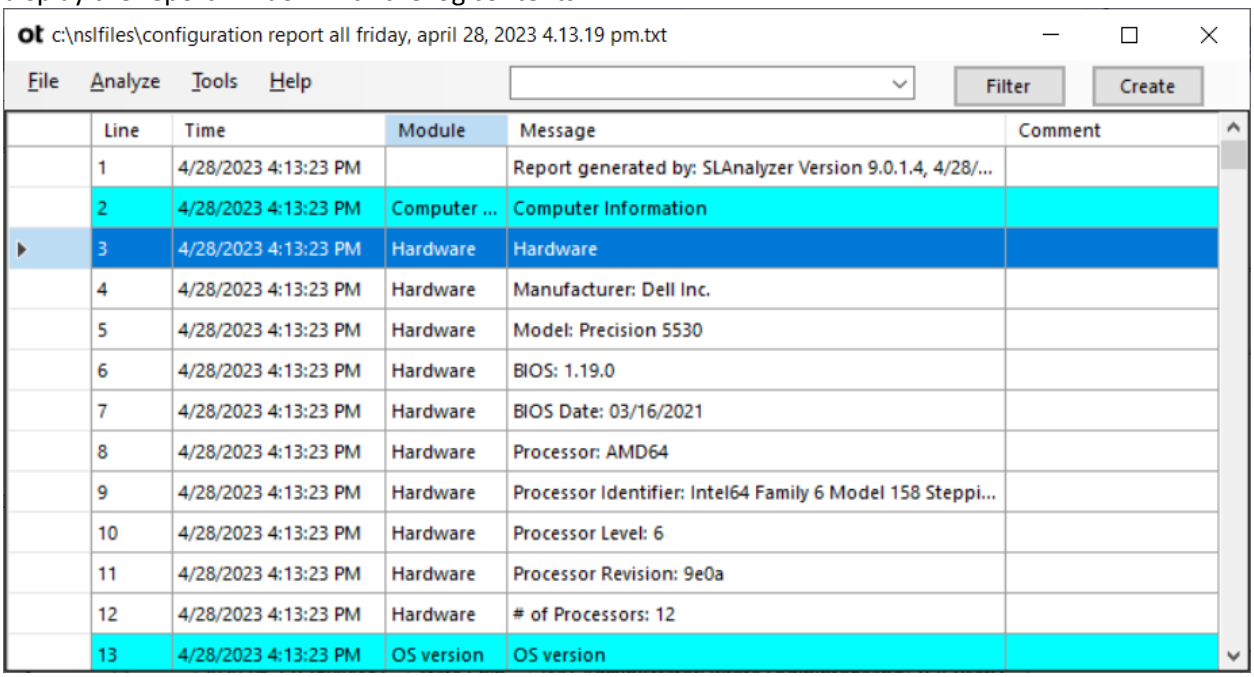
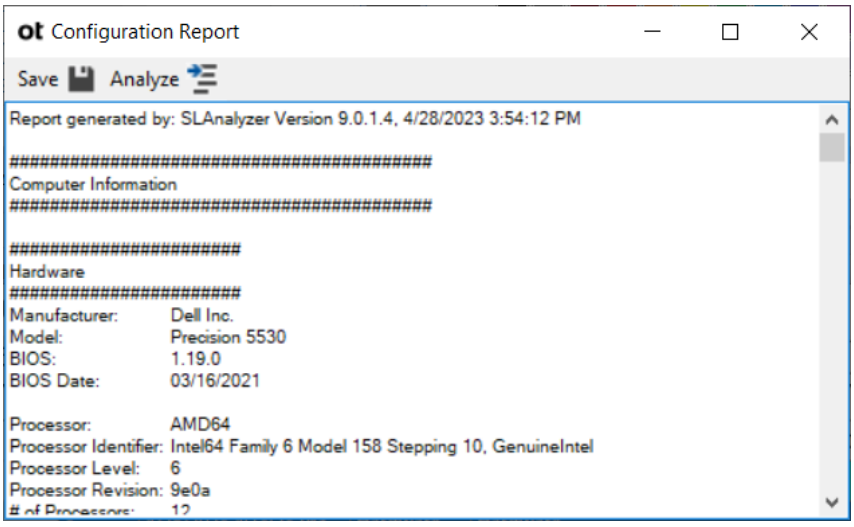


Figure 36 - Invalid line

Show

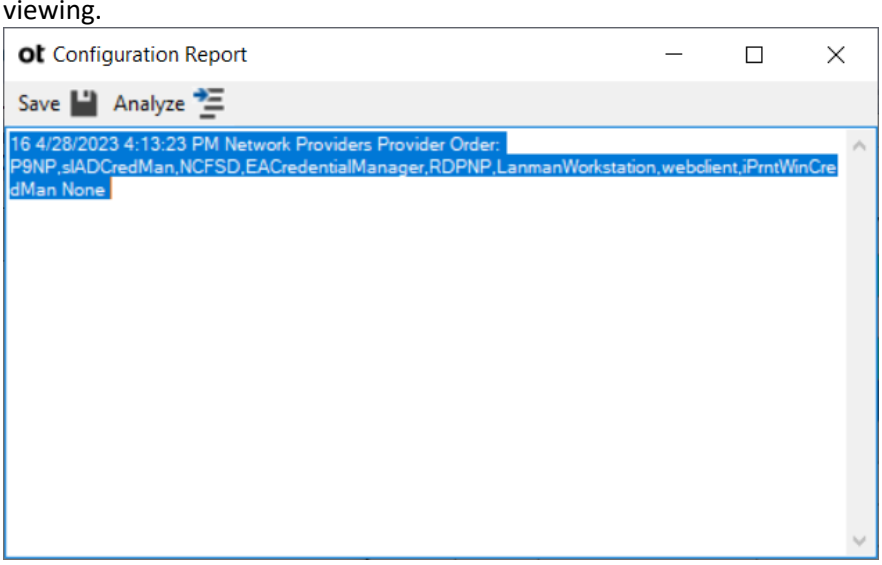
The context menu item Show will display the full log/report as text. It will open a new text window and display the report window with the log contents.



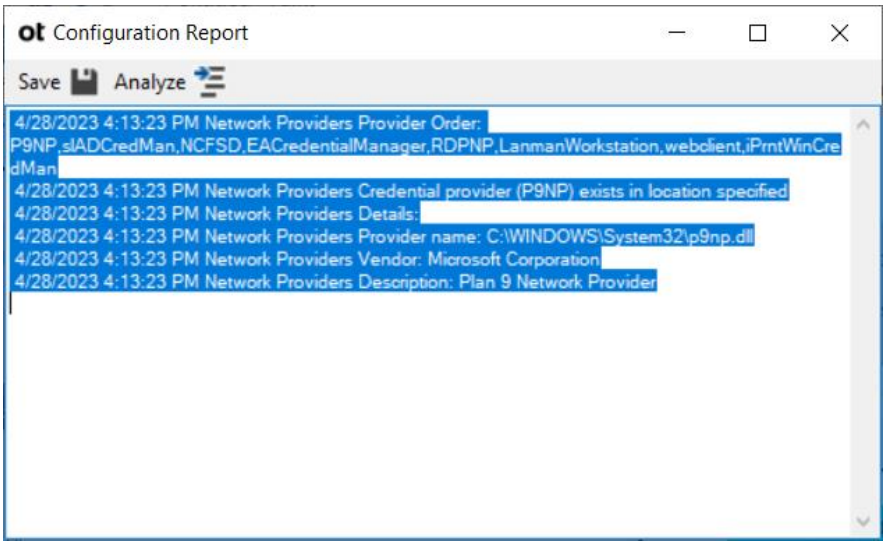


View Line

The context menu option View Line will display the currently selected line in a text window for easier viewing.



Note that you can select multiple lines and then click View Line from the context menu to display all of the selected items in the text window.



Filters

Filters allow the user to reduce the amount of information needing to be processed by displaying only specific types of data in the log file. For example it could be easier to process a log if the user could first identify the errors found in the log.

Logs can be filtered by the following:

- None: No filter, display all data – Reset
- State or Status Condition:
    - Fatal: Only display lines that were identified as Fatal status at load time
    - Errors: Only display lines that were identified as Error status at load time
    - Warnings: Only display lines that were identified as Warning status at load time
    - Information: Only display lines that were identified as Information status at load time
    - Debug: Only display lines that were identified as Debug status at load time
    - Trace: Only display lines that were identified as Trace status at load time
- Module Name: When the log file loads SLAnalyzer builds a listing of all the modules found in the log file. The module names are added to the filter list dynamically. Also a count of each filter type is listed following the name. For example if 10 errors were found in the trace then the filter item would be Error (10).
- Creating a filter: Click the create button to create a new filter
- Manually entering a filter: Typing a filter into the filter box

To filter the log the user needs to do the following:

1. Select a filter
2. Activate a filter

Selecting a filter

To select a filter then click on the filter name drop down box and select the desired item from the list.

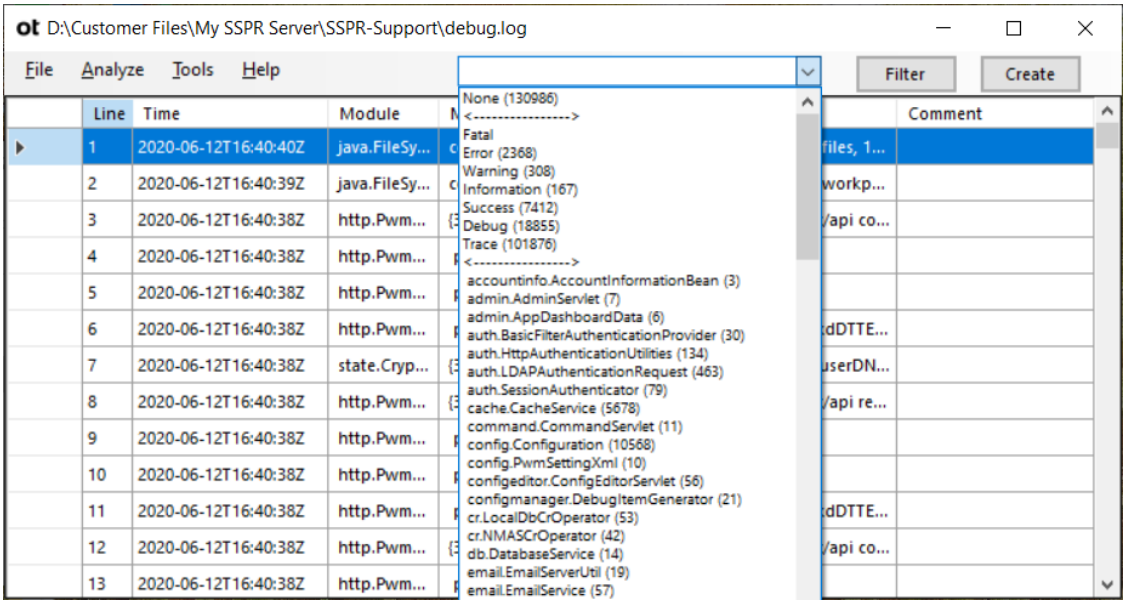


Figure 37 - Selecting a filter

After selecting a filter from the list, the currently selected item in the list will be repositioned to the first occurrence of that filter. For example, if we selected the filter Warning then the selected item would be repositioned to the first Warning message in the currently loaded log file.

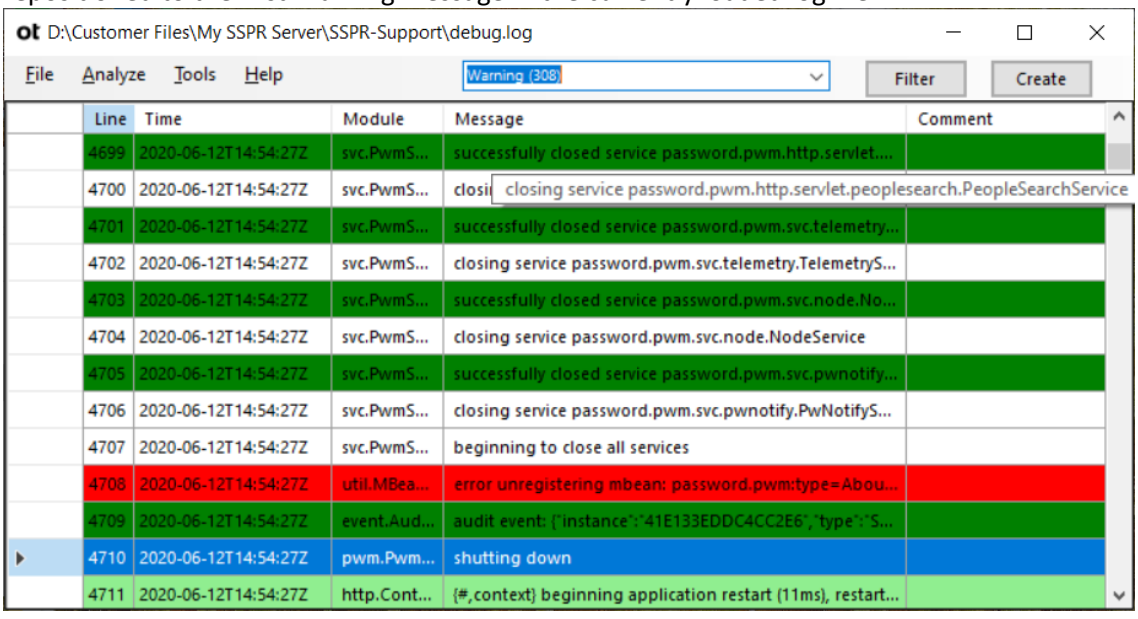


Figure 38 - Repositioned line matching selected filter

Activating a Filter

After selecting the desired filter then press the (Filter) button to activate.

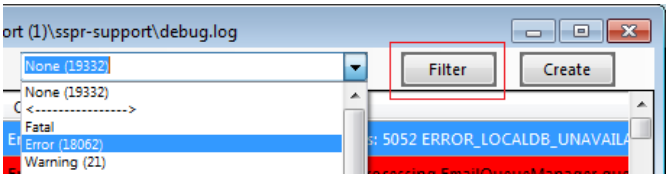


Figure 39 - Filter button

After clicking the filter button the log will be displayed again with only the lines that match the filter as visible.

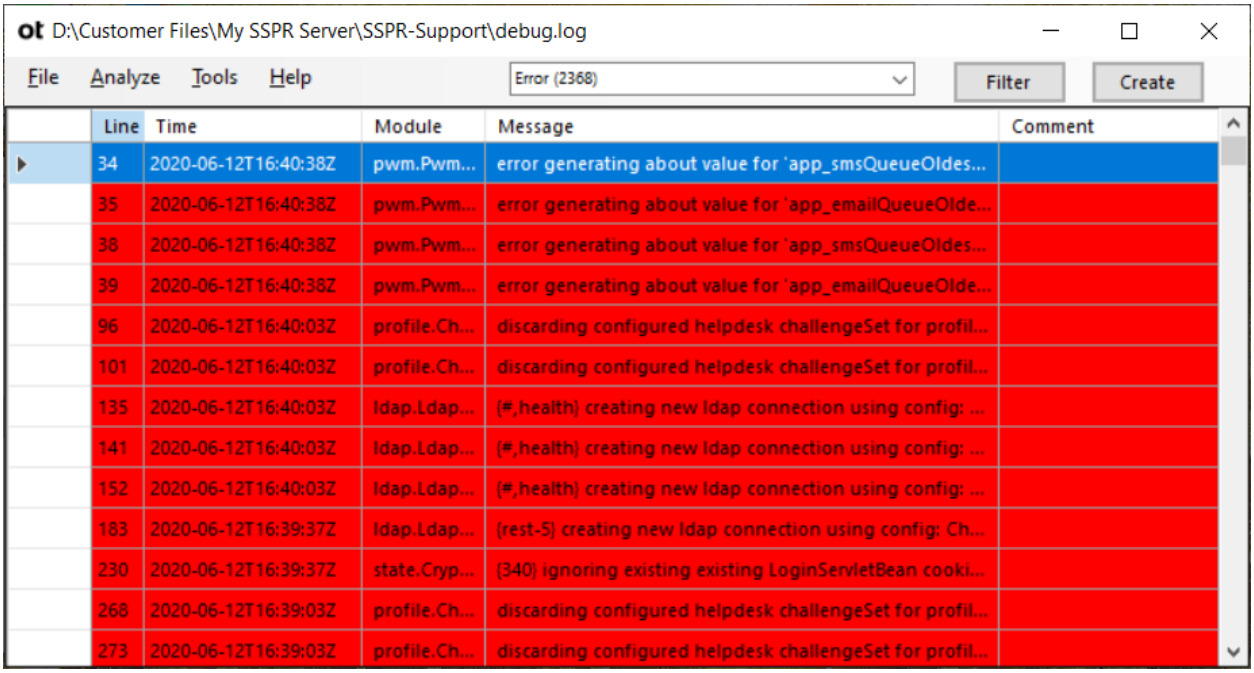


Figure 40 - Filtered log

Creating a filter

Click the create button to display the “Create custom display filter” window.

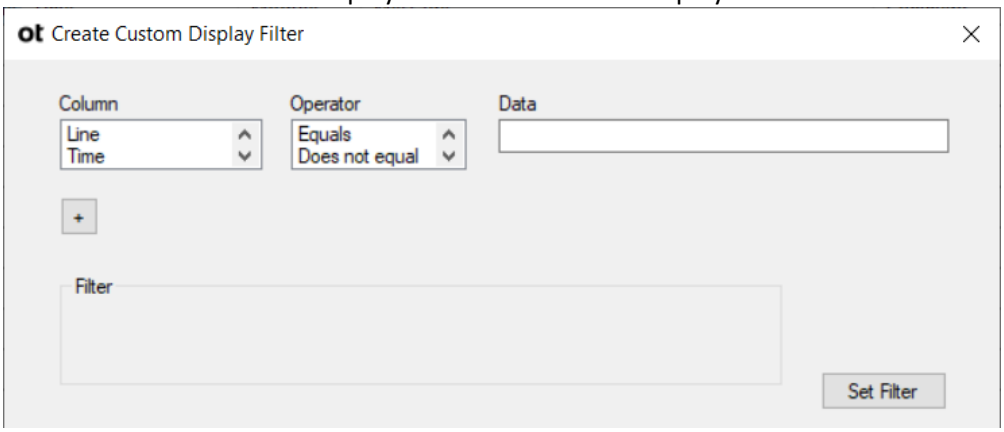


Figure 41 - Create Custom Display Filter window

Select the column that will contain the data, the operator specifies the logic of the filter and finally the data to match. For example, any instance of the word “Error” in the message column.

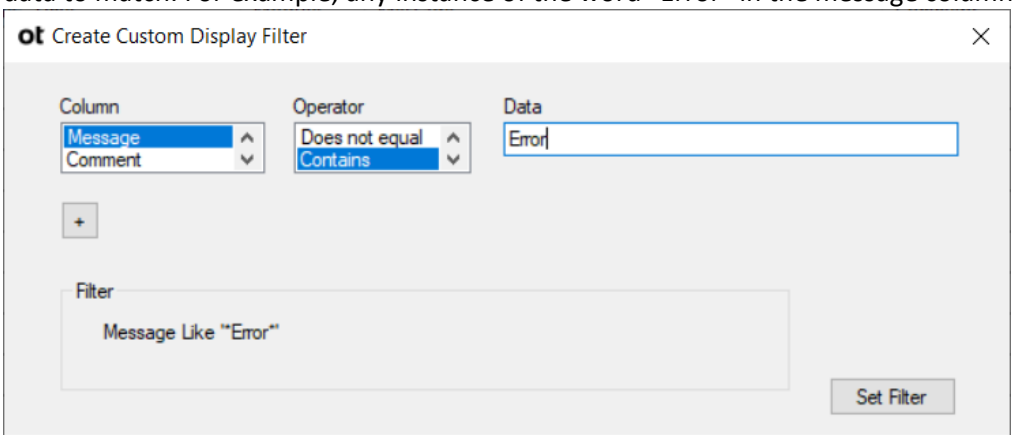


Figure 42 - Creating a custom filter

After clicking the Set Filter button, the log will be redisplayed with the filter active.

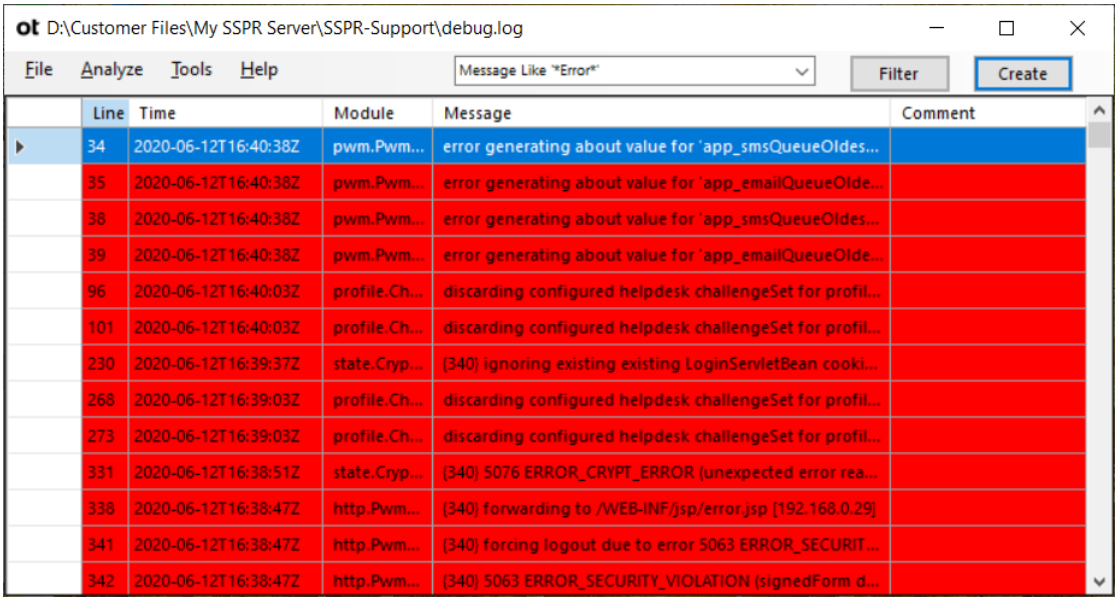


Figure 43 - Displayed custom filter

You can also create a more complex filter by adding conditions together. Click the plus button and then specify the logic (And or OR) for the filter condition.

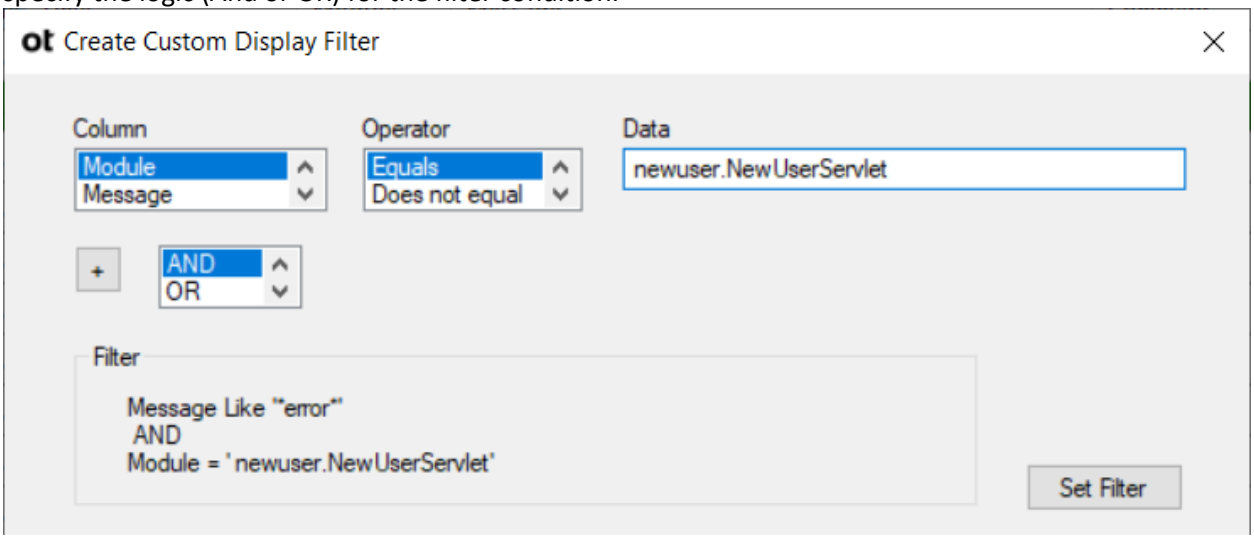


Figure 44 - Creating a complex custom filter

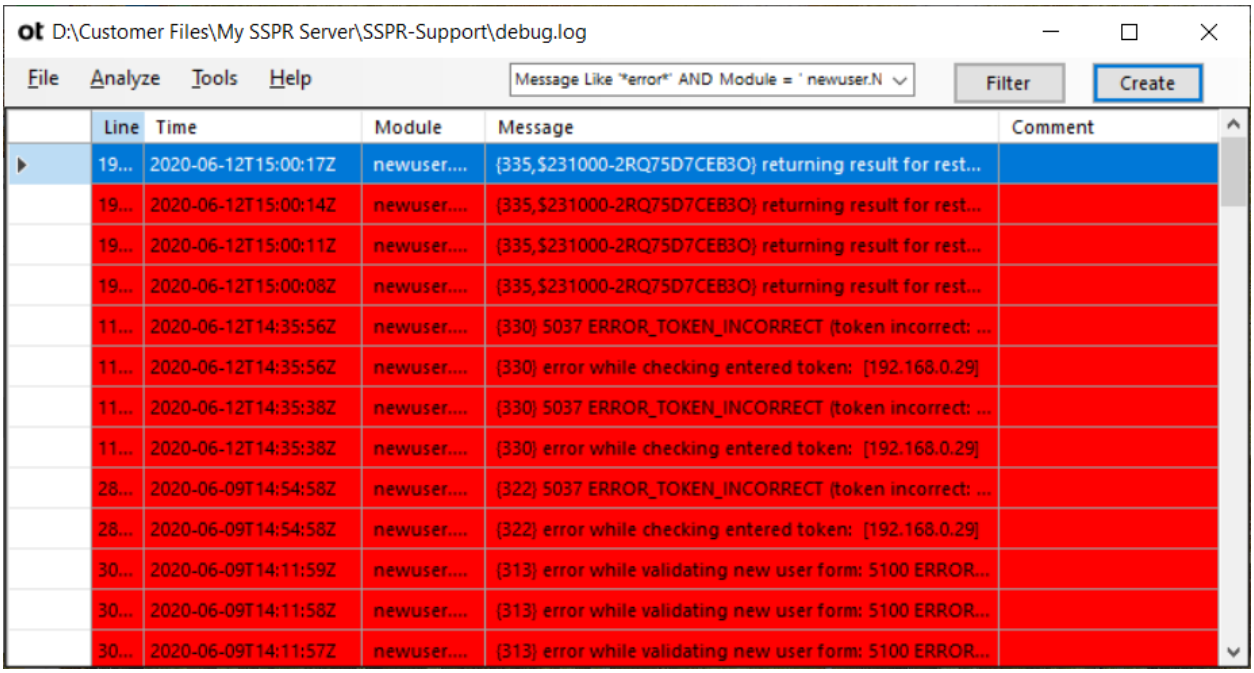


Figure 45 - Displayed complex custom filter

Manually entering a filter

You can edit the filter box manually and type in a filter.

Filters are comprised of the following

- ColumnName - column name as seen on the screen
- Operator - = (equal), <> (not equal), or Like
- Filter Text with equals operator - Text to find enclosed in single quotes 'Text'
- Filter Text with Like operator - Text to find enclosed in single quotes and wildcard (% or *) '%Text%' or '%Text' or 'Text%' or '*Text*' etc.

The filter requires the following:

- You have to use single quotes and not double quotes
- Column names that are more than one word are enclosed in []
- The filtering is not case sensitive
- Filters can be combined to filter on multiple conditions

The following are examples of different filters:

Using ColumnName = 'Text to filter on'

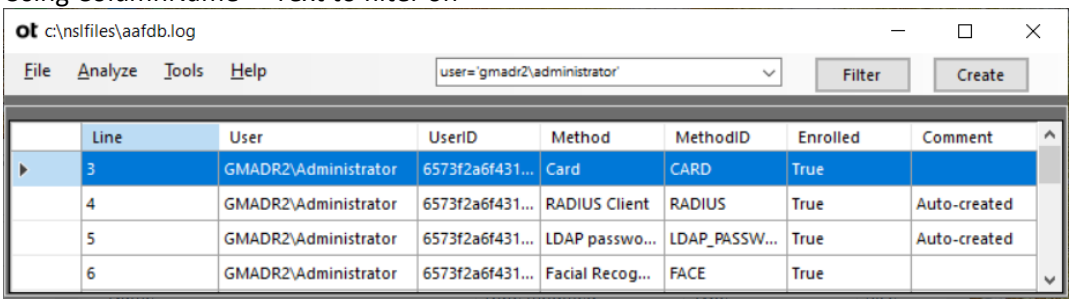


Figure 46 - Filter User='greg'

Using [Column Name] = 'Text to filter on'

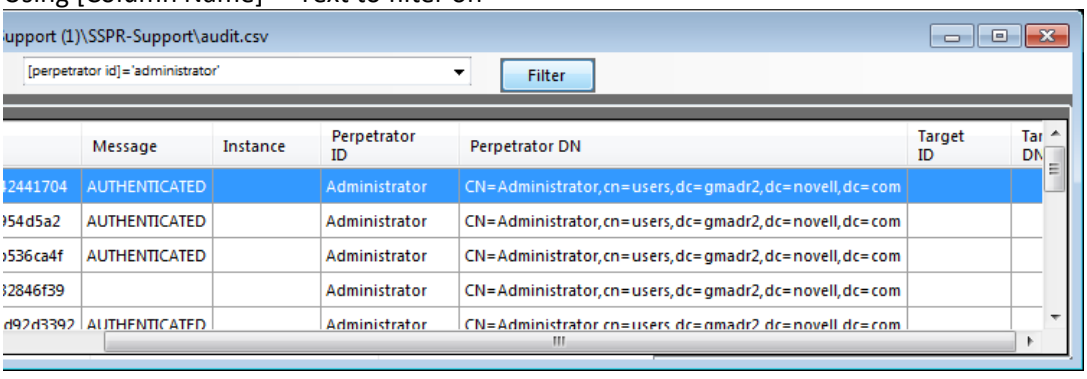


Figure 47 - Filter [perpetrator id]='administrator'

Using ColumnName Like '%Text to filter on%'

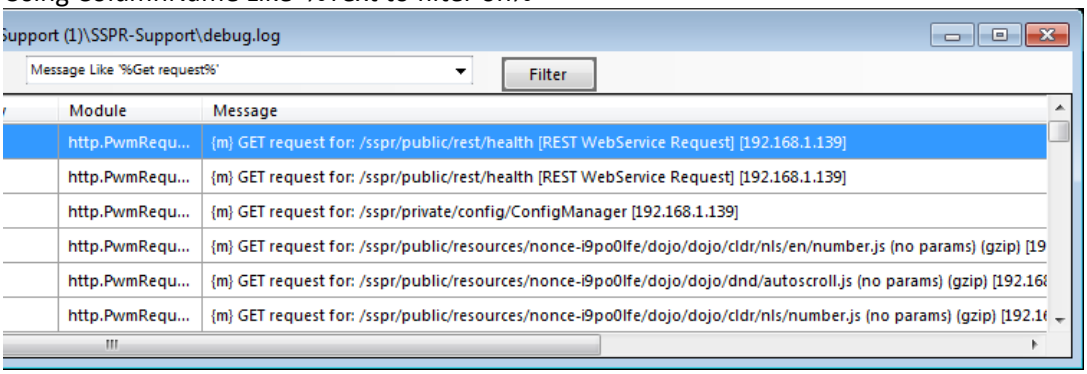


Figure 48 - Filter Message Like '%Get request%'

Using [Column Name] = 'Text to filter on' And ColumnName = 'Text to filter on'

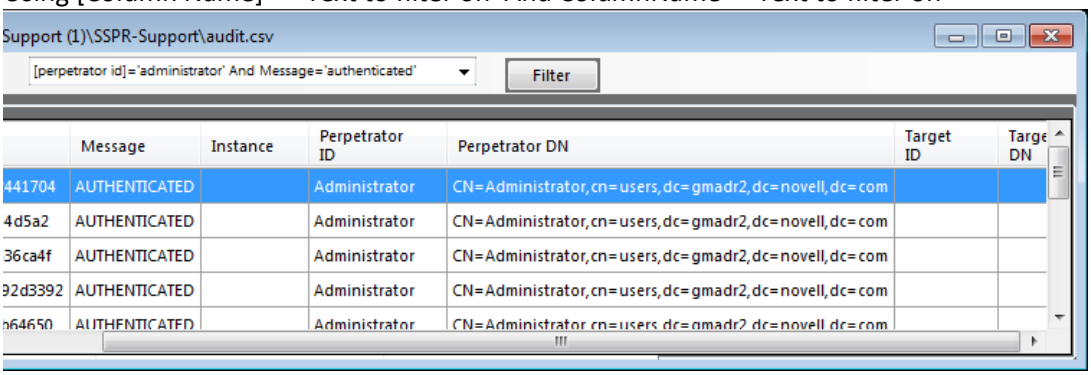


Figure 49 - Filter [perpetrator id]='administrator' And Message='authenticated'

For details on more filter possibilities see the following document on the msdn website.
https://msdn.microsoft.com/en-us/library/system.data.datacolumn.expression.aspx

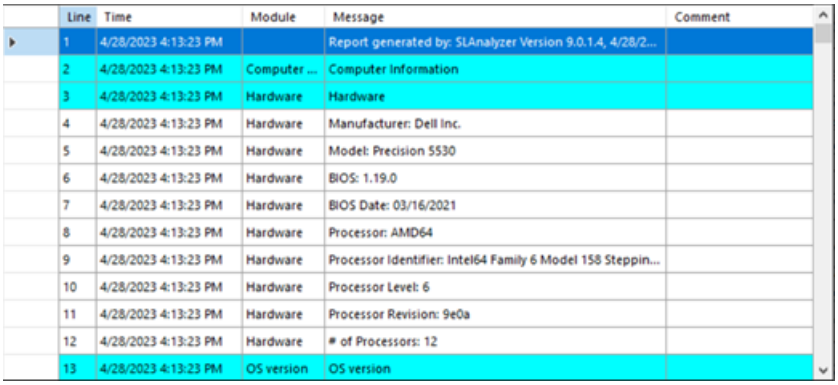
Resetting the filter

To reset the filter, select the filter of (None) from the filter drop down box and then click the filter button. The log file will be redisplayed with all lines visible.

Supported log/report file types

Opening a SLAnalyzer report

Opens a saved SLAnalyzer report and highlights issues, problems, errors, etc.

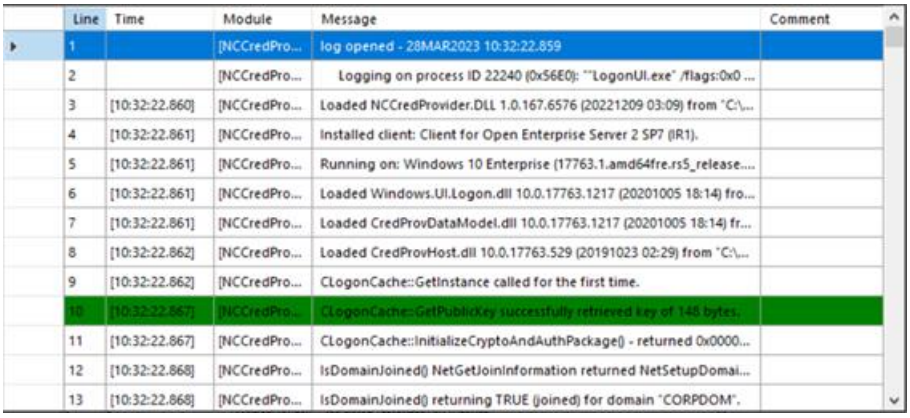


Line	Time	Module	Message	Comment
1	4/28/2023 4:13:23 PM		Report generated by: SLAnalyzer Version 9.0.1.4, 4/28/2...	
2	4/28/2023 4:13:23 PM	Computer ...	Computer Information	
3	4/28/2023 4:13:23 PM	Hardware	Hardware	
4	4/28/2023 4:13:23 PM	Hardware	Manufacturer: Dell Inc.	
5	4/28/2023 4:13:23 PM	Hardware	Model: Precision 5530	
6	4/28/2023 4:13:23 PM	Hardware	BIOS: 1.19.0	
7	4/28/2023 4:13:23 PM	Hardware	BIOS Date: 03/16/2021	
8	4/28/2023 4:13:23 PM	Hardware	Processor: AMD64	
9	4/28/2023 4:13:23 PM	Hardware	Processor Identifier: Intel64 Family 6 Model 158 Steppin...	
10	4/28/2023 4:13:23 PM	Hardware	Processor Level: 6	
11	4/28/2023 4:13:23 PM	Hardware	Processor Revision: 9e0a	
12	4/28/2023 4:13:23 PM	Hardware	# of Processors: 12	
13	4/28/2023 4:13:23 PM	OS version	OS version	

Figure 50 - Opened SLAnalyzer report

Opening a Novell Client credential provider log

Opens a credential provider log highlighting errors, warnings, etc.

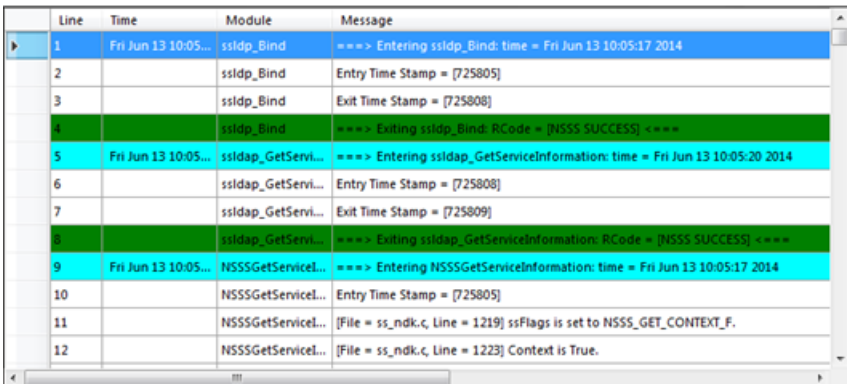


Line	Time	Module	Message	Comment
1		[NCCredPro...	log opened - 28MAR2023 10:32:22.859	
2		[NCCredPro...	Logging on process ID 22240 (0x56E0): ""LogonUI.exe" /flags:0x0 ...	
3	[10:32:22.860]	[NCCredPro...	Loaded NCCredProvider.DLL 1.0.167.6576 (20221209 03:09) from "C:\...	
4	[10:32:22.861]	[NCCredPro...	Installed client: Client for Open Enterprise Server 2 SP7 (IR1).	
5	[10:32:22.861]	[NCCredPro...	Running on: Windows 10 Enterprise (17763.1.amd64fre.rs5_release....	
6	[10:32:22.861]	[NCCredPro...	Loaded Windows.UI.Logon.dll 10.0.17763.1217 (20201005 18:14) fro...	
7	[10:32:22.861]	[NCCredPro...	Loaded CredProvDataModel.dll 10.0.17763.1217 (20201005 18:14) fr...	
8	[10:32:22.862]	[NCCredPro...	Loaded CredProvHost.dll 10.0.17763.529 (20191023 02:29) from "C:\...	
9	[10:32:22.862]	[NCCredPro...	CLogonCache::GetInstance called for the first time.	
10	[10:32:22.867]	[NCCredPro...	CLogonCache::GetPublicKey successfully retrieved key of 148 bytes.	
11	[10:32:22.867]	[NCCredPro...	CLogonCache::InitializeCryptoAndAuthPackage() - returned 0x0000...	
12	[10:32:22.868]	[NCCredPro...	IsDomainJoined() NetGetJoinInformation returned NetSetupDomai...	
13	[10:32:22.868]	[NCCredPro...	IsDomainJoined() returning TRUE (joined) for domain "CORPDOM".	

Figure 51 - Opened Novell client provider log

Opening a Novell SecretStore client debug log

Opens a SecretStore debug log highlighting errors, warnings, etc.

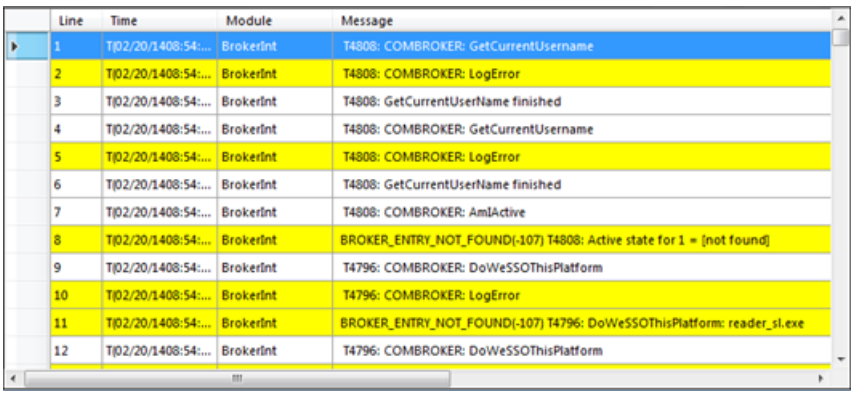


Line	Time	Module	Message
1	Fri Jun 13 10:05:...	ssldp_Bind	===> Entering ssldp_Bind: time = Fri Jun 13 10:05:17 2014
2		ssldp_Bind	Entry Time Stamp = [725805]
3		ssldp_Bind	Exit Time Stamp = [725808]
4		ssldp_Bind	<=== Exiting ssldp_Bind: RCode = [NSSS SUCCESS] <===
5	Fri Jun 13 10:05:...	ssldap_GetServi...	===> Entering ssldap_GetServiceInformation: time = Fri Jun 13 10:05:20 2014
6		ssldap_GetServi...	Entry Time Stamp = [725808]
7		ssldap_GetServi...	Exit Time Stamp = [725809]
8		ssldap_GetServi...	<=== Exiting ssldap_GetServiceInformation: RCode = [NSSS SUCCESS] <===
9	Fri Jun 13 10:05:...	NSSSGetServiceI...	===> Entering NSSSGetServiceInformation: time = Fri Jun 13 10:05:17 2014
10		NSSSGetServiceI...	Entry Time Stamp = [725805]
11		NSSSGetServiceI...	[File = ss_ndk.c, Line = 1219] ssFlags is set to NSSS_GET_CONTEXT_F.
12		NSSSGetServiceI...	[File = ss_ndk.c, Line = 1223] Context is True.

Figure 52 - Opened SecretStore debug log

Opening a SecureLogin Debug log

Opens a SecureLogin debug log (ssodebug.txt) for analysis. Most of the built-in filters apply to this log file type. Errors, warnings, and other informational items are colorized to aid in the analysis process.

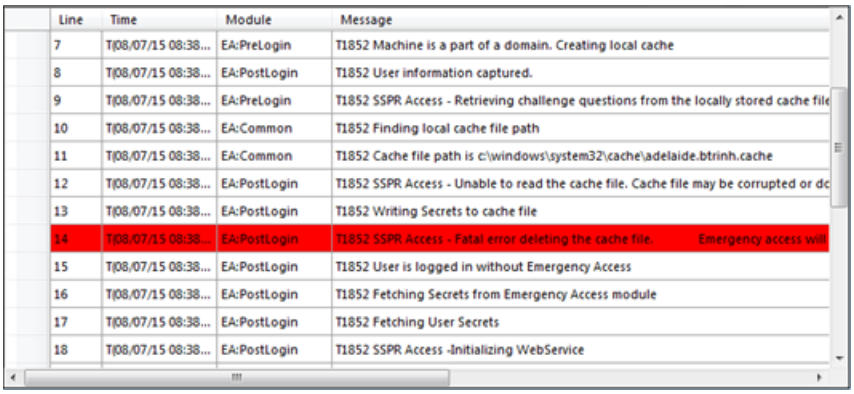


Line	Time	Module	Message
1	T[02/20/1408:54:...	BrokerInt	T4808: COMBROKER: GetCurrentUsername
2	T[02/20/1408:54:...	BrokerInt	T4808: COMBROKER: LogError
3	T[02/20/1408:54:...	BrokerInt	T4808: GetCurrentUserName finished
4	T[02/20/1408:54:...	BrokerInt	T4808: COMBROKER: GetCurrentUsername
5	T[02/20/1408:54:...	BrokerInt	T4808: COMBROKER: LogError
6	T[02/20/1408:54:...	BrokerInt	T4808: GetCurrentUserName finished
7	T[02/20/1408:54:...	BrokerInt	T4808: COMBROKER: AmIActive
8	T[02/20/1408:54:...	BrokerInt	BROKER_ENTRY_NOT_FOUND(-107) T4808: Active state for 1 = [not found]
9	T[02/20/1408:54:...	BrokerInt	T4796: COMBROKER: DoWeSSOThisPlatform
10	T[02/20/1408:54:...	BrokerInt	T4796: COMBROKER: LogError
11	T[02/20/1408:54:...	BrokerInt	BROKER_ENTRY_NOT_FOUND(-107) T4796: DoWeSSOThisPlatform: reader_sl.exe
12	T[02/20/1408:54:...	BrokerInt	T4796: COMBROKER: DoWeSSOThisPlatform

Figure 53 - Opened SecureLogin debug log

Opening a Client Login Extension Emergency Access Debug Log

Opens a SecureLogin debug log (ssodebug.txt) for analysis. Most of the built-in filters apply to this log file type. Errors, warnings, and other informational items are colorized to aid in the analysis process.

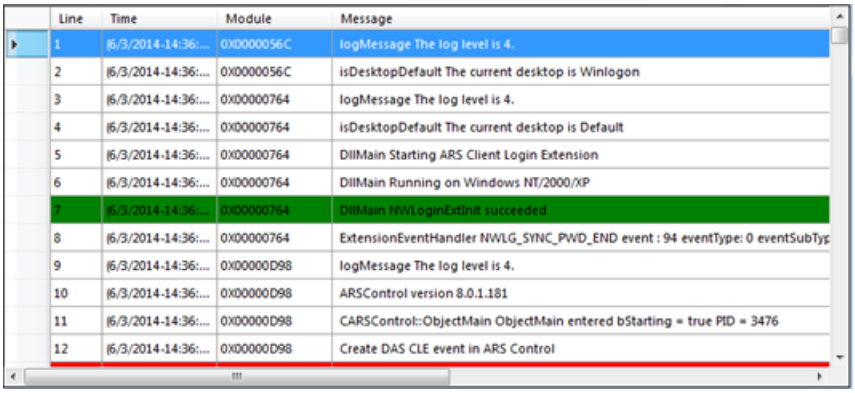


Line	Time	Module	Message
7	T(08/07/15 08:38...	EA:PreLogin	T1852 Machine is a part of a domain. Creating local cache
8	T(08/07/15 08:38...	EA:PostLogin	T1852 User information captured.
9	T(08/07/15 08:38...	EA:PreLogin	T1852 SSPR Access - Retrieving challenge questions from the locally stored cache file
10	T(08/07/15 08:38...	EA:Common	T1852 Finding local cache file path
11	T(08/07/15 08:38...	EA:Common	T1852 Cache file path is c:\windows\system32\cache\adelaide.btrinh.cache
12	T(08/07/15 08:38...	EA:PostLogin	T1852 SSPR Access - Unable to read the cache file. Cache file may be corrupted or do
13	T(08/07/15 08:38...	EA:PostLogin	T1852 Writing Secrets to cache file
14	T(08/07/15 08:38...	EA:PostLogin	T1852 SSPR Access - Fatal error deleting the cache file. Emergency access will
15	T(08/07/15 08:38...	EA:PostLogin	T1852 User is logged in without Emergency Access
16	T(08/07/15 08:38...	EA:PostLogin	T1852 Fetching Secrets from Emergency Access module
17	T(08/07/15 08:38...	EA:PostLogin	T1852 Fetching User Secrets
18	T(08/07/15 08:38...	EA:PostLogin	T1852 SSPR Access -Initializing WebService

Figure 54 - CLE eadebug.txt file

Opening a Desktop Automation Services debug log

Opens a desktop automation services log highlighting errors, warnings, etc.

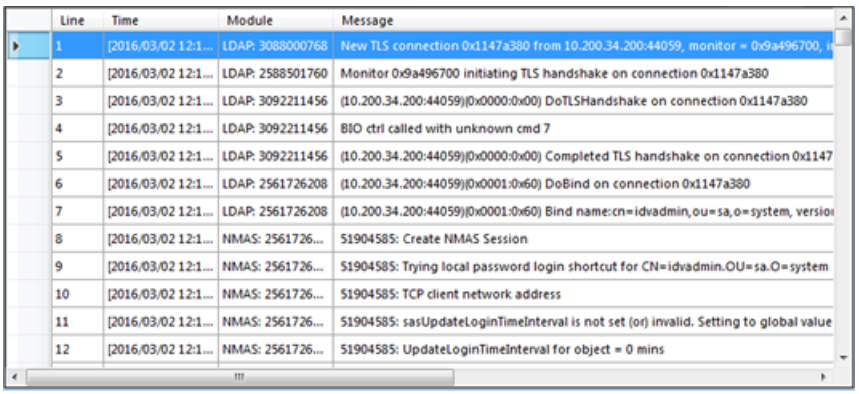


Line	Time	Module	Message
1	(6/3/2014-14:36:...	0X0000056C	logMessage The log level is 4.
2	(6/3/2014-14:36:...	0X0000056C	isDesktopDefault The current desktop is Winlogon
3	(6/3/2014-14:36:...	0X00000764	logMessage The log level is 4.
4	(6/3/2014-14:36:...	0X00000764	isDesktopDefault The current desktop is Default
5	(6/3/2014-14:36:...	0X00000764	DllMain Starting ARS Client Login Extension
6	(6/3/2014-14:36:...	0X00000764	DllMain Running on Windows NT/2000/XP
7	(6/3/2014-14:36:...	0X00000764	DllMain NWLoginExtInit succeeded
8	(6/3/2014-14:36:...	0X00000764	ExtensionEventHandler NWLG_SYNC_PWD_END event : 94 eventType: 0 eventSubTyp
9	(6/3/2014-14:36:...	0X00000D98	logMessage The log level is 4.
10	(6/3/2014-14:36:...	0X00000D98	ARSControl version 8.0.1.181
11	(6/3/2014-14:36:...	0X00000D98	CARSControl::ObjectMain ObjectMain entered bStarting = true PID = 3476
12	(6/3/2014-14:36:...	0X00000D98	Create DAS CLE event in ARS Control

Figure 55 - Opened DAS log

Opening an NDS trace file

Opens an NDS trace file and formats the data for easier viewing and processing.



Line	Time	Module	Message
1	[2016/03/02 12:1...	LDAP: 3088000768	New TLS connection 0x1147a380 from 10.200.34.200:44059, monitor = 0x9a496700, i
2	[2016/03/02 12:1...	LDAP: 2588501760	Monitor 0x9a496700 initiating TLS handshake on connection 0x1147a380
3	[2016/03/02 12:1...	LDAP: 3092211456	(10.200.34.200:44059)[0x0000:0x00] DoTLSHandshake on connection 0x1147a380
4	[2016/03/02 12:1...	LDAP: 3092211456	BIO ctrl called with unknown cmd 7
5	[2016/03/02 12:1...	LDAP: 3092211456	(10.200.34.200:44059)[0x0000:0x00] Completed TLS handshake on connection 0x1147
6	[2016/03/02 12:1...	LDAP: 2561726208	(10.200.34.200:44059)[0x0001:0x60] DoBind on connection 0x1147a380
7	[2016/03/02 12:1...	LDAP: 2561726208	(10.200.34.200:44059)[0x0001:0x60] Bind name:cn=idvadmin,ou=sa,o=system, versio
8	[2016/03/02 12:1...	NMAS: 2561726...	S1904585: Create NMAS Session
9	[2016/03/02 12:1...	NMAS: 2561726...	S1904585: Trying local password login shortcut for CN=idvadmin.OU=sa.O=system
10	[2016/03/02 12:1...	NMAS: 2561726...	S1904585: TCP client network address
11	[2016/03/02 12:1...	NMAS: 2561726...	S1904585: sasUpdateLoginTimeInterval is not set (or) invalid. Setting to global value
12	[2016/03/02 12:1...	NMAS: 2561726...	S1904585: UpdateLoginTimeInterval for object = 0 mins

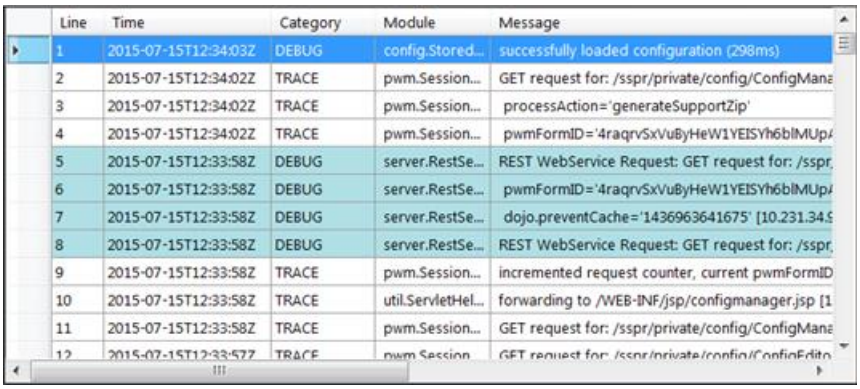
Figure 56 - Opened NDS trace file

Opening a SSPR Support Bundle

Opens a compressed SSPR support bundle package. (file: SSPR-Support.zip).
In addition to opening the compressed package this option can also be used to open any of the files contained within the support bundle (IE .log, .json, csv, txt. and .xml)

Opening a SSPR Support Bundle debug log file

Opens a SSPR debug log file highlighting errors, warnings, etc.



Line	Time	Category	Module	Message
1	2015-07-15T12:34:03Z	DEBUG	config.Stored...	successfully loaded configuration (298ms)
2	2015-07-15T12:34:02Z	TRACE	pwm.Session...	GET request for: /sspr/private/config/ConfigMana
3	2015-07-15T12:34:02Z	TRACE	pwm.Session...	processAction='generateSupportZip'
4	2015-07-15T12:34:02Z	TRACE	pwm.Session...	pwmFormID='4raqrvSxVuByHeW1YEISYh6blMUpA
5	2015-07-15T12:33:58Z	DEBUG	server.RestSe...	REST WebService Request: GET request for: /sspr
6	2015-07-15T12:33:58Z	DEBUG	server.RestSe...	pwmFormID='4raqrvSxVuByHeW1YEISYh6blMUpA
7	2015-07-15T12:33:58Z	DEBUG	server.RestSe...	dojo.preventCache='1436963641675' [10.231.34.5
8	2015-07-15T12:33:58Z	DEBUG	server.RestSe...	REST WebService Request: GET request for: /sspr
9	2015-07-15T12:33:58Z	TRACE	pwm.Session...	incremented request counter, current pwmFormID
10	2015-07-15T12:33:58Z	TRACE	util.ServletHel...	forwarding to /WEB-INF/jsp/configmanager.jsp [1
11	2015-07-15T12:33:58Z	TRACE	pwm.Session...	GET request for: /sspr/private/config/ConfigMana
12	2015-07-15T12:33:57Z	TRACE	pwm.Session...	GET request for: /sspr/private/config/ConfigEdito

Figure 57 - Opened SSPR debug log

Opening a SSPR Support Bundle json or txt file

Opens a file of the type .json or .txt. This option will utilize the JSON log file reader to parse the respective file.



Figure 58 - Opened JSON file

Opening a SSPR Support Bundle xml file

Opens a file of type .xml and will display the xml data window. This window allows you to browse the settings defined in the xml file.

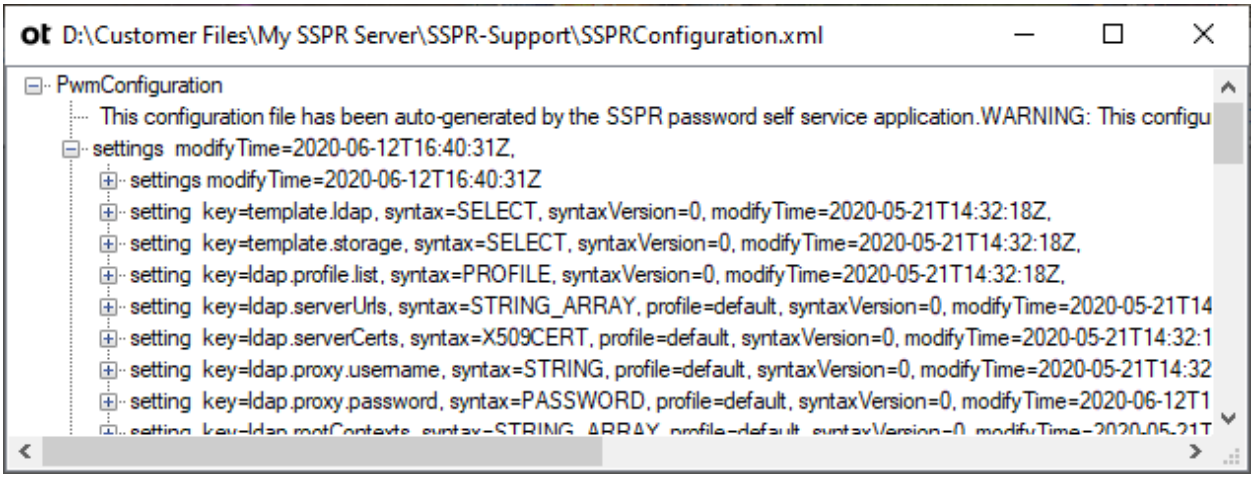
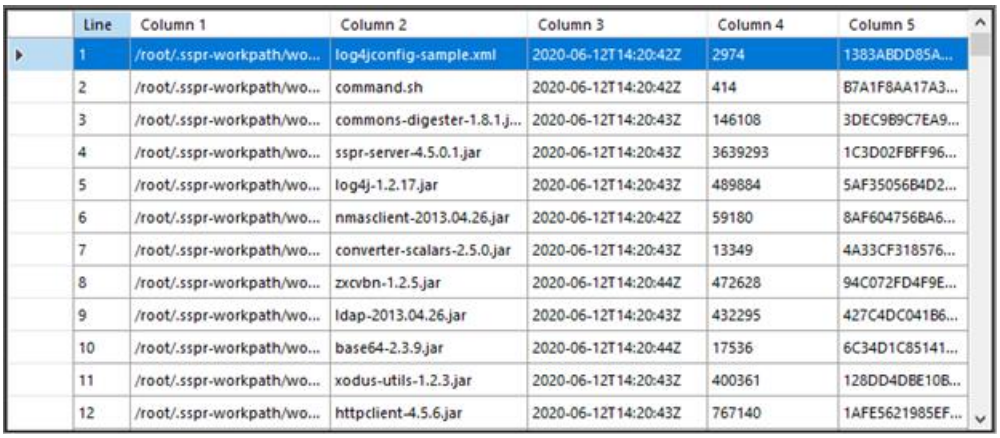


Figure 59 - Opened XML file

Opening a SSPR Support Bundle csv file

Open a comma-separated values file (csv file) and will format and display each column found.

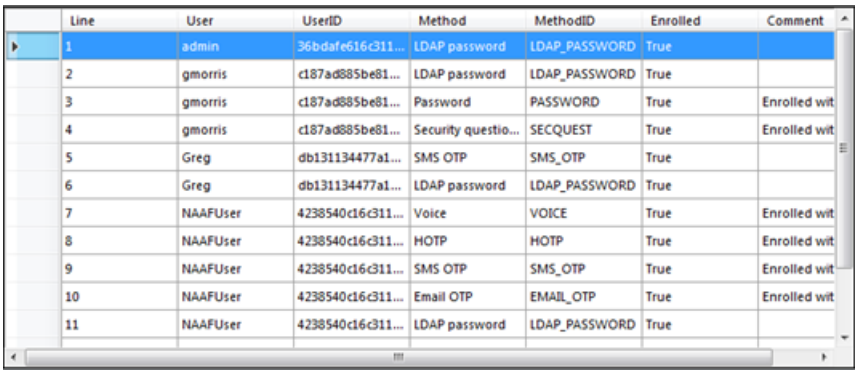


Line	Column 1	Column 2	Column 3	Column 4	Column 5
1	/root/.sspr-workpath/wo...	log4jconfig-sample.xml	2020-06-12T14:20:42Z	2974	1383ABDD85A...
2	/root/.sspr-workpath/wo...	command.sh	2020-06-12T14:20:42Z	414	B7A1F8AA17A3...
3	/root/.sspr-workpath/wo...	commons-digester-1.8.1.j...	2020-06-12T14:20:43Z	146108	3DEC9B9C7EA9...
4	/root/.sspr-workpath/wo...	sspr-server-4.5.0.1.jar	2020-06-12T14:20:43Z	3639293	1C3D02FBFF96...
5	/root/.sspr-workpath/wo...	log4j-1.2.17.jar	2020-06-12T14:20:43Z	489884	5AF35056B4D2...
6	/root/.sspr-workpath/wo...	nmasclient-2013.04.26.jar	2020-06-12T14:20:42Z	59180	8AF604756BA6...
7	/root/.sspr-workpath/wo...	converter-scalars-2.5.0.jar	2020-06-12T14:20:43Z	13349	4A33CF318576...
8	/root/.sspr-workpath/wo...	zxcvbn-1.2.5.jar	2020-06-12T14:20:44Z	472628	94C072FD4F9E...
9	/root/.sspr-workpath/wo...	ldap-2013.04.26.jar	2020-06-12T14:20:43Z	432295	427C4DC041B6...
10	/root/.sspr-workpath/wo...	base64-2.3.9.jar	2020-06-12T14:20:44Z	17536	6C34D1C85141...
11	/root/.sspr-workpath/wo...	xodus-utils-1.2.3.jar	2020-06-12T14:20:43Z	400361	128DD4DBE10B...
12	/root/.sspr-workpath/wo...	httpclient-4.5.6.jar	2020-06-12T14:20:43Z	767140	1AFE5621985EF...

Figure 60 - Opened csv file

Opening a AAF Database

SLAnalyzer has the ability to generate a report of users that have enrolled AAF methods. Follow the steps outlined in the AAF Rest section to generate an AAF Database.

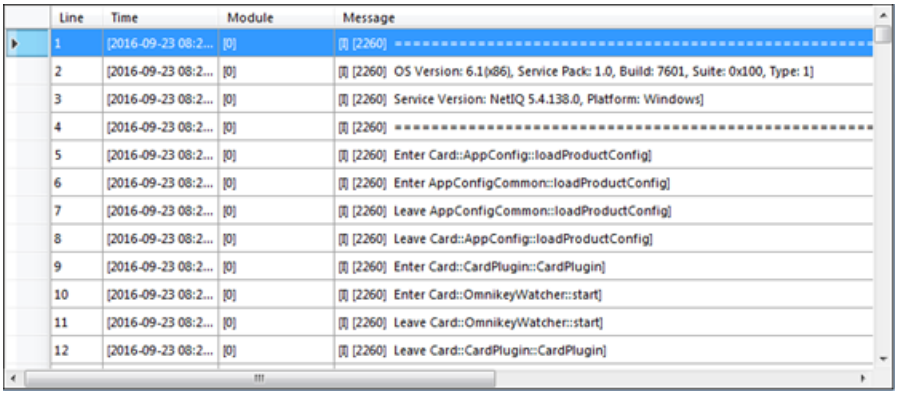


Line	User	UserID	Method	MethodID	Enrolled	Comment
1	admin	36bdafe616c311...	LDAP password	LDAP_PASSWORD	True	
2	gmorris	c187ad885be81...	LDAP password	LDAP_PASSWORD	True	
3	gmorris	c187ad885be81...	Password	PASSWORD	True	Enrolled wit
4	gmorris	c187ad885be81...	Security questio...	SECQUEST	True	Enrolled wit
5	Greg	db131134477a1...	SMS OTP	SMS_OTP	True	
6	Greg	db131134477a1...	LDAP password	LDAP_PASSWORD	True	
7	NAAFUser	4238540c16c311...	Voice	VOICE	True	Enrolled wit
8	NAAFUser	4238540c16c311...	HOTP	HOTP	True	Enrolled wit
9	NAAFUser	4238540c16c311...	SMS OTP	SMS_OTP	True	Enrolled wit
10	NAAFUser	4238540c16c311...	Email OTP	EMAIL_OTP	True	Enrolled wit
11	NAAFUser	4238540c16c311...	LDAP password	LDAP_PASSWORD	True	

Figure 61 - Opened AAF Database

Opening a AAF Debug Log

SLAnalyzer will attempt to parse all of the AAF debug log file types.

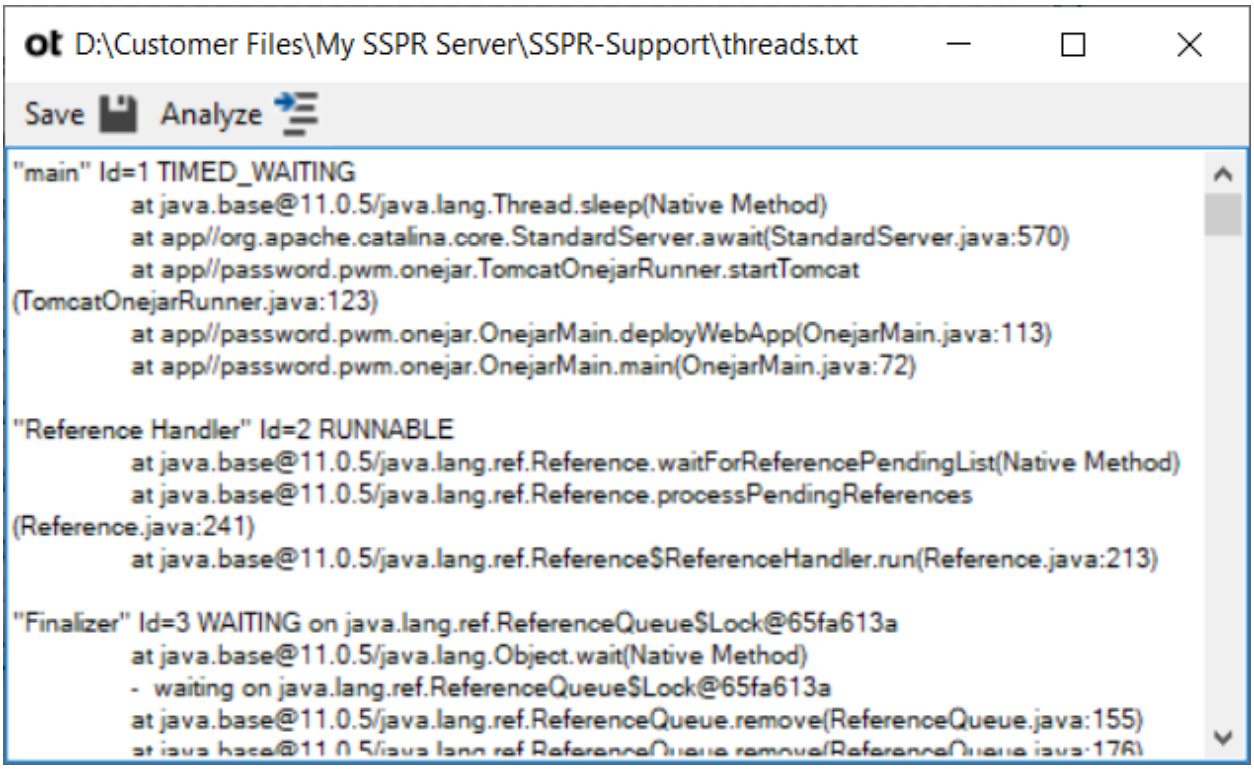


Line	Time	Module	Message
1	[2016-09-23 08:2...	[0]	[I] [2260] ==========
2	[2016-09-23 08:2...	[0]	[I] [2260] OS Version: 6.1(x86), Service Pack: 1.0, Build: 7601, Suite: 0x100, Type: 1]
3	[2016-09-23 08:2...	[0]	[I] [2260] Service Version: NetIQ 5.4.138.0, Platform: Windows]
4	[2016-09-23 08:2...	[0]	[I] [2260] ==========
5	[2016-09-23 08:2...	[0]	[I] [2260] Enter Card::AppConfig::loadProductConfig]
6	[2016-09-23 08:2...	[0]	[I] [2260] Enter AppConfigCommon::loadProductConfig]
7	[2016-09-23 08:2...	[0]	[I] [2260] Leave AppConfigCommon::loadProductConfig]
8	[2016-09-23 08:2...	[0]	[I] [2260] Leave Card::AppConfig::loadProductConfig]
9	[2016-09-23 08:2...	[0]	[I] [2260] Enter Card::CardPlugin::CardPlugin]
10	[2016-09-23 08:2...	[0]	[I] [2260] Enter Card::OmnikeyWatcher::start]
11	[2016-09-23 08:2...	[0]	[I] [2260] Leave Card::OmnikeyWatcher::start]
12	[2016-09-23 08:2...	[0]	[I] [2260] Leave Card::CardPlugin::CardPlugin]

Figure 62 - Opened AAF Debug Log

Opening a text file with the Generic log reader

When SLAnalyzer doesn't know how to handle the file type then it will attempt to open the file as generic text.



Clicking the Analyze button will open log (text file) and highlights warnings, errors, etc.

	Line	Message	Comment
▶	1	"main" Id=1 TIMED_WAITING	
	2	at java.base@11.0.5/java.lang.Thread.sleep(Native Method)	
	3	at app//org.apache.catalina.core.StandardServer.await(StandardServer.java:570)	
	4	at app//password.pwm.onejar.TomcatOnejarRunner.startTomcat(TomcatOnejarRu...	
	5	at app//password.pwm.onejar.OnejarMain.deployWebApp(OnejarMain.java:113)	
	6	at app//password.pwm.onejar.OnejarMain.main(OnejarMain.java:72)	
	7		
	8	"Reference Handler" Id=2 RUNNABLE	
	9	at java.base@11.0.5/java.lang.ref.Reference.waitForReferencePendingList(Native ...	
	10	at java.base@11.0.5/java.lang.ref.Reference.processPendingReferences(Reference...	
	11	at java.base@11.0.5/java.lang.ref.Reference$ReferenceHandler.run(Reference.java...	
	12		
	13	"Finalizer" Id=3 WAITING on java.lang.ref.ReferenceQueue$Lock@65fa613a	

Figure 63 - Log file opened with the generic log reader

Opening a Comma-Separated Values (CSV) file

Opens a csv file highlighting any errors, warnings, etc.

When loading a csv file typically the first line of the file provides the column names. SLAnalyzer will prompt the user if they want to use the first line as the column header names or to assign default column names. Answering No will display
Column 1, Column 2, etc...

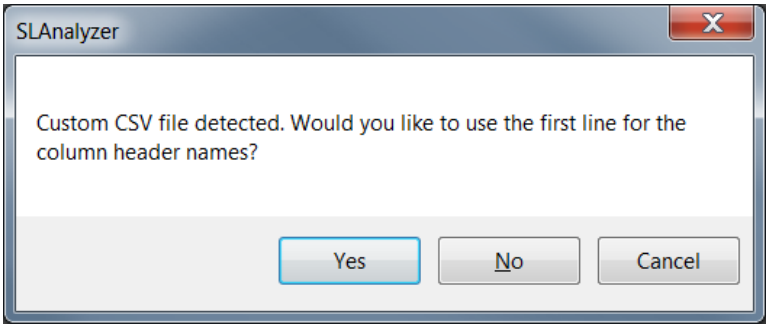
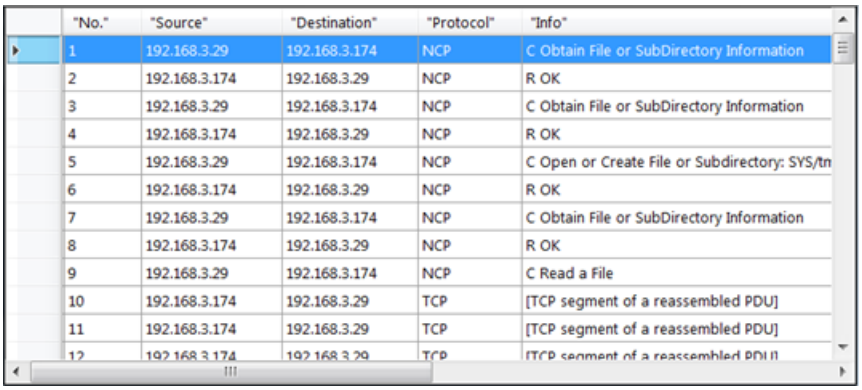


Figure 64 - CSV header prompt



"No."	"Source"	"Destination"	"Protocol"	"Info"
1	192.168.3.29	192.168.3.174	NCP	C Obtain File or SubDirectory Information
2	192.168.3.174	192.168.3.29	NCP	R OK
3	192.168.3.29	192.168.3.174	NCP	C Obtain File or SubDirectory Information
4	192.168.3.174	192.168.3.29	NCP	R OK
5	192.168.3.29	192.168.3.174	NCP	C Open or Create File or Subdirectory: SYS/tn
6	192.168.3.174	192.168.3.29	NCP	R OK
7	192.168.3.29	192.168.3.174	NCP	C Obtain File or SubDirectory Information
8	192.168.3.174	192.168.3.29	NCP	R OK
9	192.168.3.29	192.168.3.174	NCP	C Read a File
10	192.168.3.174	192.168.3.29	TCP	[TCP segment of a reassembled PDU]
11	192.168.3.174	192.168.3.29	TCP	[TCP segment of a reassembled PDU]
12	192.168.3.174	192.168.3.29	TCP	[TCP segment of a reassembled PDU]

Figure 65 - Opened csv file

Opening a JSON formatted file (JSON)

If the content of the log file is determined to be JSON data the JSON data window will display the formatted data.



Figure 66 - Formatted JSON data window

Opening an XML formatted file (XML)

If the content of the log file is determined to be XML data the XML data window will be displayed with the formatted data.

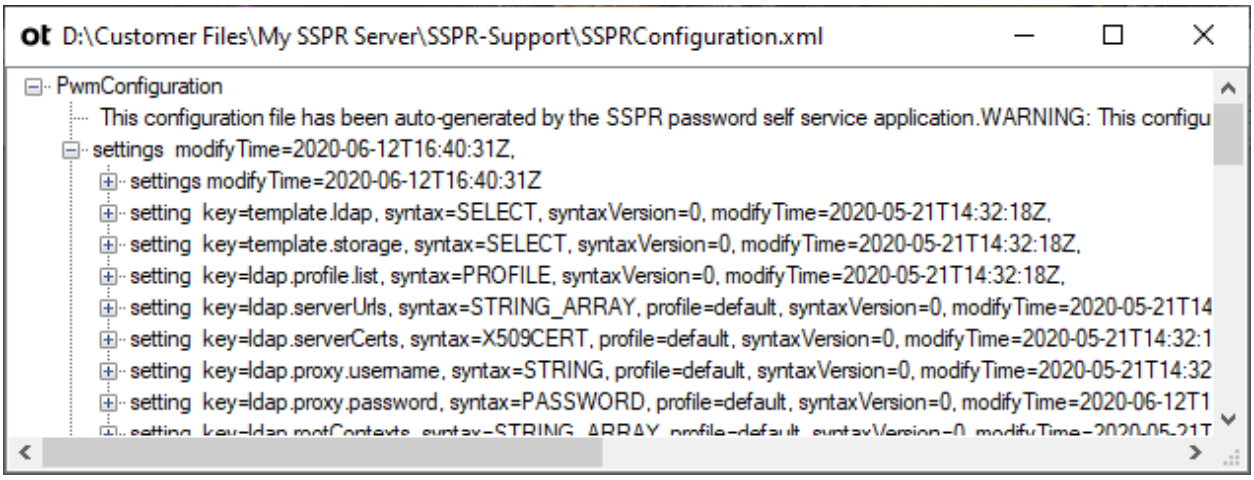


Figure 67 - Formatted XML data window

Note: XML files can include additional support modules. When opening an XML file that links another file (dtd) if SLAnalyzer is unable to locate the file specified, it will present an error message to the user. To open this xml file, place a copy of the missing file in the path specified.

Opening a HyperText Markup formatted file (HTM/HTML/URL)

SLAnalyzer will detect HTML files when they have the file extension of htm, html or url. The file will be opened with the built-in internal web browser control.

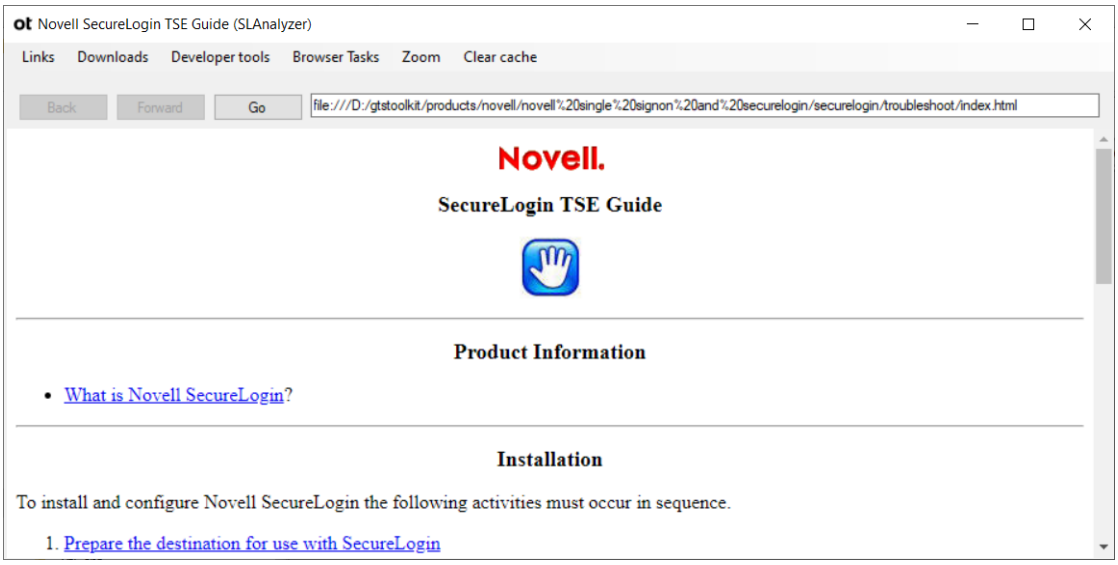


Figure 68 - Opened html file

Note that some URL files created with old browsers are actually xml data files that reference content on a web server. These types of URL files will be opened as a text file and not as a website.

Opening a ZEN message log

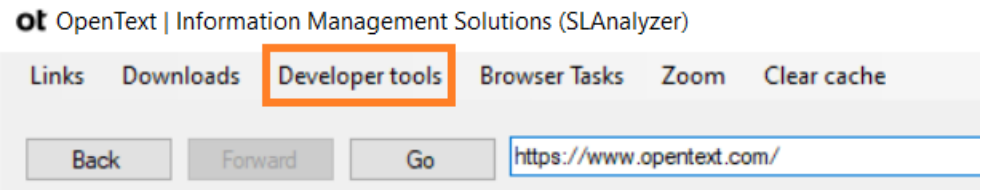
SLAnalyzer will detect ZEN message logs. It will display the information in proper columns, automatically build module filters, and highlight errors and other conditions.



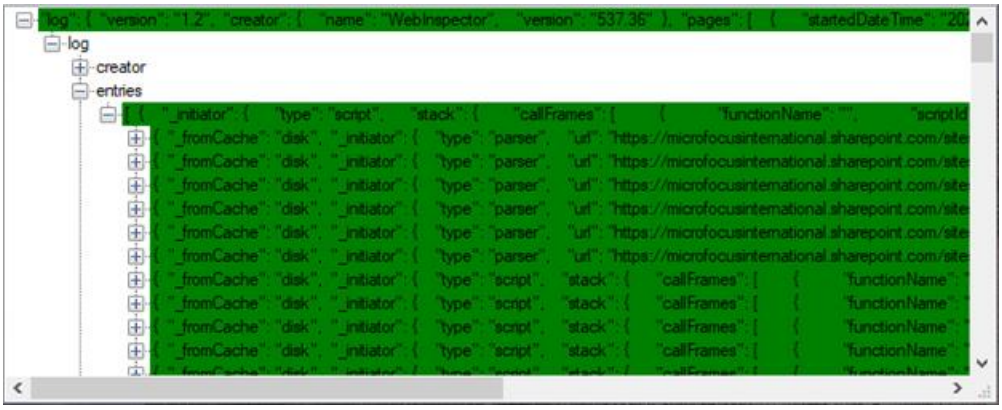
Figure 69 - Opened ZEN message log

Opening a HAR log file

HAR log files are created by browser developer tools option (F12 key in most browsers). Starting with version 9.0 of SLAnalyzer the internal browser is Chromium based and includes the developer tools option.



A Har log is a text based file that lists the request/reply information that occurred during that browser session.



Under the entries section of the file are the packets captured during the browser session.

Expand each request/reply structure by clicking the + symbol at the beginning of the line.

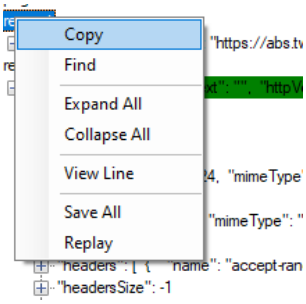


The HAR file display in SLAnalyzer has a couple of features to allow for:

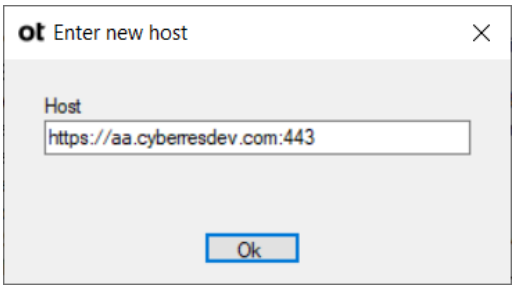
- Replaying packet
- Viewing content returned by server
- Downloading content returned by server

Replaying a HAR file packet

To replay a packet, expand the desired request/reply packet and then right click on the header “request”. The menu will display the option “Replay”

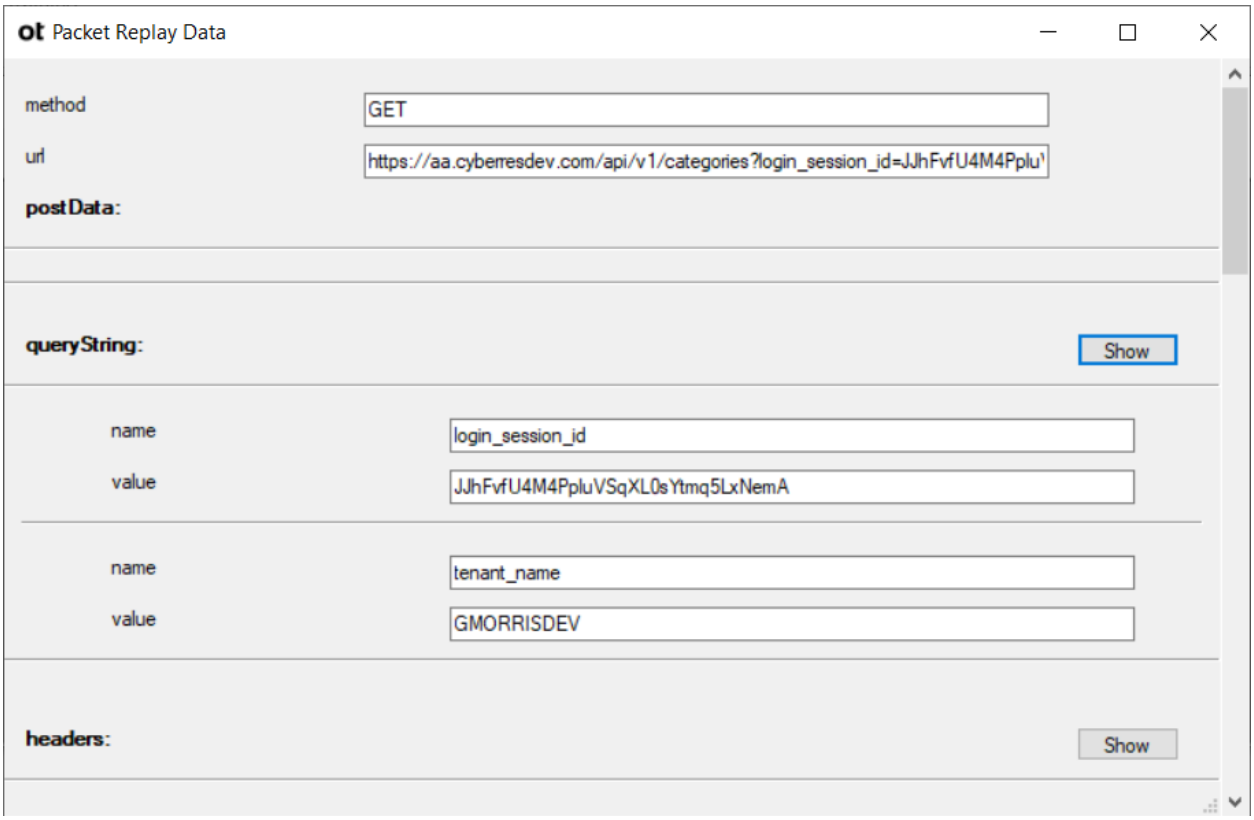


When replaying a request, SLAnalyzer will prompt for the destination server. The original server is listed but this can be changed to point to a different server.



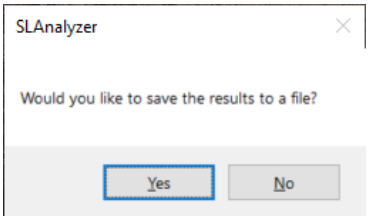
Accepting the host listed simply replays the packet to the original server. By entering a new server then this same packet will be sent to the server defined.

After selecting the desired host, SLAnalyzer will allow the user to modify the headers and other parameters for the call.

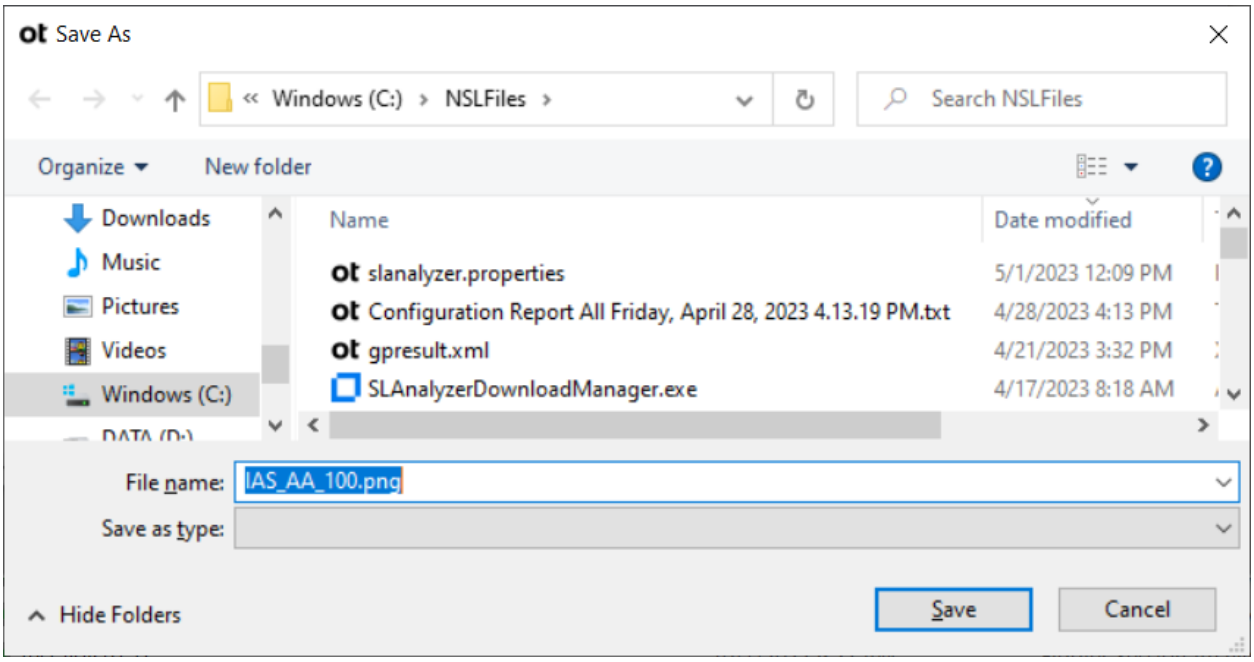


Click the Ok button at the bottom of the page to send the packet defined to the specified host.

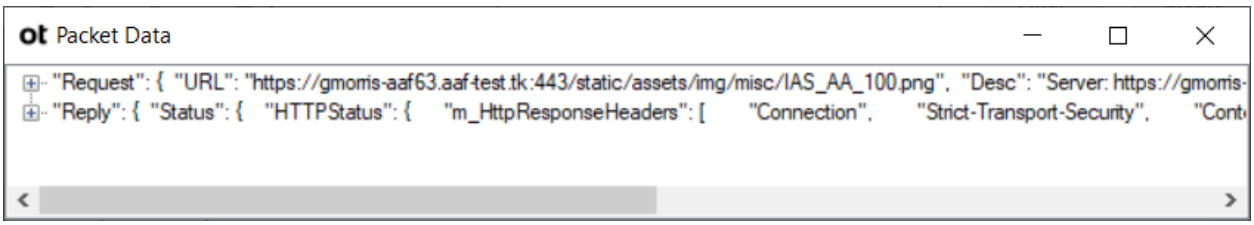
After the packet has been sent then SLAnalyzer will prompt if the user would like to save the response to a file.



Clicking Yes will display a file browser to save the information/data that was returned by the server. In this example the original request was for an image (png). The filename in the original request is automatically populated into the File name field.

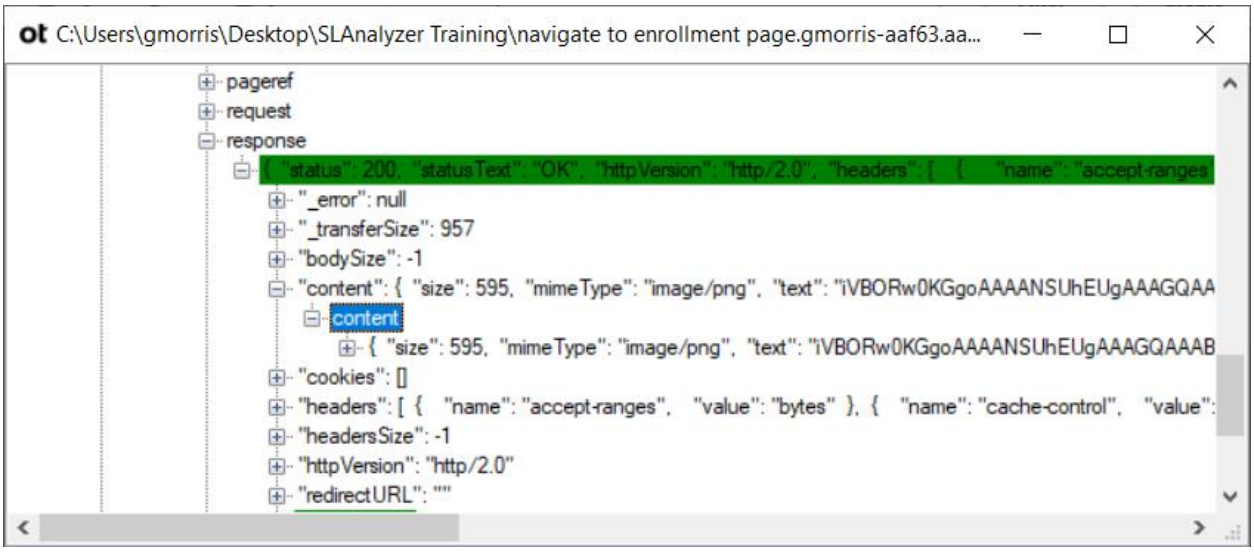


If there was no content or if the user has clicked no to save the response then a new window will be displayed showing the packet request/reply data.

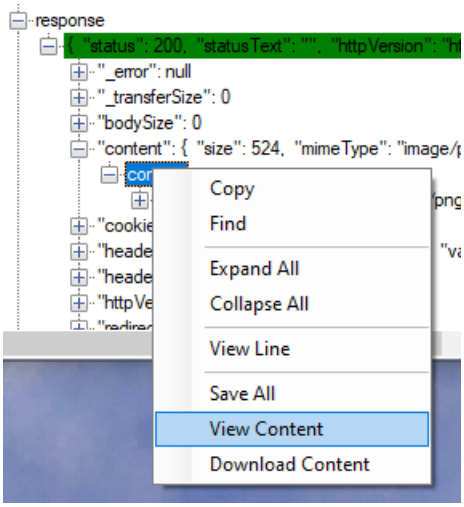


Viewing content from HAR file

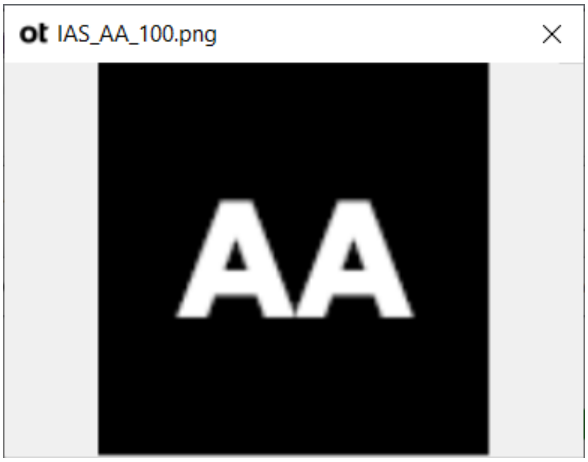
If the HAR file was saved with content then in the reply packet the returned information would have captured the response data. This in most cases is an image or some type of script. Expand the Reply packet until you see the header “content”.



Right click on the header “content” and then select View Content



SLAnalyzer will then extract the content from the HAR file and display the data.



Downloading content

The process for download is the same as the process for viewing content from a HAR file. Instead from the context menu select Download Content instead of View Content.

After selecting Download Content SLAnalyzer will display a file browser to allow the user to specify the file name and or download location.

Save

The Save menu option allows comments made to log files to be saved. For details see the previous section, “Comments”

Close

The Close menu option closes any open tools or log window. Cleans up temporary files and closes any open resources. If comments had been performed but not yet saved, then SLAnalyzer will prompt the user to save the modified comments. (See notes on comments for more details)

Exit

The Exit menu option closes the SLAnalyzer application. If comments had been performed but not yet saved, then SLAnalyzer will prompt the user to save the modified comments. (See notes on comments for more details)

Analyze Menu

The Analyze menu allows the user to select several different types of reports. Each report will contain error and warning messages that pertain to the tests performed within the analysis.

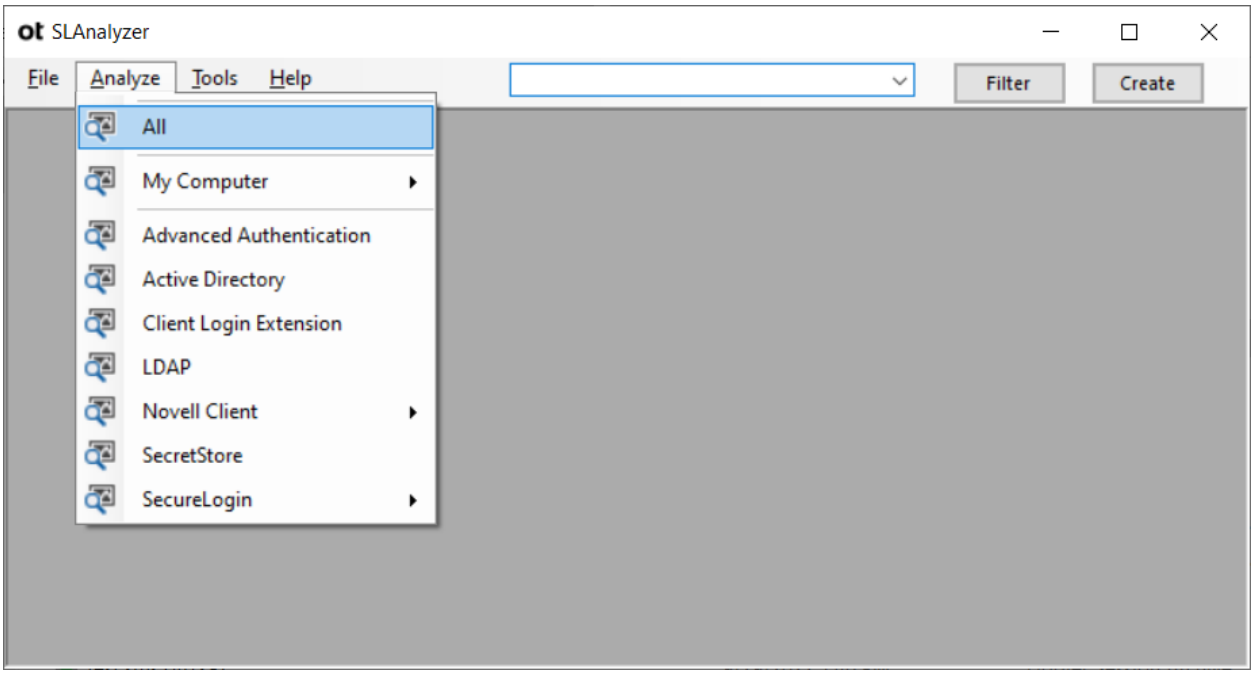


Figure 70 - Analyze menu

Configuration Report Window

When the user selects one of the Analyze Reports, SLAnalyzer will display the Configuration Report window. This will display the information found and the results of tests performed during the analysis. The information contained within this window will be different based upon the Analysis report selected.

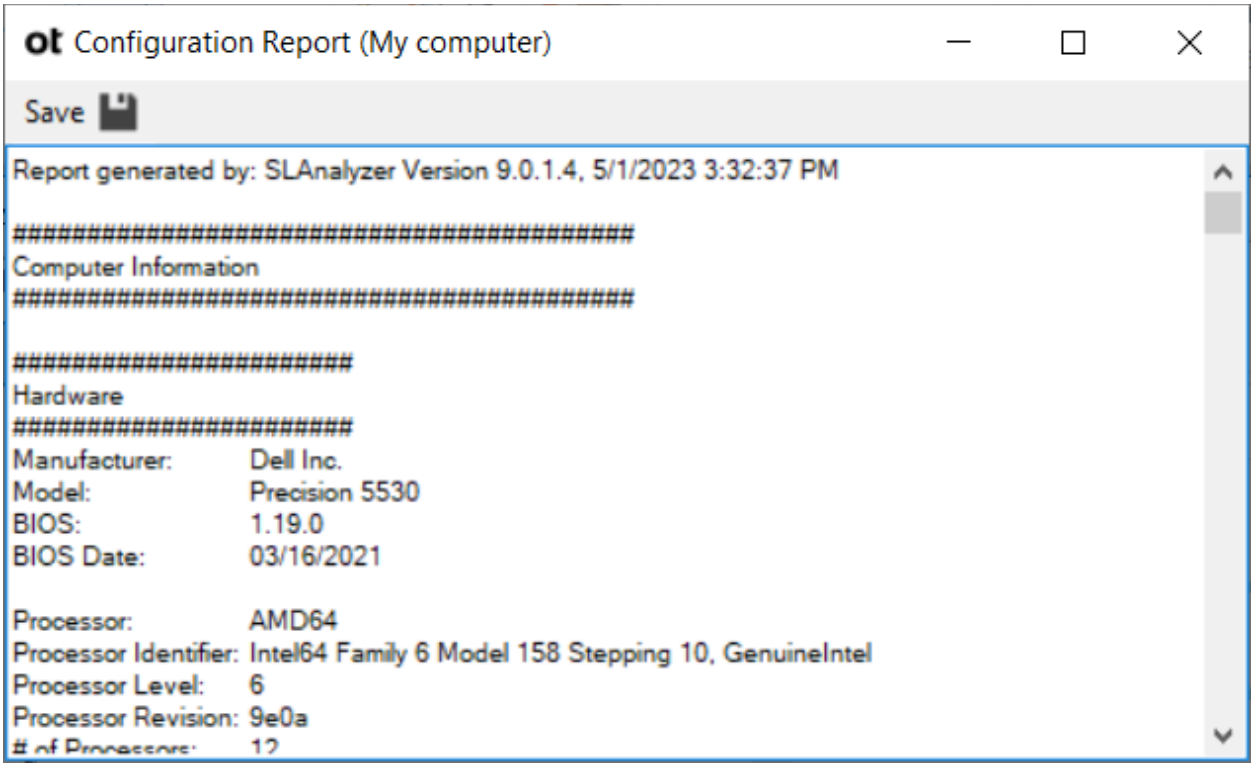


Figure 71 - Configuration Report

Saving report information

After the analysis is completed then the user can save the report by clicking on the Save button in the upper left corner of the window. Hovering the mouse over the Save button will display the location where the report file will be created.

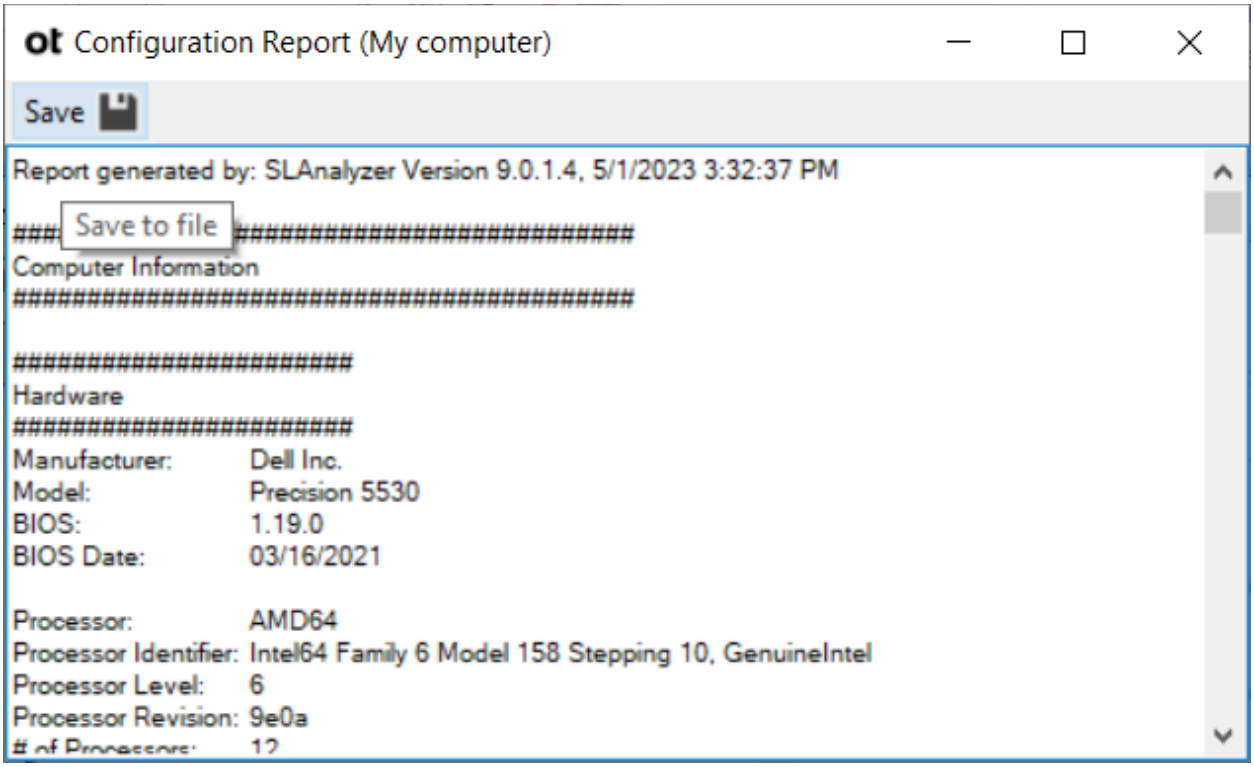


Figure 72 - Click to save tip

By default, SLAnalyzer will attempt to save the report to the default log file location.

There are two types of file formats supported:

- Report Format (*.txt)
- XML (*.xml)

Saving report as Report Format (.txt)*

The default file type is Report Format (*.txt). Clicking the save button will create the report with the name provided in the File name field and as the type text.

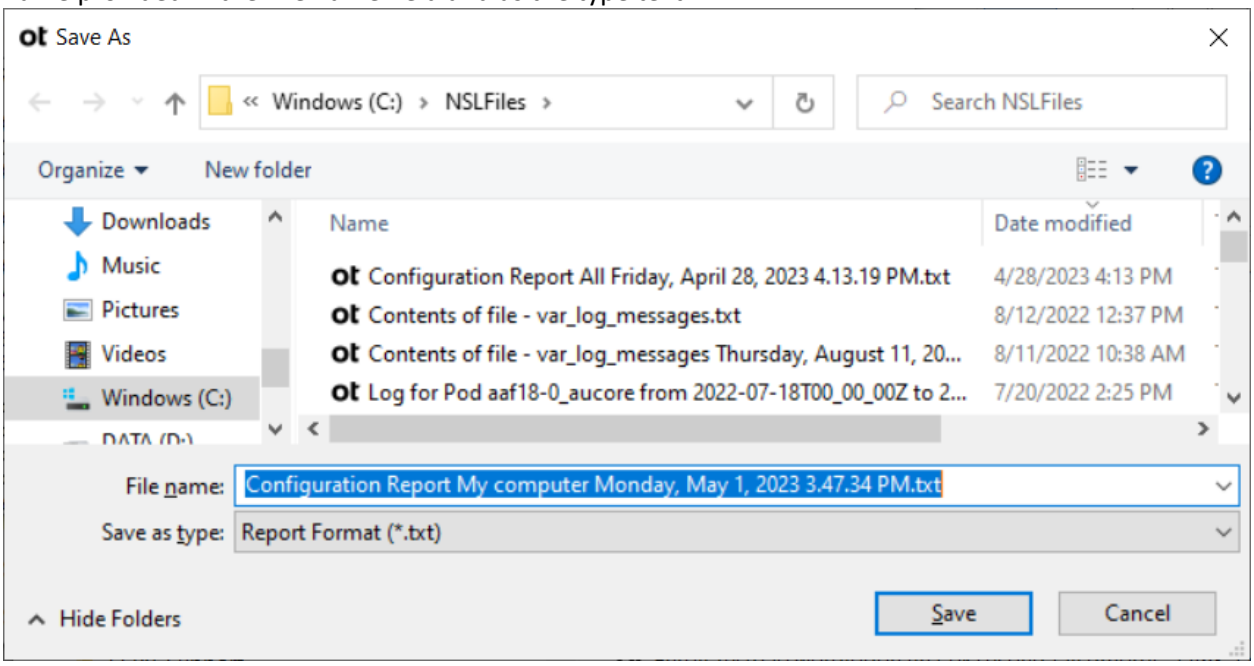


Figure 73 – Save report as Report Format (*.txt)

Saving report as XML Format (.xml)*

To save the report in an XML formatted file, then click the Save as type button and select XML (*.xml). Then click the Save button to create the report with the File name selected as type xml.

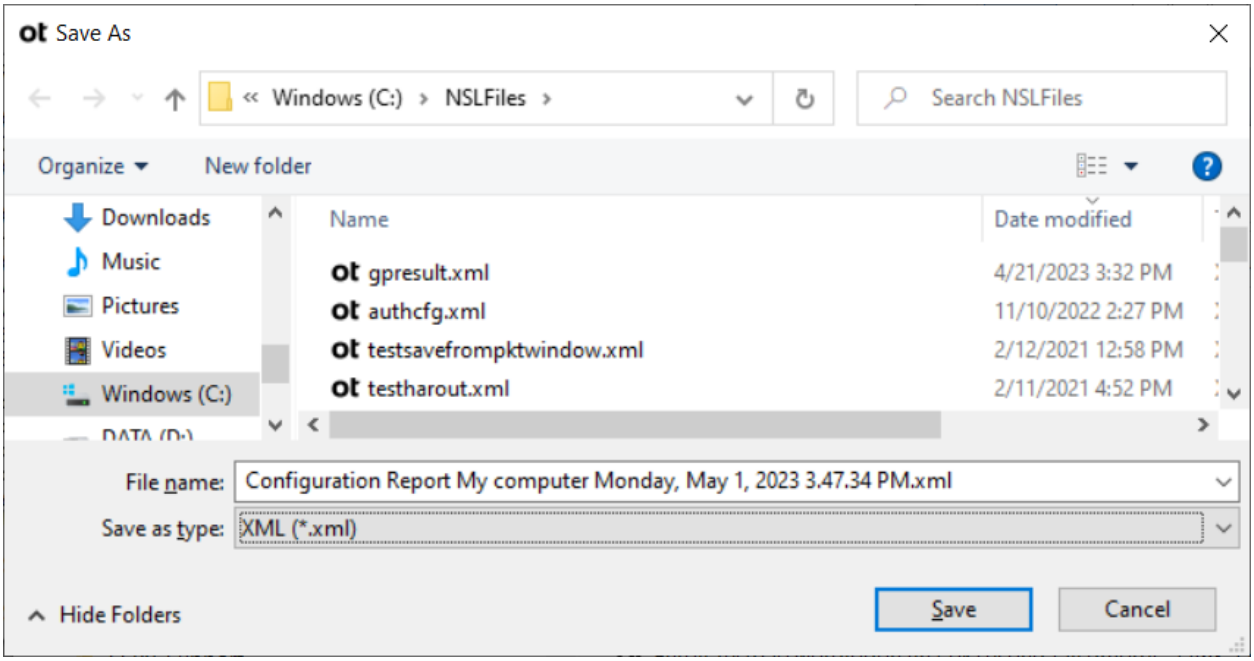
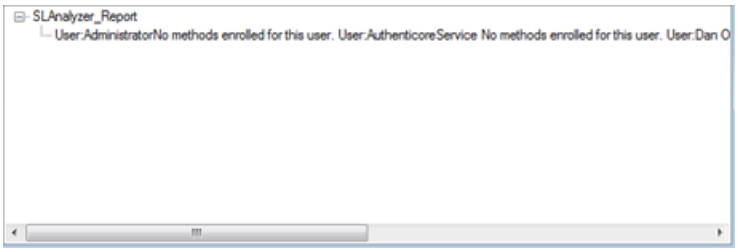


Figure 74 - Save report as XML (*.xml)

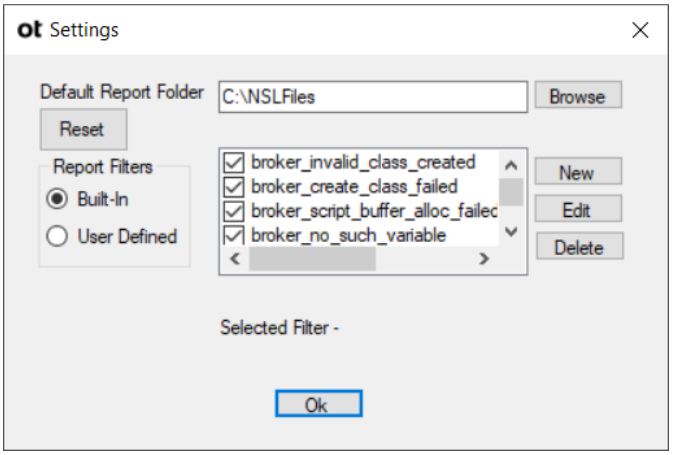
Note that the Default report folder can be changed in the SLAnalyzer settings under the Tools menu. Alternatively, the user can use the mouse and right click, then click “select all” followed by “copy”. This will copy the selected text to the system copy/paste buffer. The user can then paste the copied data into any valid text editor.

XML report formatting

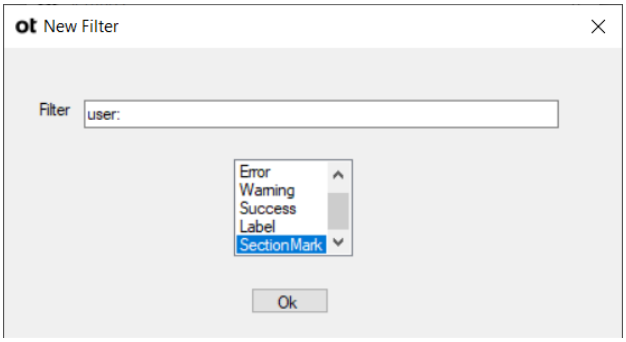
SLAnalyzer will attempt to format the XML output based upon hardcoded section breaks. But in some cases, the output format needs to be customized. As we can see in the below window the XML data is displayed in a single entry/line. It would be easier to read if we could break on the text “User:”.



Create a new section header in SLAnalyzer (Tools/Configure SLAnalyzer)



Click the New button and specify the new section header



Now resave the report as XML and the new section header will be used.



Available Reports

- All
- My Computer
- AAF
- AD
- CLE
- LDAP
- Novell Client
- SecretStore
- SecureLogin

All

This option runs all reports for the installed configuration. Some of the analysis is based upon the installed configuration of SecureLogin. If SecureLogin is not installed on the workstation, then the individual reports might need to be selected.

The following reports are generated when the run all reports is selected:

- My Computer
- SecureLogin
- Client Login Extension
- AAF

Note that if any of the reports listed fails then analysis of that section is aborted. The next report in the list will then be evaluated and executed.

For example, if the SecureLogin client is not installed then the whole SecureLogin section will be skipped.

Workstations running CLE only would receive a report of

- Computer Information
- Registry keys
- Debug logging status
- Client Login Extension

My Computer

This option reports local computer information. When clicking on the menu item My Computer the following reports will be generated. Clicking on a sub item will generate just the selected report.

- Hardware
- OS version
- Network/Credential providers
- Authentication providers
- Installed Software
- Installed System components
- Startup Applications
- Internet Browser configuration
- Environment variables
- Network information (ipconfig)
- ARP table
- Available Resources
- DNS cache
- Debug Logging
- Group Policy summary
- TCP Ports
- Routing table

The following optional reports that can be generated individually.

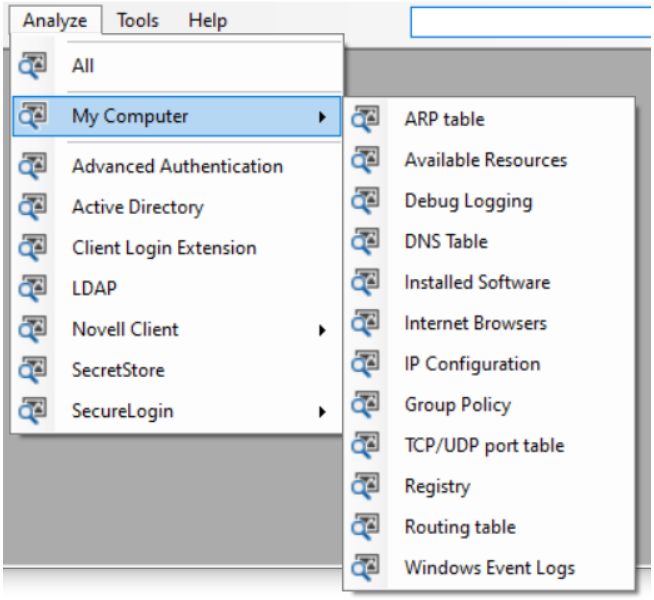


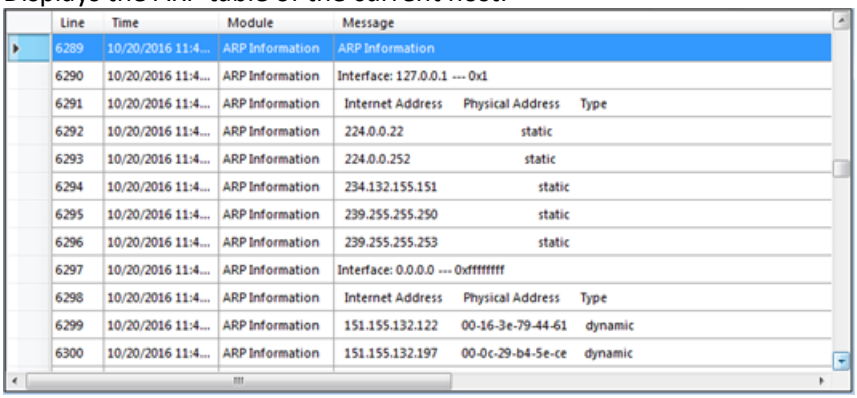
Figure 75 - Optional My Computer reports

Clicking My Computer will run all reports except for the Windows Event Logs. To generate the Windows Event Logs report you must select the item from the Analyze/My Computer menu.

The following details the optional My Computer reports that can be generated individually.

ARP table

Displays the ARP table of the current host.



Line	Time	Module	Message
6289	10/20/2016 11:4...	ARP Information	ARP Information
6290	10/20/2016 11:4...	ARP Information	Interface: 127.0.0.1 --- 0x1
6291	10/20/2016 11:4...	ARP Information	Internet Address Physical Address Type
6292	10/20/2016 11:4...	ARP Information	224.0.0.22 static
6293	10/20/2016 11:4...	ARP Information	224.0.0.252 static
6294	10/20/2016 11:4...	ARP Information	234.132.155.151 static
6295	10/20/2016 11:4...	ARP Information	239.255.255.250 static
6296	10/20/2016 11:4...	ARP Information	239.255.255.253 static
6297	10/20/2016 11:4...	ARP Information	Interface: 0.0.0.0 --- 0xffffffff
6298	10/20/2016 11:4...	ARP Information	Internet Address Physical Address Type
6299	10/20/2016 11:4...	ARP Information	151.155.132.122 00-16-3e-79-44-61 dynamic
6300	10/20/2016 11:4...	ARP Information	151.155.132.197 00-0c-29-b4-5e-ce dynamic

Figure 76 - My Computer/ARP table

My Computer/Available Resources

This option reports the information seen in task manager regarding the running processes of the workstation.

Note that to get the full information about all running processes then you need to execute SLAnalyzer with the Runas Administrator option. Otherwise only the processes ran by the current logged in user will provide full details about the process.

The resource data provided includes:

- Product Name
- Version
- Description
- Path and filename
- Company
- Language
- Process ID
- Start time
- CPU utilization
- Memory Usage
- Response status
- Priority

My Computer/Debug Logging

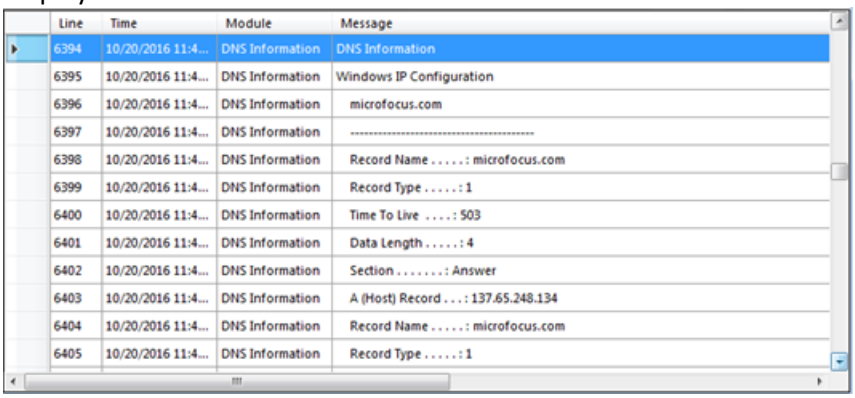
This option reports the status of debug logging based upon entries in the registry of the workstation.

The following logging options are checked.

- User and Machine level debug logging for SecureLogin
- User and Machine level debug logging for SecureLogin virtual channel
- User and Machine level debug logging for SecureLogin LDAP Gina
- User and Machine level debug logging for Novell client for Windows
- User and Machine level debug logging for NMAS client
- User and Machine level debug logging for SecretStore client
- User and Machine level debug logging for SecureWorkstation
- User and Machine level debug logging for Desktop Automation Services (DAS)
- User and Machine level debug logging for Client Login Extension (CLE)
- User and Machine level debug logging for PCProx

My Computer/DNS Table

Displays the DNS table of the current host.

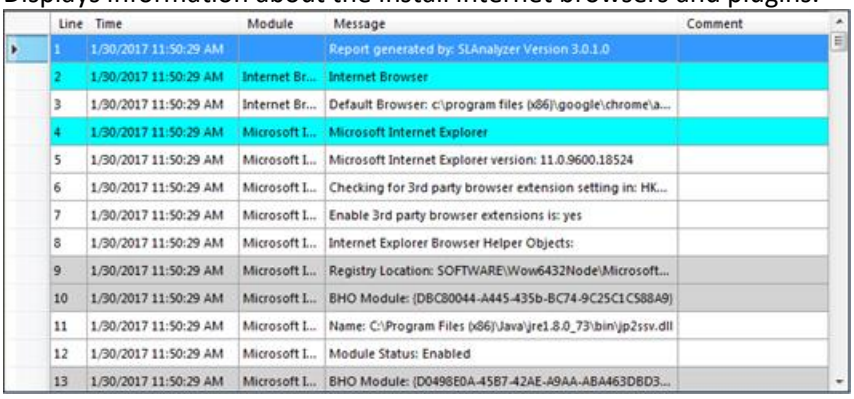


Line	Time	Module	Message
6394	10/20/2016 11:4...	DNS Information	DNS Information
6395	10/20/2016 11:4...	DNS Information	Windows IP Configuration
6396	10/20/2016 11:4...	DNS Information	microfocus.com
6397	10/20/2016 11:4...	DNS Information	----------
6398	10/20/2016 11:4...	DNS Information	Record Name . . . . . : microfocus.com
6399	10/20/2016 11:4...	DNS Information	Record Type . . . . . : 1
6400	10/20/2016 11:4...	DNS Information	Time To Live . . . . : 503
6401	10/20/2016 11:4...	DNS Information	Data Length . . . . . : 4
6402	10/20/2016 11:4...	DNS Information	Section . . . . . : Answer
6403	10/20/2016 11:4...	DNS Information	A (Host) Record . . . : 137.65.248.134
6404	10/20/2016 11:4...	DNS Information	Record Name . . . . . : microfocus.com
6405	10/20/2016 11:4...	DNS Information	Record Type . . . . . : 1

Figure 77 - My Computer/DNS Information

My Computer/Internet Browsers

Displays information about the install internet browsers and plugins.

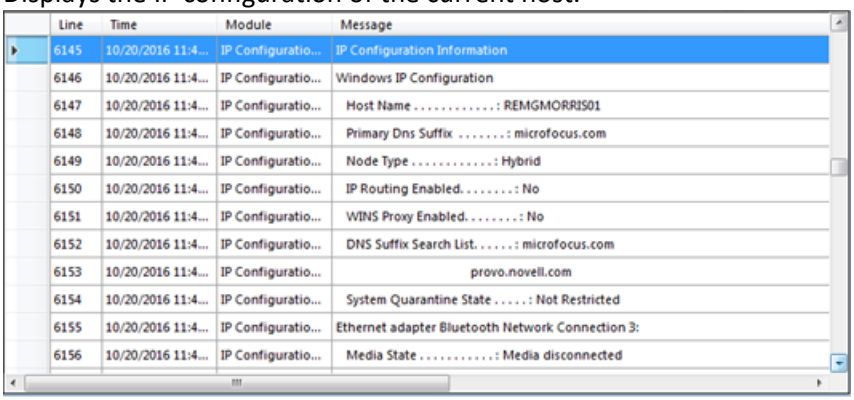


Line	Time	Module	Message	Comment
1	1/30/2017 11:50:29 AM		Report generated by: SLAnalyzer Version 3.0.1.0	
2	1/30/2017 11:50:29 AM	Internet Br...	Internet Browser	
3	1/30/2017 11:50:29 AM	Internet Br...	Default Browser: c:\program files (x86)\google\chrome\a...	
4	1/30/2017 11:50:29 AM	Microsoft I...	Microsoft Internet Explorer	
5	1/30/2017 11:50:29 AM	Microsoft I...	Microsoft Internet Explorer version: 11.0.9600.18524	
6	1/30/2017 11:50:29 AM	Microsoft I...	Checking for 3rd party browser extension setting in: HK...	
7	1/30/2017 11:50:29 AM	Microsoft I...	Enable 3rd party browser extensions is: yes	
8	1/30/2017 11:50:29 AM	Microsoft I...	Internet Explorer Browser Helper Objects:	
9	1/30/2017 11:50:29 AM	Microsoft I...	Registry Location: SOFTWARE\Wow6432Node\Microsoft...	
10	1/30/2017 11:50:29 AM	Microsoft I...	BHO Module: {DBC80044-A445-435b-BC74-9C25C1C588A9}	
11	1/30/2017 11:50:29 AM	Microsoft I...	Name: C:\Program Files (x86)\Java\jre1.8.0_73\bin\jp2ssv.dll	
12	1/30/2017 11:50:29 AM	Microsoft I...	Module Status: Enabled	
13	1/30/2017 11:50:29 AM	Microsoft I...	BHO Module: {D0498E0A-45B7-42AE-A9AA-ABA463DBD3...	

Figure 78 - My Computer/Internet Browsers

My Computer/IP Configuration

Displays the IP configuration of the current host.

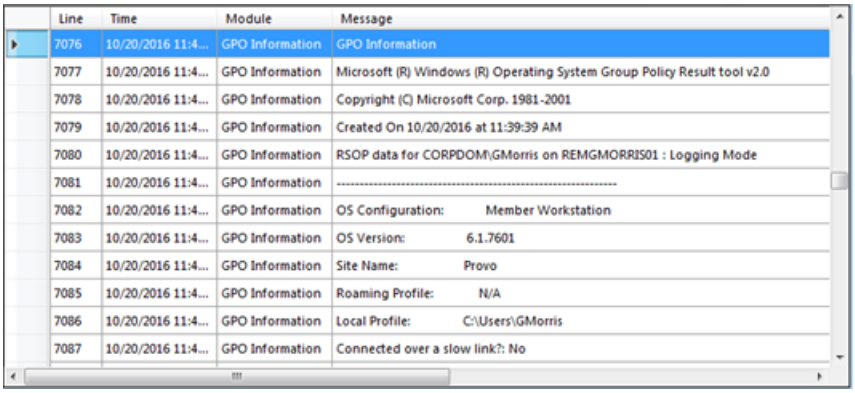


Line	Time	Module	Message
6145	10/20/2016 11:4...	IP Configuratio...	IP Configuration Information
6146	10/20/2016 11:4...	IP Configuratio...	Windows IP Configuration
6147	10/20/2016 11:4...	IP Configuratio...	Host Name . . . . . : REMGMORRIS01
6148	10/20/2016 11:4...	IP Configuratio...	Primary Dns Suffix . . . . . : microfocus.com
6149	10/20/2016 11:4...	IP Configuratio...	Node Type . . . . . : Hybrid
6150	10/20/2016 11:4...	IP Configuratio...	IP Routing Enabled. . . . . : No
6151	10/20/2016 11:4...	IP Configuratio...	WINS Proxy Enabled. . . . . : No
6152	10/20/2016 11:4...	IP Configuratio...	DNS Suffix Search List. . . . . : microfocus.com
6153	10/20/2016 11:4...	IP Configuratio...	provo.novell.com
6154	10/20/2016 11:4...	IP Configuratio...	System Quarantine State . . . . . : Not Restricted
6155	10/20/2016 11:4...	IP Configuratio...	Ethernet adapter Bluetooth Network Connection 3:
6156	10/20/2016 11:4...	IP Configuratio...	Media State . . . . . : Media disconnected

Figure 79 - My Computer/IP configuration

My Computer/Group Policy

This option generates the GPO summary report. The information is generated from the gpresult /r command.

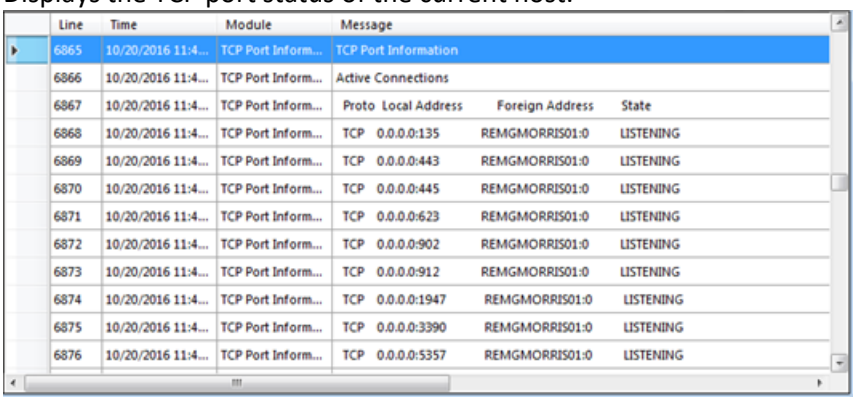


Line	Time	Module	Message
7076	10/20/2016 11:4...	GPO Information	GPO Information
7077	10/20/2016 11:4...	GPO Information	Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
7078	10/20/2016 11:4...	GPO Information	Copyright (C) Microsoft Corp. 1981-2001
7079	10/20/2016 11:4...	GPO Information	Created On 10/20/2016 at 11:39:39 AM
7080	10/20/2016 11:4...	GPO Information	RSOP data for CORPDOM\GMorris on REMGMORRIS01 : Logging Mode
7081	10/20/2016 11:4...	GPO Information	----------
7082	10/20/2016 11:4...	GPO Information	OS Configuration: Member Workstation
7083	10/20/2016 11:4...	GPO Information	OS Version: 6.1.7601
7084	10/20/2016 11:4...	GPO Information	Site Name: Provo
7085	10/20/2016 11:4...	GPO Information	Roaming Profile: N/A
7086	10/20/2016 11:4...	GPO Information	Local Profile: C:\Users\GMorris
7087	10/20/2016 11:4...	GPO Information	Connected over a slow link?: No

Figure 80 - My Computer/GPO Information

My Computer/TCP port table

Displays the TCP port status of the current host.



Line	Time	Module	Message			
6865	10/20/2016 11:4...	TCP Port Inform...	TCP Port Information			
6866	10/20/2016 11:4...	TCP Port Inform...	Active Connections			
6867	10/20/2016 11:4...	TCP Port Inform...	Proto	Local Address	Foreign Address	State
6868	10/20/2016 11:4...	TCP Port Inform...	TCP	0.0.0.0:135	REMGMORRIS01:0	LISTENING
6869	10/20/2016 11:4...	TCP Port Inform...	TCP	0.0.0.0:443	REMGMORRIS01:0	LISTENING
6870	10/20/2016 11:4...	TCP Port Inform...	TCP	0.0.0.0:445	REMGMORRIS01:0	LISTENING
6871	10/20/2016 11:4...	TCP Port Inform...	TCP	0.0.0.0:623	REMGMORRIS01:0	LISTENING
6872	10/20/2016 11:4...	TCP Port Inform...	TCP	0.0.0.0:902	REMGMORRIS01:0	LISTENING
6873	10/20/2016 11:4...	TCP Port Inform...	TCP	0.0.0.0:912	REMGMORRIS01:0	LISTENING
6874	10/20/2016 11:4...	TCP Port Inform...	TCP	0.0.0.0:1947	REMGMORRIS01:0	LISTENING
6875	10/20/2016 11:4...	TCP Port Inform...	TCP	0.0.0.0:3390	REMGMORRIS01:0	LISTENING
6876	10/20/2016 11:4...	TCP Port Inform...	TCP	0.0.0.0:5357	REMGMORRIS01:0	LISTENING

Figure 81 - My Computer/TCP port information

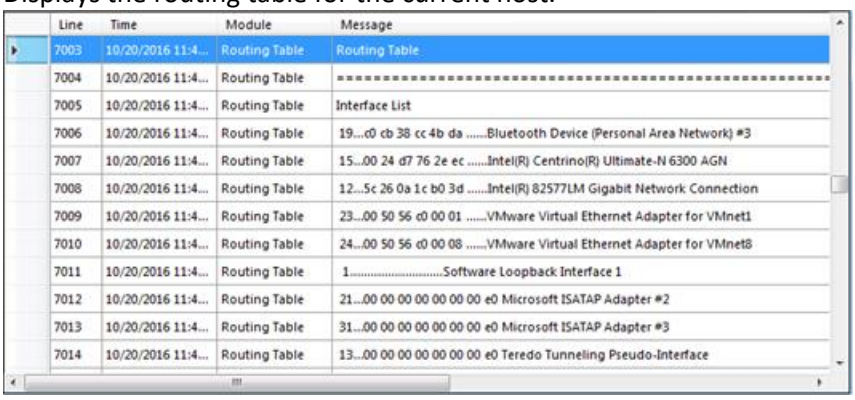
My Computer/Registry

This option displays the information stored in the following registry key locations

- (HKLM and HKCU)\SOFTWARE\Protocom\SecureLogin
- (HKLM and HKCU)\SOFTWARE\Novell
- (HKLM and HKCU)\SOFTWARE\Wow6432Node\SecureLogin
- (HKLM and HKCU)\SOFTWARE\Wow6432Node\Novell

My Computer/Routing table

Displays the routing table for the current host.



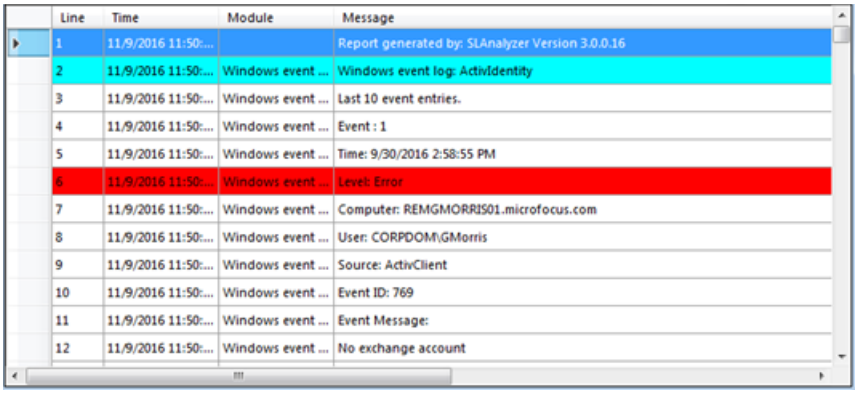
Line	Time	Module	Message
7003	10/20/2016 11:4...	Routing Table	Routing Table
7004	10/20/2016 11:4...	Routing Table	==========
7005	10/20/2016 11:4...	Routing Table	Interface List
7006	10/20/2016 11:4...	Routing Table	19...c0 cb 38 cc 4b da .....Bluetooth Device (Personal Area Network) #3
7007	10/20/2016 11:4...	Routing Table	15...00 24 d7 76 2e ec .....Intel(R) Centrino(R) Ultimate-N 6300 AGN
7008	10/20/2016 11:4...	Routing Table	12...5c 26 0a 1c b0 3d .....Intel(R) 82577LM Gigabit Network Connection
7009	10/20/2016 11:4...	Routing Table	23...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
7010	10/20/2016 11:4...	Routing Table	24...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
7011	10/20/2016 11:4...	Routing Table	1.....Software Loopback Interface 1
7012	10/20/2016 11:4...	Routing Table	21...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
7013	10/20/2016 11:4...	Routing Table	31...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
7014	10/20/2016 11:4...	Routing Table	13...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface

Figure 82 - My Computer/Routing table

My Computer/Windows Event Logs

Displays the last 10 events from each of the logs found on the current host.

Note that you must run SLAnalyzer with administrative rights (runAs Administrator) to generate this report.

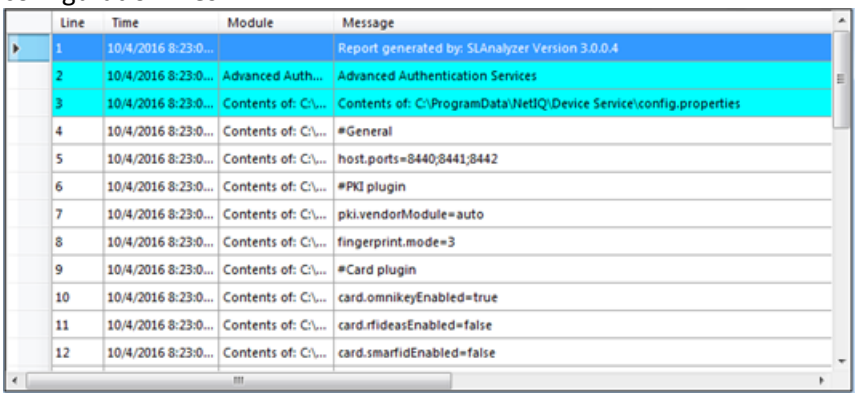


Line	Time	Module	Message
1	11/9/2016 11:50:...		Report generated by: SLAnalyzer Version 3.0.0.16
2	11/9/2016 11:50:...	Windows event ...	Windows event log: ActivIdentity
3	11/9/2016 11:50:...	Windows event ...	Last 10 event entries.
4	11/9/2016 11:50:...	Windows event ...	Event : 1
5	11/9/2016 11:50:...	Windows event ...	Time: 9/30/2016 2:58:55 PM
6	11/9/2016 11:50:...	Windows event ...	Level: Error
7	11/9/2016 11:50:...	Windows event ...	Computer: REMGMORRIS01.microfocus.com
8	11/9/2016 11:50:...	Windows event ...	User: CORPDOM\GMorris
9	11/9/2016 11:50:...	Windows event ...	Source: ActivClient
10	11/9/2016 11:50:...	Windows event ...	Event ID: 769
11	11/9/2016 11:50:...	Windows event ...	Event Message:
12	11/9/2016 11:50:...	Windows event ...	No exchange account

Figure 83 – My Computer/Windows event logs

AAF

This option will generate a report on the Advanced Authentication Framework Windows client and configuration files.



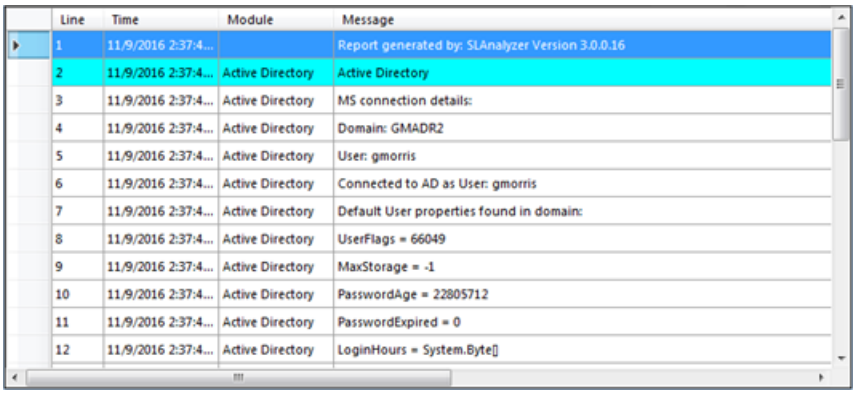
Line	Time	Module	Message
1	10/4/2016 8:23:0...		Report generated by: SLAnalyzer Version 3.0.0.4
2	10/4/2016 8:23:0...	Advanced Auth...	Advanced Authentication Services
3	10/4/2016 8:23:0...	Contents of: C:\...	Contents of: C:\ProgramData\NetIQ\Device Service\config.properties
4	10/4/2016 8:23:0...	Contents of: C:\...	#General
5	10/4/2016 8:23:0...	Contents of: C:\...	host.ports=8440;8441;8442
6	10/4/2016 8:23:0...	Contents of: C:\...	#PKI plugin
7	10/4/2016 8:23:0...	Contents of: C:\...	pki.vendorModule=auto
8	10/4/2016 8:23:0...	Contents of: C:\...	fingerprint.mode=3
9	10/4/2016 8:23:0...	Contents of: C:\...	#Card plugin
10	10/4/2016 8:23:0...	Contents of: C:\...	card.omnikeyEnabled=true
11	10/4/2016 8:23:0...	Contents of: C:\...	card.rfideasEnabled=false
12	10/4/2016 8:23:0...	Contents of: C:\...	card.smartidEnabled=false

Figure 84 - Analyze AAF

AD

This option reports AD client information. Also attempts to connect through Microsoft client and read the NSL attributes. AD information is gathered from the workstation environment settings. Workstation must be joined to a domain to have these valid settings. (USERDOMAIN, USERNAME, LOGONSERVER)

- Display logged on user and domain
    - Connect to AD server
    - Read and display SecureLogin attributes found on user

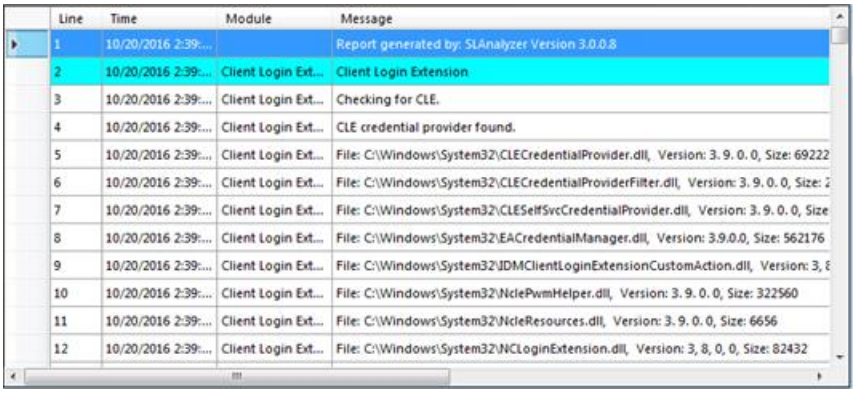


Line	Time	Module	Message
1	11/9/2016 2:37:4...		Report generated by: SLAnalyzer Version 3.0.0.16
2	11/9/2016 2:37:4...	Active Directory	Active Directory
3	11/9/2016 2:37:4...	Active Directory	MS connection details:
4	11/9/2016 2:37:4...	Active Directory	Domain: GMADR2
5	11/9/2016 2:37:4...	Active Directory	User: gmorris
6	11/9/2016 2:37:4...	Active Directory	Connected to AD as User: gmorris
7	11/9/2016 2:37:4...	Active Directory	Default User properties found in domain:
8	11/9/2016 2:37:4...	Active Directory	UserFlags = 66049
9	11/9/2016 2:37:4...	Active Directory	MaxStorage = -1
10	11/9/2016 2:37:4...	Active Directory	PasswordAge = 22805712
11	11/9/2016 2:37:4...	Active Directory	PasswordExpired = 0
12	11/9/2016 2:37:4...	Active Directory	LoginHours = System.Byte[]

Figure 85 - AD report

CLE

This option will list installed CLE files (credential managers and emergency access), it will then read the configuration and open a browser window to the defined forgotten password link. The user will be prompted to validate if the forgotten password page is displayed correctly or not. User response is logged as success or failure of this browser session.



Line	Time	Module	Message
1	10/20/2016 2:39:...		Report generated by: SLAnalyzer Version 3.0.0.8
2	10/20/2016 2:39:...	Client Login Ext...	Client Login Extension
3	10/20/2016 2:39:...	Client Login Ext...	Checking for CLE.
4	10/20/2016 2:39:...	Client Login Ext...	CLE credential provider found.
5	10/20/2016 2:39:...	Client Login Ext...	File: C:\Windows\System32\CLECredentialProvider.dll, Version: 3. 9. 0. 0, Size: 69222
6	10/20/2016 2:39:...	Client Login Ext...	File: C:\Windows\System32\CLECredentialProviderFilter.dll, Version: 3. 9. 0. 0, Size: 2
7	10/20/2016 2:39:...	Client Login Ext...	File: C:\Windows\System32\CLESelfSvcCredentialProvider.dll, Version: 3. 9. 0. 0, Size
8	10/20/2016 2:39:...	Client Login Ext...	File: C:\Windows\System32\EACredentialManager.dll, Version: 3.9.0.0, Size: 562176
9	10/20/2016 2:39:...	Client Login Ext...	File: C:\Windows\System32\JDMClientLoginExtensionCustomAction.dll, Version: 3, 8
10	10/20/2016 2:39:...	Client Login Ext...	File: C:\Windows\System32\NclePwmHelper.dll, Version: 3. 9. 0. 0, Size: 322560
11	10/20/2016 2:39:...	Client Login Ext...	File: C:\Windows\System32\NcleResources.dll, Version: 3. 9. 0. 0, Size: 6656
12	10/20/2016 2:39:...	Client Login Ext...	File: C:\Windows\System32\NCLoginExtension.dll, Version: 3, 8, 0, 0, Size: 82432

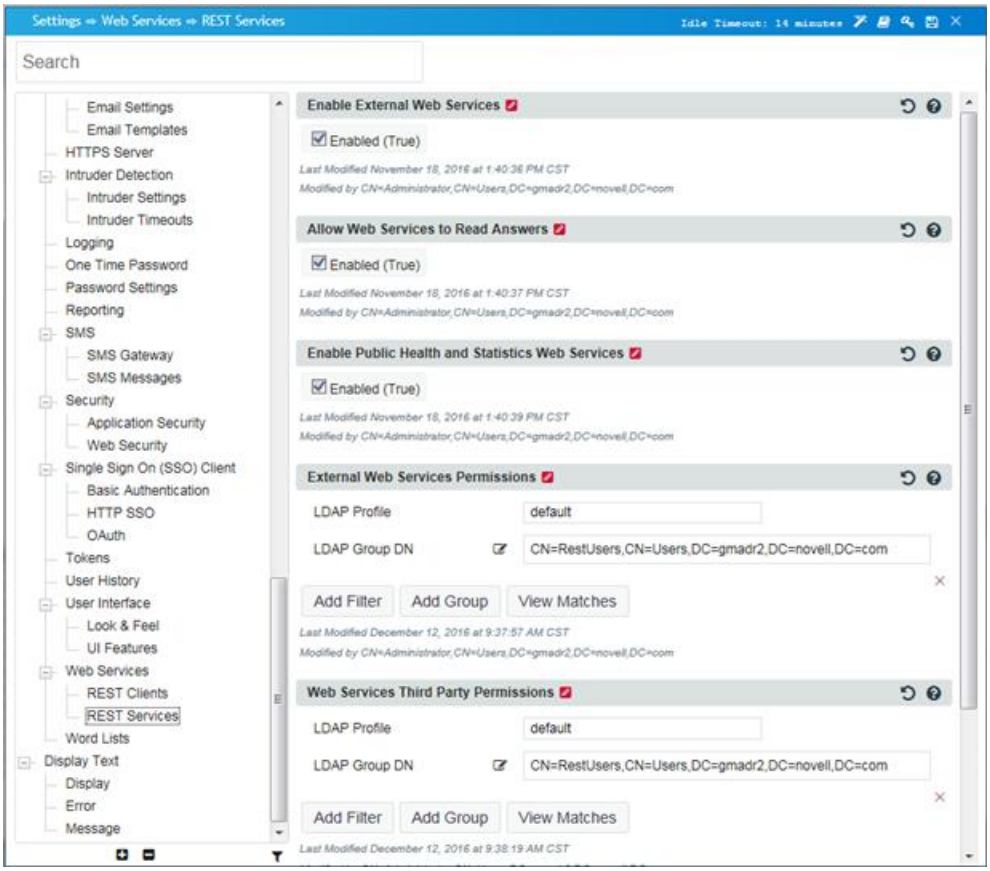
Figure 86 - CLE report

The following logic is used to generate the CLE report.

- Check for CLE provider (C:\Windows\System32\CLECredentialProvider.dll)
  - Report CLE files found in System32 folder
  - Report Emergency Access files found in C:\Program Files\NCLE\EmergencyAccess or C:\Program Files (x86)\NCLE\EmergencyAccess\
    - Test EA file access
    - Create file
    - Encrypt file
    - Decrypt file
    - Delete file
  - Display built-in CLE restricted web browser window
    - Read Forgotten Password URL from HKLM\SOFTWARE\Novell\MsPssGina\LinkURL
    - Prompt user for validation of forgotten password link data
      - If the user reports a failure then prompt to retry test with embedded browser
      - Report version of IE installed on system
      - Report local host name
      - Validate SSL certificate
      - Connect to URL
        - Report connection data (local and server host information)
        - Display browser screen
        - Prompt user for validation of forgotten password link data
- Read REST URI from HKLM\SOFTWARE\Novell\RestrictedBrowser\RestUri
  - Validate SSL certificate
  - Issue Web Request to REST URI for Public Health
  - Issue Web Request to REST URI for Statistics
  - Prompt user for credentials

    - Read user challenge data
    - Issue Web Request to REST URI for User Status
- Read registry keys

For the CLE testing and SSPR REST client tool to function properly, ensure the following settings are enabled/configured on the SSPR server.



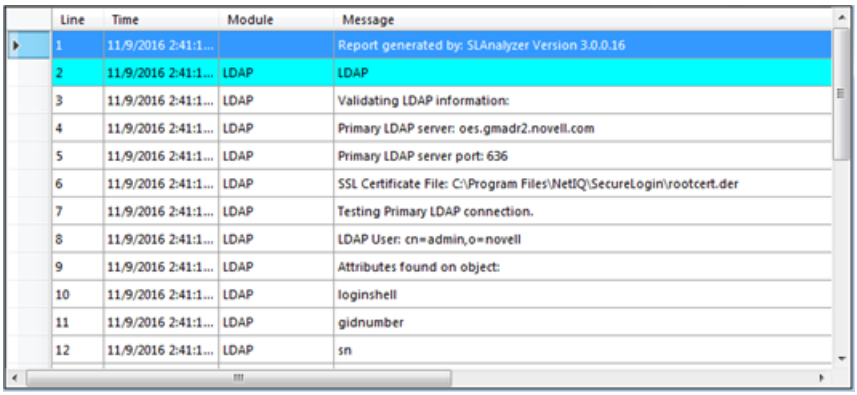
LDAP

This option reports LDAP connection related information. It also attempts to connect to the LDAP server with the configured NSL LDAP settings from the registry.

The LDAP settings used are defined at
HKEY_CURRENT_USER\Software\Protocom\SecureLogin\LDAP Settings

This includes
LastUser – REG_SZ – should reflect the LDAP DN of the user (IE cn=testusergm,o=novell)
PrimaryHost – REG_SZ – should be either the DNS name or ip address of LDAP server
SecondaryHost – REG_SZ – should be either the DNS name or ip address of LDAP server
PrimaryPort – REG_DWORD – port used (IE 0x27c, 636)
SecondaryPort – REG_DWORD – port used (IE 0x27c, 636)
SSL Cert File – REG_SZ – should be path to SSL certificate (IE C:\Program Files\NetIQ\SecureLogin\rootcert.der)

- Read LDAP settings from registry
  - HKCU\SOFTWARE\Protocom\SecureLogin\LDAP Settings\PrimaryHost
  - HKCU\SOFTWARE\Protocom\SecureLogin\LDAP Settings\PrimaryPort
  - HKCU\SOFTWARE\Protocom\SecureLogin\LDAP Settings\SSL Cert File
  - HKCU\SOFTWARE\Protocom\SecureLogin\LDAP Settings\LastUser
  - HKCU\SOFTWARE\Protocom\SecureLogin\LDAP Settings\SecondaryHost
  - HKCU\SOFTWARE\Protocom\SecureLogin\LDAP Settings\SecondaryPort
- Connect to LDAP server
- Read and display LDAP attributes of user



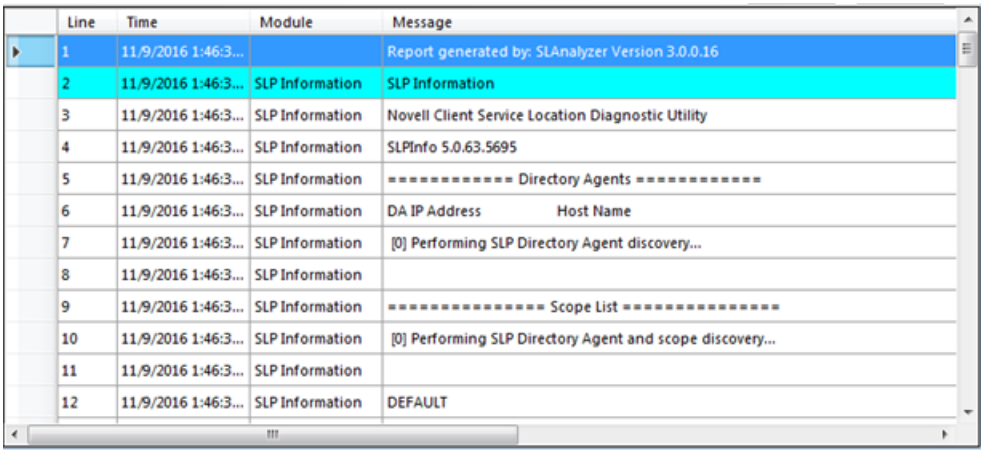
Line	Time	Module	Message
1	11/9/2016 2:41:1...		Report generated by: SLAnalyzer Version 3.0.0.16
2	11/9/2016 2:41:1...	LDAP	LDAP
3	11/9/2016 2:41:1...	LDAP	Validating LDAP information:
4	11/9/2016 2:41:1...	LDAP	Primary LDAP server: oes.gmadr2.novell.com
5	11/9/2016 2:41:1...	LDAP	Primary LDAP server port: 636
6	11/9/2016 2:41:1...	LDAP	SSL Certificate File: C:\Program Files\NetIQ\SecureLogin\rootcert.der
7	11/9/2016 2:41:1...	LDAP	Testing Primary LDAP connection.
8	11/9/2016 2:41:1...	LDAP	LDAP User: cn=admin,o=novell
9	11/9/2016 2:41:1...	LDAP	Attributes found on object:
10	11/9/2016 2:41:1...	LDAP	loginshell
11	11/9/2016 2:41:1...	LDAP	gidnumber
12	11/9/2016 2:41:1...	LDAP	sn

Figure 87 - LDAP report

Novell Client

This option reports Novell client information.

- SLPInfo
- Check for Novell client
- Check for NSL credential provider
- Check for nwtray
- Check for XTSvcMgr
- Connect to client API
    - Create NCP connection
    - Get existing primary NCP connection
    - Get eDirectory connection
    - Read logged on User
    - Get Server Name
    - Read and display eDirectory attributes and rights of logged on user



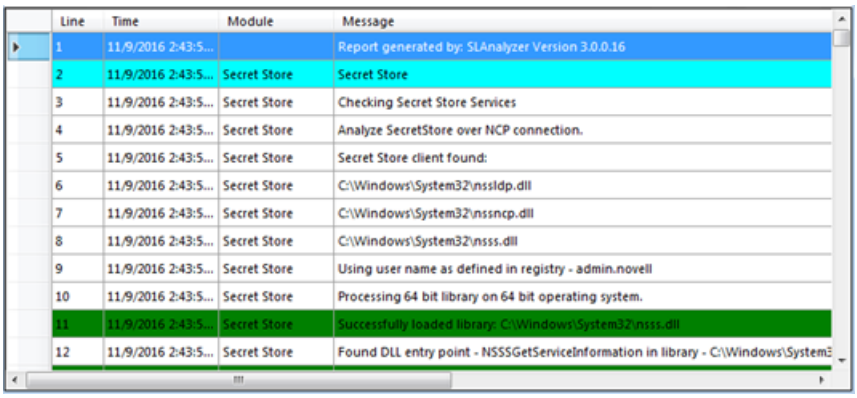
Line	Time	Module	Message
1	11/9/2016 1:46:3...		Report generated by: SLAnalyzer Version 3.0.0.16
2	11/9/2016 1:46:3...	SLP Information	SLP Information
3	11/9/2016 1:46:3...	SLP Information	Novell Client Service Location Diagnostic Utility
4	11/9/2016 1:46:3...	SLP Information	SLPInfo 5.0.63.5695
5	11/9/2016 1:46:3...	SLP Information	========== Directory Agents ==========
6	11/9/2016 1:46:3...	SLP Information	DA IP Address Host Name
7	11/9/2016 1:46:3...	SLP Information	[0] Performing SLP Directory Agent discovery...
8	11/9/2016 1:46:3...	SLP Information	
9	11/9/2016 1:46:3...	SLP Information	========== Scope List ==========
10	11/9/2016 1:46:3...	SLP Information	[0] Performing SLP Directory Agent and scope discovery...
11	11/9/2016 1:46:3...	SLP Information	
12	11/9/2016 1:46:3...	SLP Information	DEFAULT

Figure 88 - Novell Client report

SecretStore

This option will attempt to connect to SecretStore server and read secret information. It will prompt for the users credentials to read the stored gina credentials (SecureLogin runtime variables “?sysuser”, “?syspassword”)

- Validate Novell client installation
- Perform NDS validation (See NDS above)
- Check SecretStore interface (Novell client)
- Find and validate SecretStore client files
- Connect to SecretStore via API (NCP)
    - Call NSSGetServiceInformation (Server Information)
    - Call NSSEnumerateSecretIDs (Get statistics on secrets)



Line	Time	Module	Message
1	11/9/2016 2:43:5...		Report generated by: SLAnalyzer Version 3.0.0.16
2	11/9/2016 2:43:5...	Secret Store	Secret Store
3	11/9/2016 2:43:5...	Secret Store	Checking Secret Store Services
4	11/9/2016 2:43:5...	Secret Store	Analyze SecretStore over NCP connection.
5	11/9/2016 2:43:5...	Secret Store	Secret Store client found:
6	11/9/2016 2:43:5...	Secret Store	C:\Windows\System32\nssldp.dll
7	11/9/2016 2:43:5...	Secret Store	C:\Windows\System32\nssncp.dll
8	11/9/2016 2:43:5...	Secret Store	C:\Windows\System32\nsss.dll
9	11/9/2016 2:43:5...	Secret Store	Using user name as defined in registry - admin.novell
10	11/9/2016 2:43:5...	Secret Store	Processing 64 bit library on 64 bit operating system.
11	11/9/2016 2:43:5...	Secret Store	Successfully loaded library: C:\Windows\System32\nsss.dll
12	11/9/2016 2:43:5...	Secret Store	Found DLL entry point - NSSSGetServiceInformation in library - C:\Windows\System3

Figure 89 - Secret Store report

SecureLogin

This option will attempt to communicate with the SecureLogin client running on the workstation. The following is a list of the logic used.

.

- NSL client information
- NSL client files
- NSL processes
- Primary NSL mode
    - NDS (See Novell Client)
    - AD (See AD)
    - LDAP (See LDAP)
    - SecretStore (See SecretStore)
    - LDAPSecretStore (See SecretStore)
    - SecureLoginAdvancedEdition (See Azure)
- Secondary NSL mode
    - File
        - Validate that cache file is enabled
        - Validates cache file path and filename are correct
    - Smart Card (See Smart Card)
- Call SecureLogin API for realtime statistics
    - Check online status
    - Check for active status
    - Check for cache
    - Report database version
    - Read NSL username
    - Read active passphrase question
    - Validate gina credentials
    - Read NSL preferences
    - Read NSL applications
        - Read application preferences
        - Read application linked logins
        - Read application credentials
    - Read NSL Logins
    - Read NSL Credential Sets
        - Normal
        - SetPlat
    - Corporate redirection
    - Validate DotNet service support
    - Validate Flash service support
    - Validate Java service support
        - Java is registered with NSL
        - Validate properties files exist
        - Validate jar files installed

The SecureLogin report will run all of the possible reports when clicking on SecureLogin. Optionally the user can click on one of the listed individual report to generate just that information.

Optional SecureLogin reports

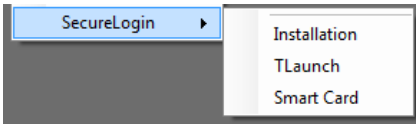


Figure 90 - Optional SecureLogin reports

Installation

- Print contents of C:\NSLFiles\Log.txt
- Print contents of C:\NSLFiles\responsefile.ini

TLaunch

This option parses each emulator definition in tlaunch and tlaunch64 ini files. It validates if emulator executable can be found in the program path and if HLLAPI based, if the HLLAPI function can be found in the designated HLLAPI DLL. This process loads the configured HLLAPI dll into memory and attempts to locate the specified HLLAPI function.

Note: SLAnalyzer cannot analyze 32-bit tlaunch configurations when ran on a 64-bit workstation. The reason is that a 64-bit executable is restricted from being able to load a 32-bit library. For analysis of 32-bit emulator configurations when running on a 64 bit workstation, use the 32 bit executable "Tlaunch32Analyzer.exe" or run this option from a 32 bit workstation.

- Checks OS version 64/32 bit for load library operations
- Validates path to tlaunch.ini file
- Opens tlaunch.ini and parses each emulator definition
    - Checks for emulator executable in specified location
        - Check for HLLAPI type
        - Load HLLAPI library
        - Validate HLLAPI function
- Opens tlaunch64.ini if applicable
    - Checks for emulator executable in specified location
        - Check for HLLAPI type
        - Load HLLAPI library
        - Validate HLLAPI function

Smart Card

This option attempts to locate the specified PKCS11 library and open it.

- Read PKCS11 library from registry
  - `HKLM\SOFTWARE\Protocom\SecureLogin\Security\StorageDeviceInterfaceLibraryPKCS11`
- Load library into memory to validate package

Tools Menu

The tools menu consists of the following items.

- Debugging Logging
- Debug Console
- File Browser
- View Registry Keys
- Registry Key by Product
- Group Policy
  - Generate HTML Report
  - Generate Report
  - Force Update
- Common Appliance Framework
  - Generate Support Config
  - Get Registration/zypper Logs
  - Reset Appliance Certificate
  - Update Appliance
- Self Service Password Reset
  - REST Client
  - Rights Validator
- Advanced Authentication
  - REST Client
  - Risk Services
  - Add CA Root Certificate
  - Find PostGres User
  - Gather Server Stats
  - Monitor Server Performance
  - Replace OSP Certificates
  - Reset Local Admin Pwd
  - OSP/OAuth2
  - Get OpenID Config
  - Get SAML metadata
- SaaS
  - CBA
    - Gather CBA Stats
    - Start CBA
    - Stop CBA
    - Debug Settings
    - Get Install Log
    - Get Debug Logs
- Azure
  - Azure AD Login
  - Azure Client Login
  - SecureLogin AE Login
  - Get AD Application Info
  - Get Subscriptions
  - Get Resources
  - Get Kubernetes Info

        - Get Kubernetes Name Space
        - Get Kubernetes Pods
        - Get Kubernetes Logs
        - Initialize for Kubernetes
        - KubeCtl terminal
        - Kubernetes Node Explorer
        - Get File
        - Send File
        - Send a Command
        - Send REST Get Request
- Identity Manager
    - REST Client
    - Gather Support Bundle
- LDAP Browser
- JSON Console
- SSH/SCP
    - Explorer
    - Terminal
    - Download File
    - Upload File
    - Restart Host
- SQL Browser
- Web Browser
- Configure SLAnalyzer

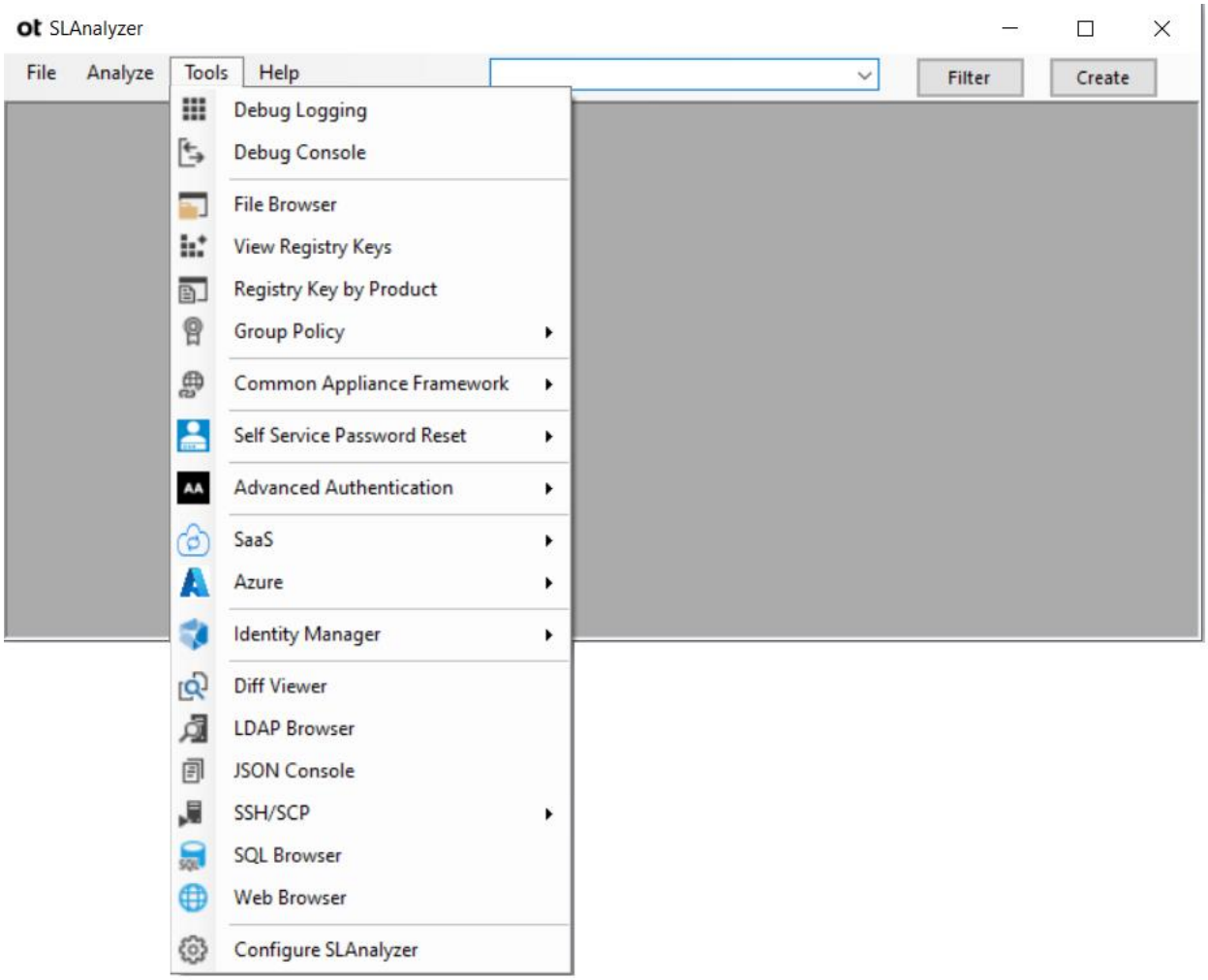


Figure 91 - Tools Menu

Debugging Options

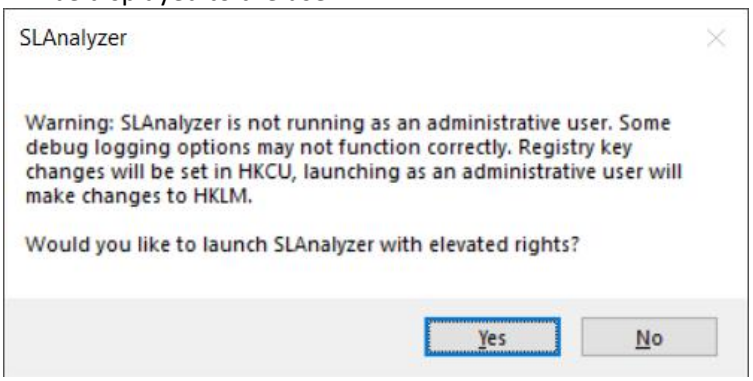
Provides access to enable debug logging for SecureLogin (Client modules, LdapAuth, Virtual Channel drivers, and Emergency Access), Also Novell Client, SecretStore client (NCP and LDAP), NMAS, DAS, SecureWorkstation, PCProx NMAS method, and Client Login Extension)

Debug scope

There are two types of debugging that can be enabled in the Windows operating system.

- User level debugging
- Machine level debugging

When selecting this option, if SLAnalyzer detects that user level debugging is effective, then a message will be displayed to the user.



Clicking No to the prompt will open the debug logging form with user level debug scope.
Clicking Yes will close the current SLAnalyzer instance and open an explorer window to the SLAnalyzer executable. Right click on the executable SLAnalyzer.exe and select Run as administrator.

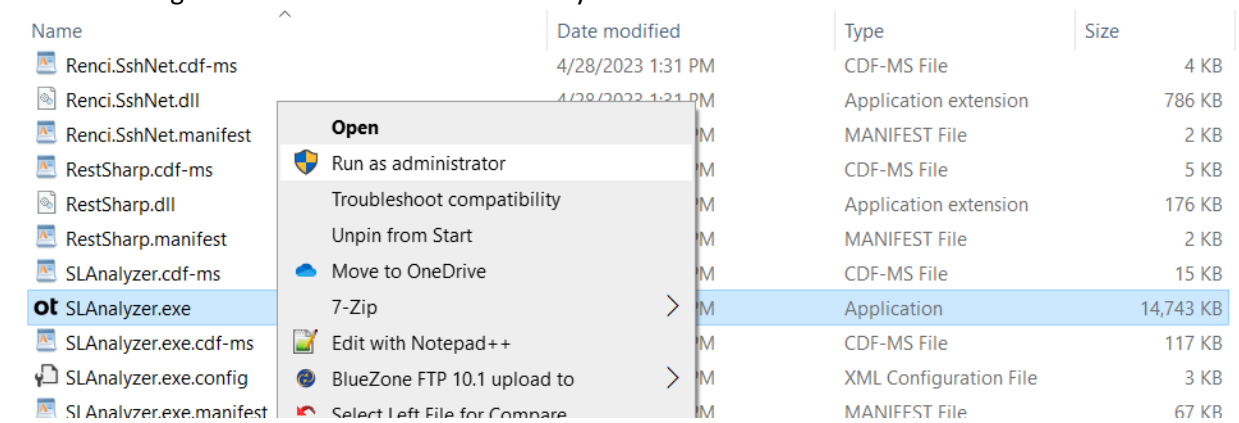


Figure 92 - Run as administrator

User level debugging

User level debugging is based upon the currently logged on user. These are settings that are generally found in the registry under HKCU. Debug logging enabled with user level debugging only effects the user that was logged in when the logging was enabled. Other users are not affected.

The Title of the debug window will inform you if user or workstation level debugging will be configured when changing a value. The user or workstation level debugging is controlled by user rights. If logged into the workstation as a domain admin then SLAnalyzer will default to workstation level logging (meaning that logging keys will be set at HKLM). When logging in as a normal user, then opening the executable normally will provide user level debugging.

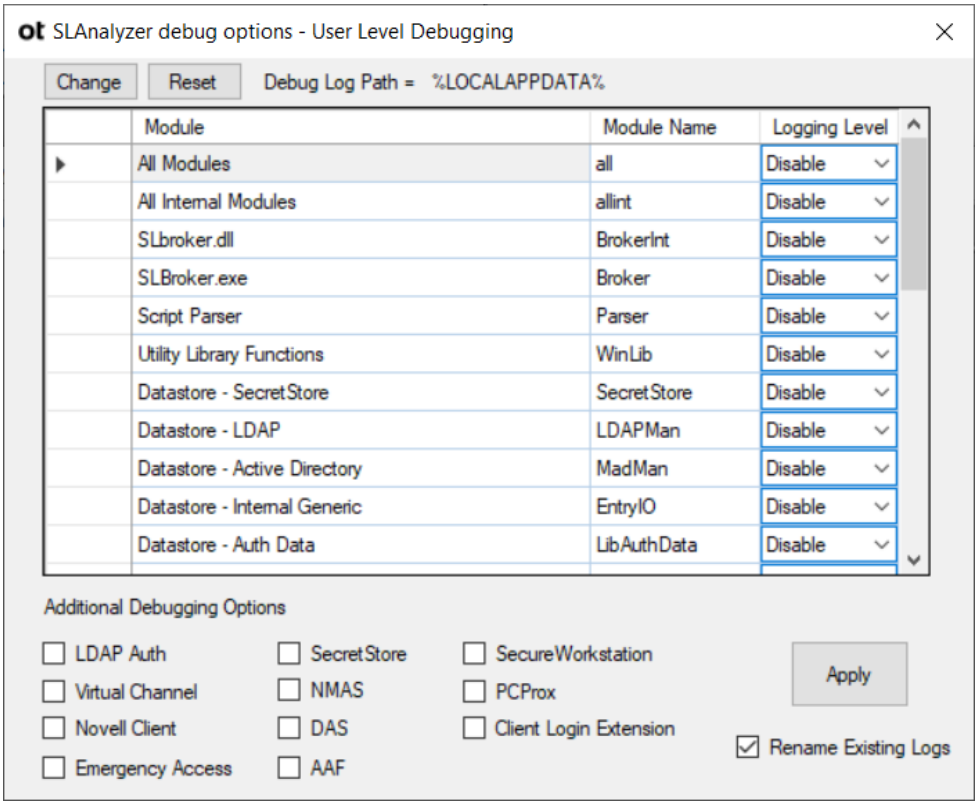


Figure 93 - User level debugging

Machine level debugging

Opening the executable with “Run as administrator” will provide workstation level debugging. Workstation level debugging applies to any user logging into the workstation whereas user level debugging only applies to the currently logged in user.

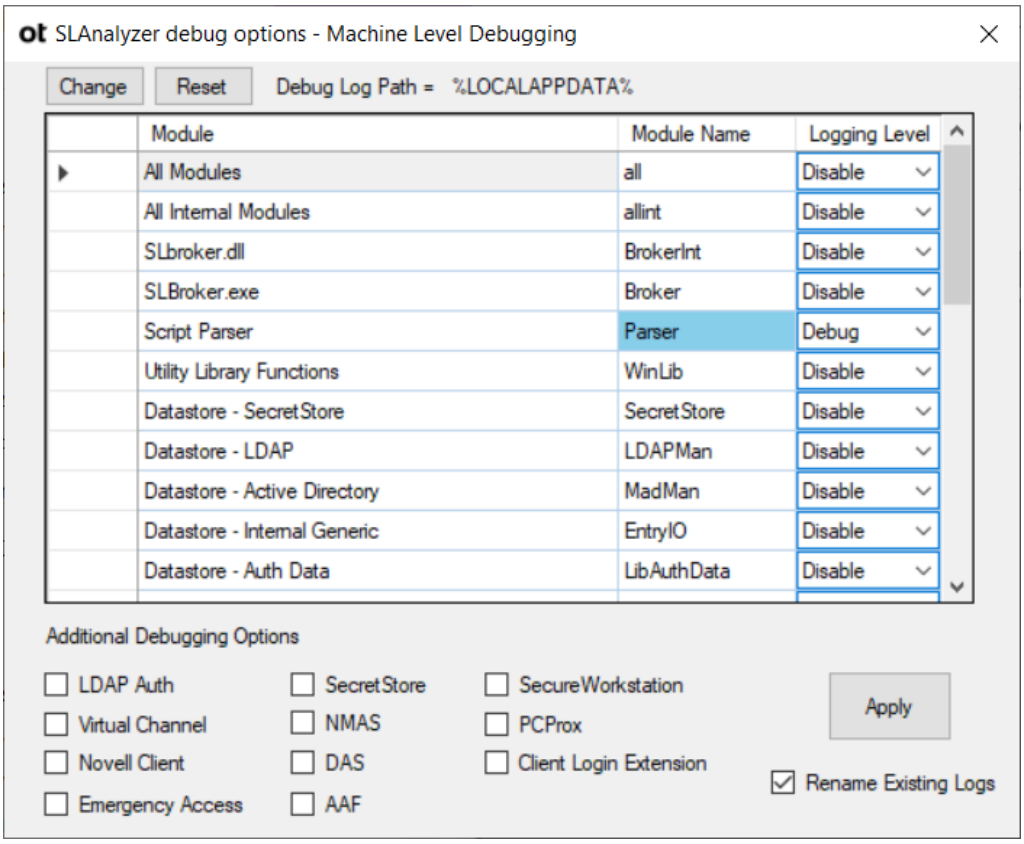


Figure 94 - Machine level debugging

Debug window components

The debug logging window is composed of several different components.

- Change Button
- Reset Button
- Debug Log Path
- SecureLogin module selection
- Additional Debugging Options
    - LDAP Auth
    - Virtual Channel
    - Novell Client
    - Emergency Access
    - SecretStore
    - NMAS
    - DAS
    - SecureWorkstation
    - PCProx
    - Client Login Extension
    - AAF

Change button

Clicking on the Change button will bring up an explorer window so that the user can browse to the desired location to save the debug log information. Note that not all modules will log to a custom location but if possible SLAnalyzer will redirect the log to the location specified.

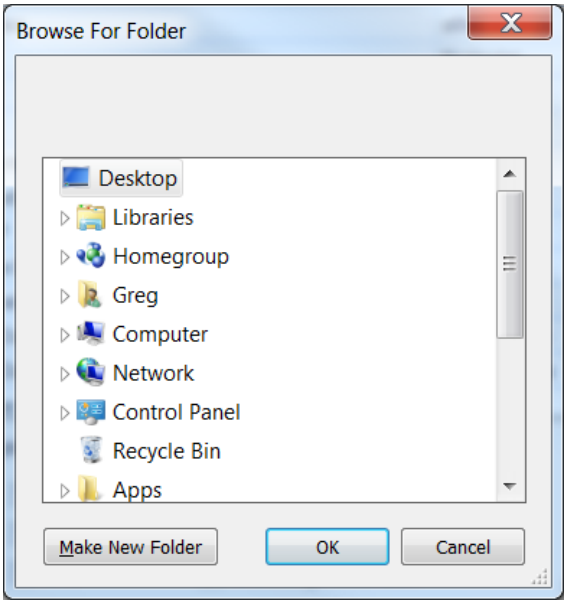


Figure 95 - Change debug file location

Reset button

Clicking the reset button will reset the debug log path to c:\nslfiles

Debug Log Path

On the Debug log window, the current debug log path is displayed. It is possible to click the change button to change the location where SecureLogin will generate the ssodebug.log file. If you change this value it is important to ensure that you point to a location where SecureLogin will be able to obtain the appropriate rights to create and modify this file. To reset the log file path to the default value then click the reset button.

Note that the Debug Log Path does not apply to all debug logging options contained within this window. Some debug logging features do not allow the redirection of the log files to a specified location.

For example, the Novell client credential provider logs will always log to the C:\ProgramData\Novell\Client\Log folder regardless of this setting. Hovering the mouse over the desired debug option will provide information as to the default log file path.

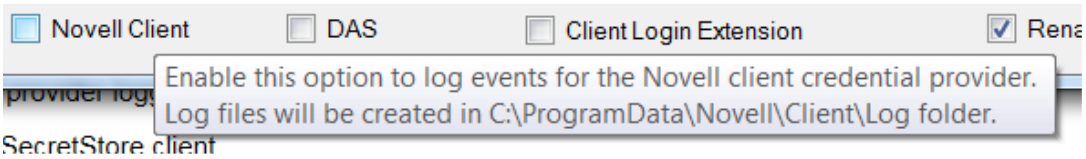
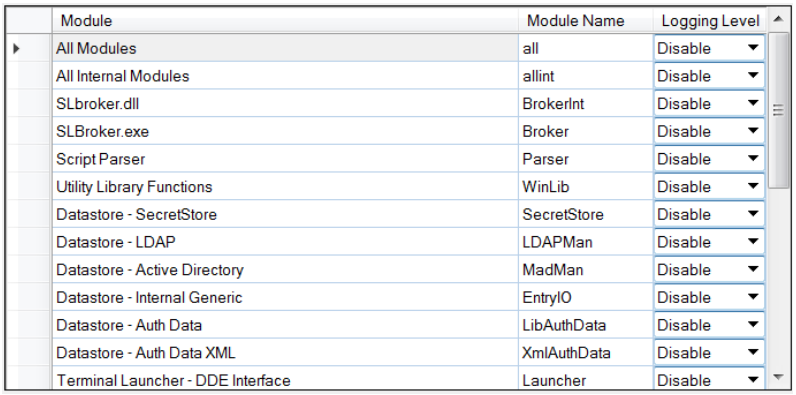


Figure 96 - Static log path

SecureLogin Debug module box

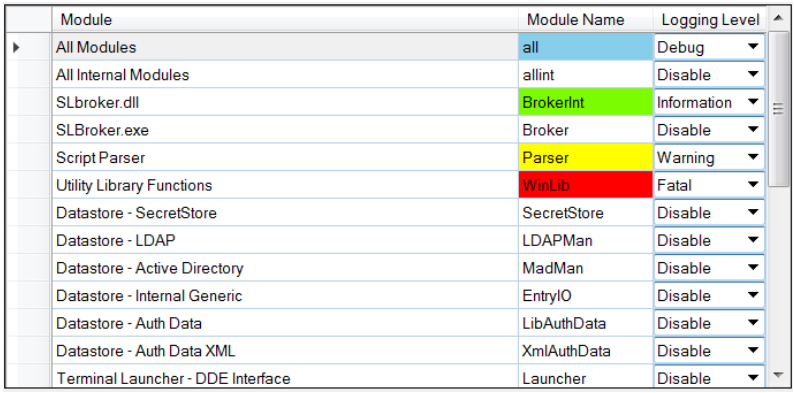
The SecureLogin debug module box lists all the possible SecureLogin modules that have logging capabilities. To enable logging for a specific module then select the module and click on the Logging Level drop down box. Select the desired logging level of Disable, Debug, Information, Warning, or Fatal. One the desired logging levels have been set then click the apply button.
Note that in most cases, technical support will suggest enabling debug logging for All Modules.



Module	Module Name	Logging Level
All Modules	all	Disable
All Internal Modules	allint	Disable
SLbroker.dll	BrokerInt	Disable
SLBroker.exe	Broker	Disable
Script Parser	Parser	Disable
Utility Library Functions	WinLib	Disable
Datastore - SecretStore	SecretStore	Disable
Datastore - LDAP	LDAPMan	Disable
Datastore - Active Directory	MadMan	Disable
Datastore - Internal Generic	EntryIO	Disable
Datastore - Auth Data	LibAuthData	Disable
Datastore - Auth Data XML	XmlAuthData	Disable
Terminal Launcher - DDE Interface	Launcher	Disable

Figure 97 - SecureLogin module logging

After clicking the apply button SLAnalyzer will colorize any logging enabled module.



Module	Module Name	Logging Level
All Modules	all	Debug
All Internal Modules	allint	Disable
SLbroker.dll	BrokerInt	Information
SLBroker.exe	Broker	Disable
Script Parser	Parser	Warning
Utility Library Functions	WinLib	Fatal
Datastore - SecretStore	SecretStore	Disable
Datastore - LDAP	LDAPMan	Disable
Datastore - Active Directory	MadMan	Disable
Datastore - Internal Generic	EntryIO	Disable
Datastore - Auth Data	LibAuthData	Disable
Datastore - Auth Data XML	XmlAuthData	Disable
Terminal Launcher - DDE Interface	Launcher	Disable

Figure 98 - SecureLogin module logging with items set

Additional Debugging options

In addition to SecureLogin module debugging SLAnalyzer can enable debug logging for a number of other products.

LDAP Auth

When this checkbox is checked the SecureLogin LDAPAuth component will generate debug information. The LDAPAuth debug file will be created in the currently configured debug log path.

Virtual Channel

When this checkbox is checked the SecureLogin Virtual Channel Drivers debug logging will be enabled. This can be used for both server and client-side debugging. The SecureLogin Virtual Channel Drivers are for the Citrix Virtual channel which SecureLogin uses to pass credential and biometric information between the SecureLogin client on a workstation and a Citrix session.

Logs will be created in...
Server - slina.dll - c:\windows\system32\slina.ica.log or slina.ts.log
Server - sl_tsgina.dll - c:\windows\system32\sl_tsgina.ica.log or sl_tsgina.ts.log
Workstation - slina.dll (wks) - c:\windows\system32\slina.log
Workstation - vdslssoN.dll - c:\program Files\Citrix\ICA Client\vdslsso.log
Workstation - tsslsso.dll - c:\windows\system32\tsslsso.log

Novell Client

When this checkbox is checked the Novell client debug logging will be enabled.

Log files will be created in C:\ProgramData\Novell\Client\Log folder.

Emergency Access

When this checkbox is checked emergency access included in SecureLogin 8 logging will be enabled.

Note that in versions of SecureLogin higher than 8.0.1 the Emergency Access feature is moved to CLE.
To enable logging of Emergency Access included in CLE, check the checkbox for Client Login Extension.

Log will be created in the configured log path.

SecretStore

When this checkbox is checked then debug logging for the SecretStore client will be enabled.

Log file will be created in the current log file path as nsss.log

NMAS

If this checkbox is checked then debug logging for the NMAS client will be enabled.

Log file will be created in the current log file path as nmclient.log

DAS

If this checkbox is checked then debug logging for Desktop Automation Services will be enabled.

Log file will be created in the current log file path as DASLog.txt

AAF

If this checkbox is checked then debug logging for the Advanced Authentication Framework Windows client will be enabled on the workstation. When debug logging for this module is enabled, the processes for AAF hold open the debug log files. For this reason, SLAnalyzer will stop the running processes when performing the rename operation, rename the files, and then restart the processes. Files will be stored in the static path of C:\ProgramData\NetIQ\Logging\Logs.

SecureWorkstation

If this checkbox is checked then debug logging for SecureWorkstation will be enabled.

Log files will be created in the folder C:\SWLog
C:\SWLog\wsaccsvc.log
C:\SWLog\wsaccsmp.log

PCProx

If this checkbox is checked then debug logging for the PCProx NMAS method will be enabled.

Log file will be created in the folder c:\pcProxLog

Client Login Extension

If this checkbox is checked then debug logging for Client Login Extension will be enabled.

Log files will be created in the current log file path. The files will be named RestrictedBrowserDLL.log and RestrictedBrowserEXE.log

Apply button

Clicking the apply button will make the changes to the registry to enable the logging options selected.

Rename existing logs checkbox

This option is checked by default and will cause any existing log files found in the log file path or default path for modules that cannot be redirected to be renamed. The file will be renamed with the original name followed with a timestamp (IE Tuesday, October 11, 2016 4.28.13 PM). Note that the rename action only occurs when you click the Apply button.

Debug Console

This option displays a window that will capture any debug information sent from applications to the operating system debugger. This would include information from debug modules, services where debug logging has been enabled, and even SecureLogin scripts where the debugprint command is used.

This option is similar to Microsoft debugview application and other debug monitors available for debugging windows applications.

The debug console window contains 4 buttons.

- Save – This allows the contents of the debug console to be saved to the default log folder.
- Clear – Clear information in the Debug Console window
- Stop/Start – This toggles from Stop to Start and pauses the debug output.
- Filter – Enable/Disable processes being monitored

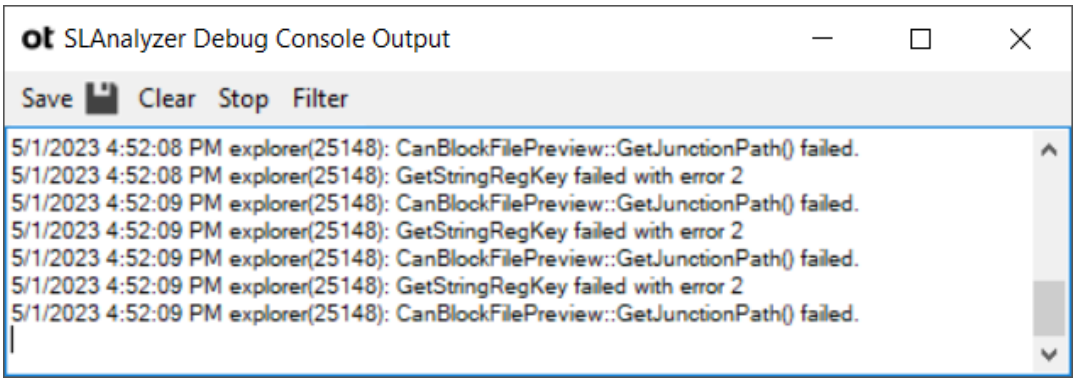


Figure 99 - Debug Console window

An entry in the debug console window is composed of the service name(process ID) and the message logged by the service.

Filtering debug data

SLAnalyzer builds the list of services dynamically as they are generated by applications running on the system. If you do not want to see messages from a specific service then uncheck that service. By default SLAnalyzer will log for all applications.

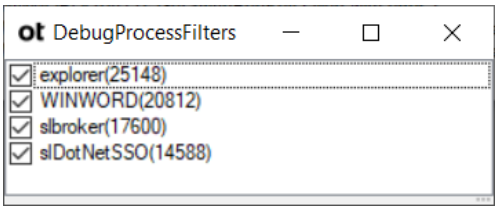


Figure 100 - Debug Process Filters

File Browser

Opens a file browser.

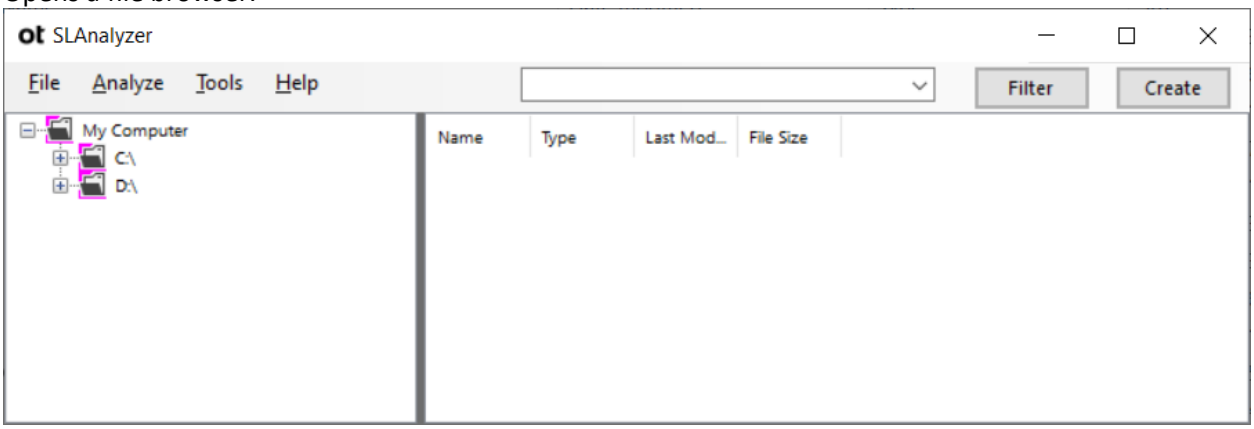


Figure 101 - File Browser

From the file browser menu you can double click on a file to open.

Note that you can open just about any file type with SLAnalyzer. If SLAnalyzer cannot determine the content type it will prompt the user to open with the generic text reader. If there is a built-in routine for the file type, then SLAnalyzer will display the file content. If there is no built-in routine for the file type, then the Windows default application for the content will be called. For example, attempting to open a wmv file will result in the default media player being loaded to display the file content.

View Registry Keys

This feature will display all the Novell related registry keys currently defined in the workstation registry. Clicking on any entry will display detail information (if available) on the selected registry key. Note that not all of the Novell/SecureLogin registry keys are currently documented. Only those keys we have information on, will display the appropriate detailed information.

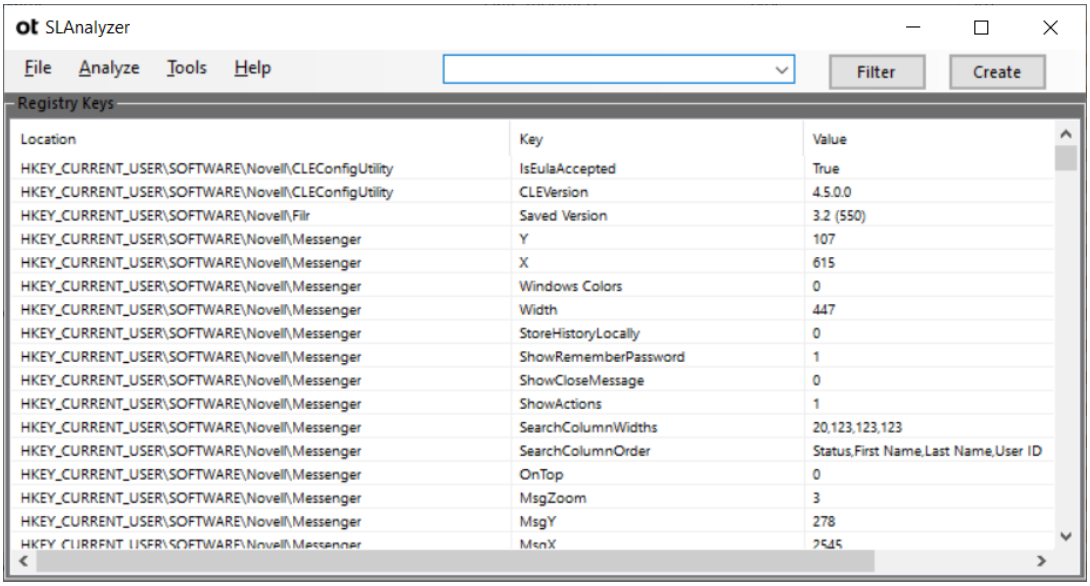


Figure 102 - View registry keys

Registry key detail

Selecting an item in the registry key browser will display the details currently defined for the registry key. The information provided is derived from several different sources

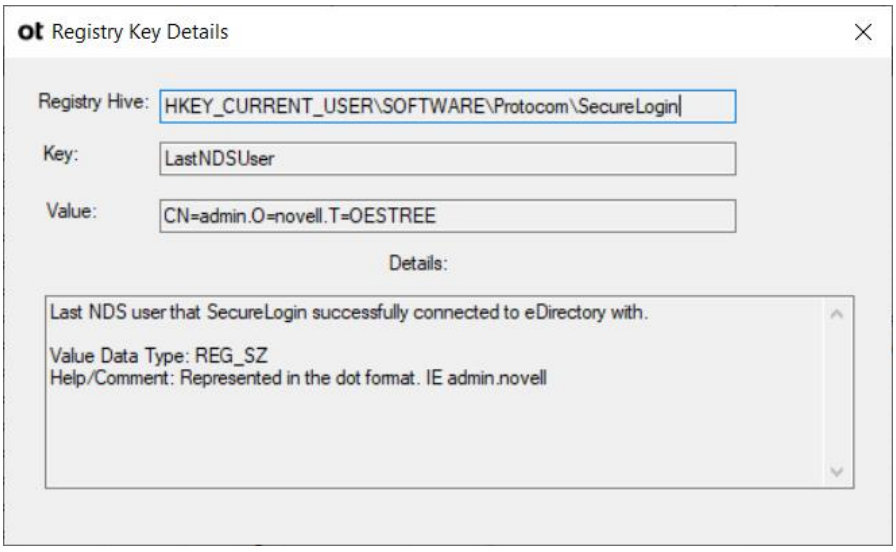


Figure 103 - Registry key detail

Registry Keys by Product

This option provides a tree view of possible registry keys by product.

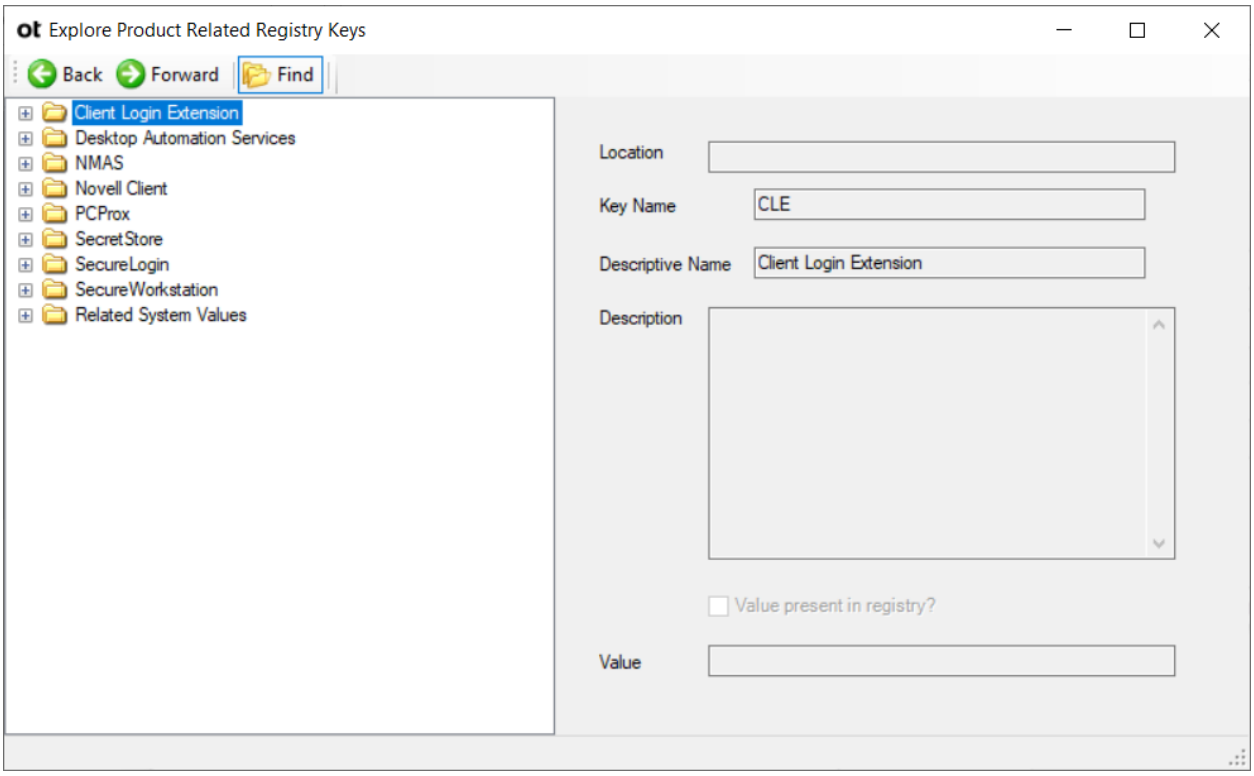


Figure 104 - Explore Product Related Registry Keys

Registry Key by Product Details

When the user selects a possible registry key, the following information is displayed:

- Location – path in the registry
- Key Name – name of the key in the registry
- Descriptive Name – in some cases registry keys have another name that is easier to understand.
- Description – Description of the possible usage for this registry key and its associated values
- Value present in registry? - This checkbox if checked indicates if the value is present in the registry. Most if not all registry keys used by products have a default value even if the key is not defined in the registry. This checkbox provides the ability to determine if the key is overriding a default value.
- Value – lists the value of the registry key, if defined.

Find

Find a registry key (exact match) – If you know the name of the registry key, and would like an explanation of the keys purpose, you can click on the find button and enter the name of the key. Note that this search is an exact match so you must type the key name correctly. So, a find for “forcehklm” will fail for a registry key named “forcehklmandnodpapi”. This find is not character case sensitive so a find for “nds” and “Nds” would be considered the same.

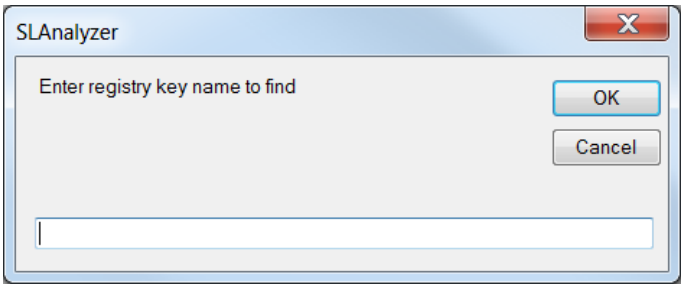


Figure 105 - Find registry key

Select item Forward/Back

Clicking the forward or backwards button will scroll through the list of registry keys currently expanded.

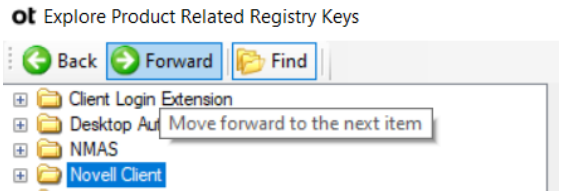


Figure 106 - Move forward

Group Policy

There are three optional tools for Group Policy.

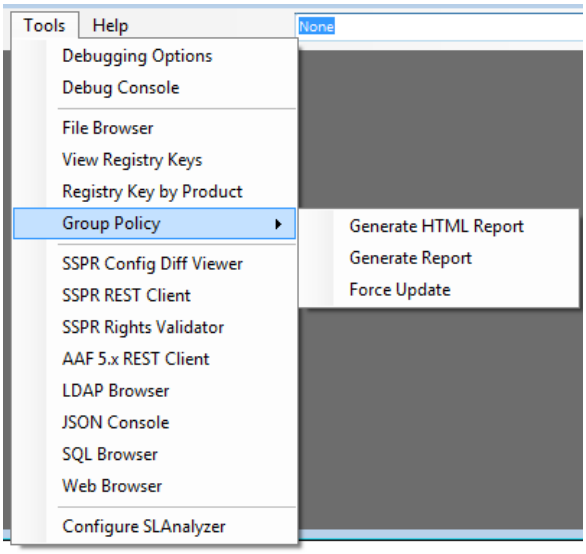


Figure 107 - Group Policy Tools

- Generate HTML Report
- Generate Report
- Force Update

Generate HTML Report

The tool generate HTML report creates a report in HTML format that contains detailed information regarding GPO policies and settings that are applied to the user/workstation.

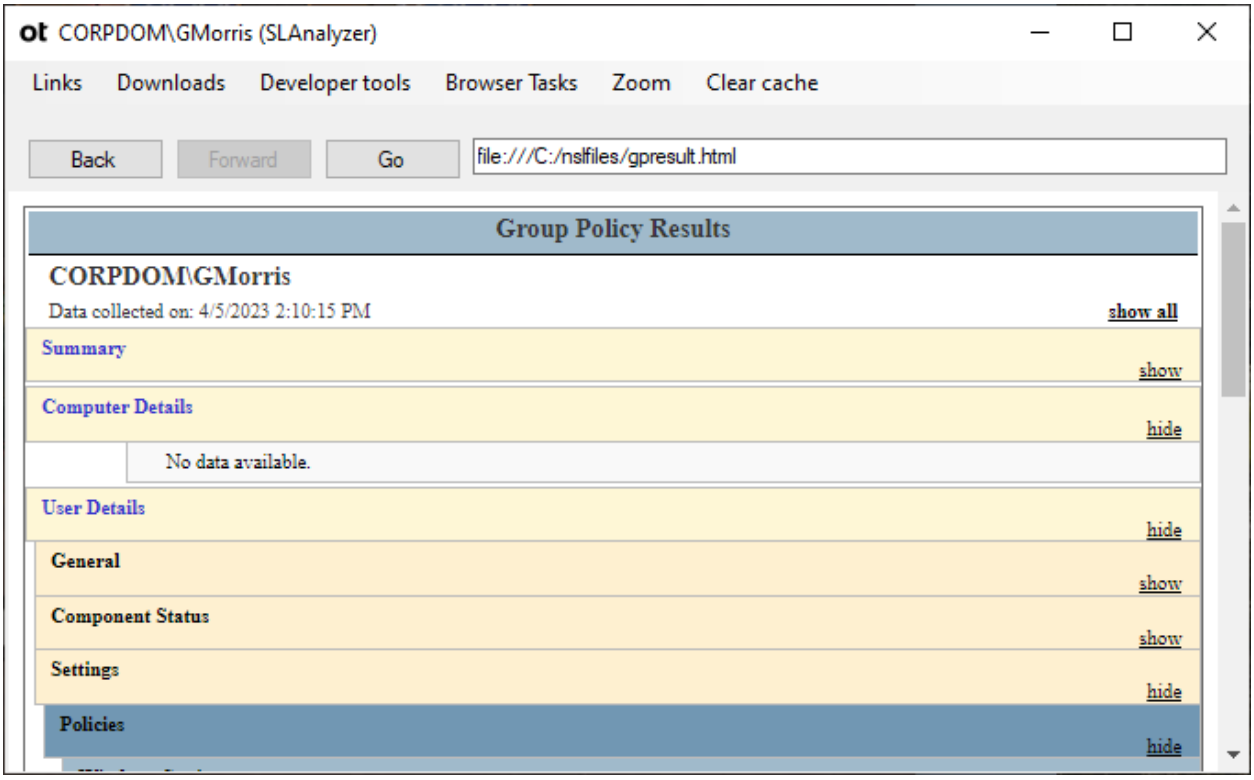


Figure 108 - GPO HTML Report

Generate Report

The tool generate report executes the Window utility gpresult.exe to query the domain for GPO information. Once the report has been generated then the XML viewer is used to display the report data.

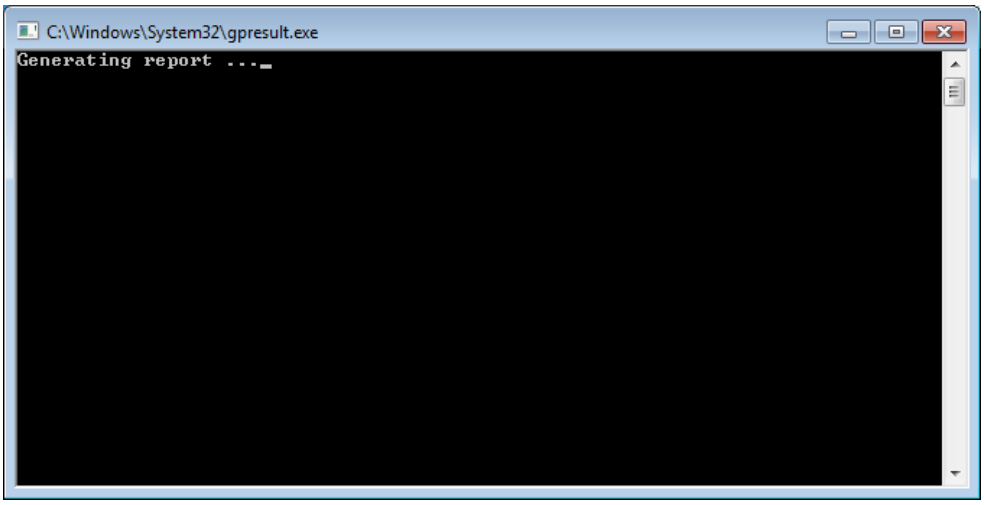


Figure 109 - GPO generate report

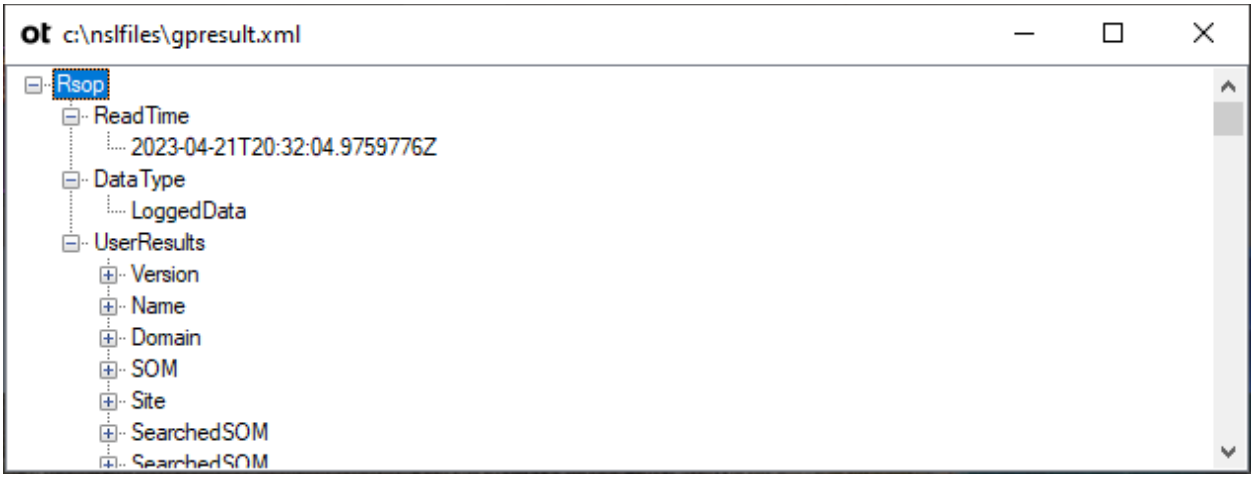


Figure 110 - GPO report

Force Update

Selecting this option forces the Group Policy data to be updated from the domain.

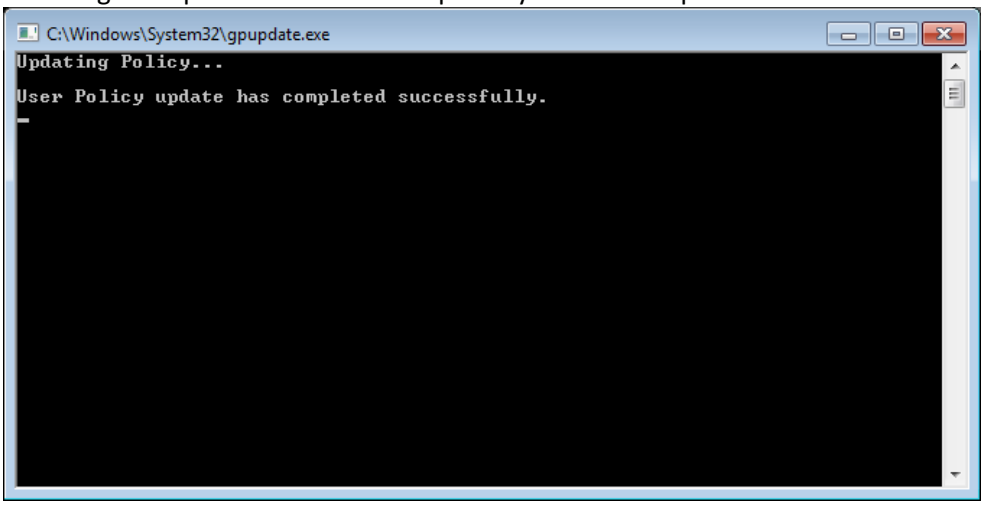
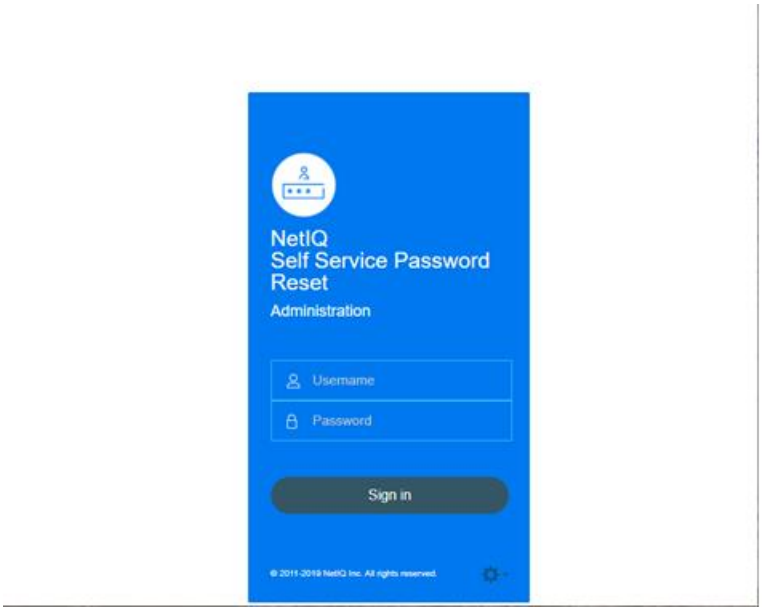


Figure 111 - Force update

Common Appliance Framework

The CAF is a common platform used by several different appliance-based products. The appliance is delivered as a VMWare image that includes a preconfigured OS and necessary components for the target application.



The CAF appliance console can be accessed via the server URL at port 9443.

Reset Appliance Certificate

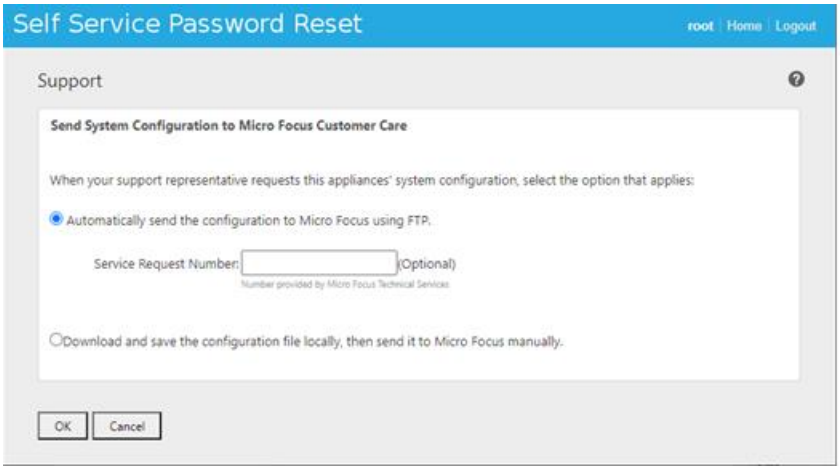
The CAF appliance console has its own set of certificates for access. By default, the 9443 console is protected by a self signed certificate created during install. If replaced this certificate could expire or need to be reset. The option “Reset Appliance Certificate” will regenerate and assign the self signed certificate. Note that this option requires SSH access to the appliance. If you are unable to access the appliance console, login to the session at the VMWare host and use YAST to enable the SSH service. If you can login to the appliance console, then click on the services icon and enable SSH.

Get Registration/zypper Logs

The CAF appliance menu allows for registration of the appliance to the Micro Focus update channels. This allows the auto-update or manual update of the underlying OS and the appliance application. The registration logs help in the diagnosis of issues related to the registration process. Note that this option requires SSH access to the appliance. If you are unable to access the appliance console, login to the session at the VMWare host and use YAST to enable the SSH service. If you can login to the appliance console, then click on the services icon and enable SSH.

Generate Support Config

This feature mimics the same feature from the CAF appliance (9443) console. Within the appliance console, if the user clicks on the Support icon, the support page is displayed.



This feature in SLAnalyzer allows for the generation of the support config in cases where the support config fails from within the appliance console.

When selecting this option in SLAnalyzer the SSH credentials for the server will need to be provided. After successfully connecting to the server via SSH then the support bundle will be generated and saved to the local workstation.

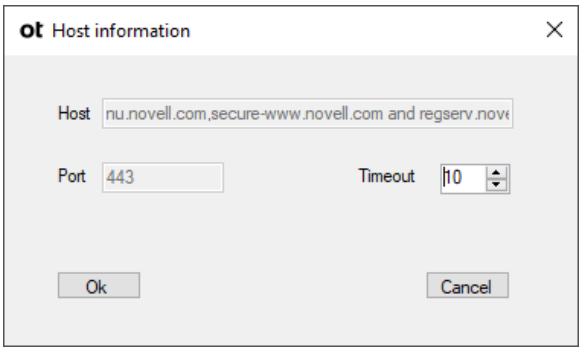
Update Appliance

This option will cleanup the update files and then launch a browser to the Update page of the appliance.

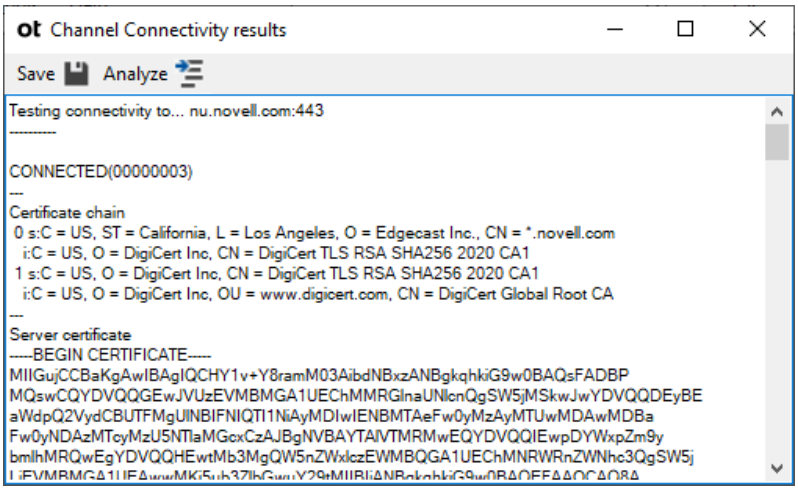
Verify Channel Connectivity

This option provides the ability to validate connectivity between the common appliance framework host of the AA server and the servers needed for channel updates. This utilizes OpenSSL to test the connectivity to the channel hosts. This option can be used to validate if the common appliance framework host can communicate with nu.novell.com, secure-www.novell.com and regserv.novell.com.

When prompted, the timeout value can be adjusted for cases where response times might exceed the default of 10 seconds.



After completing the connectivity test the results window will display the information discovered from the connection.



Registration

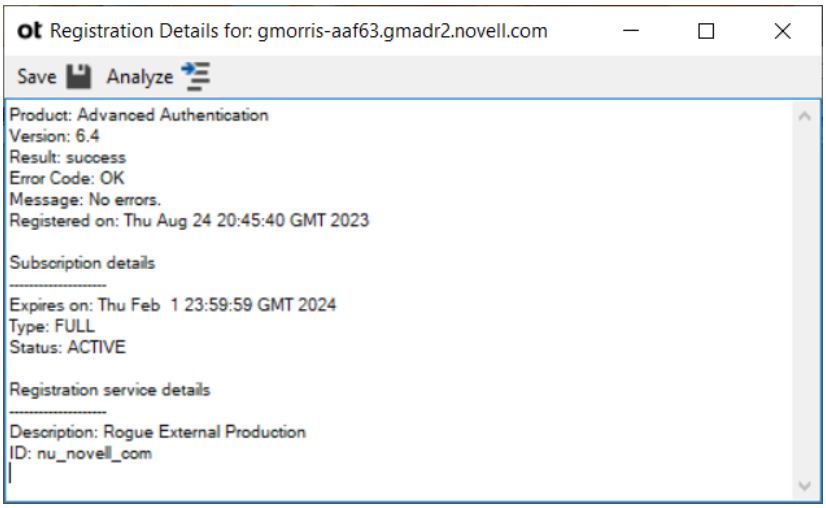
The registration menu contains 3 options

- Check Registration Status
- Clear Registration
- New Registration

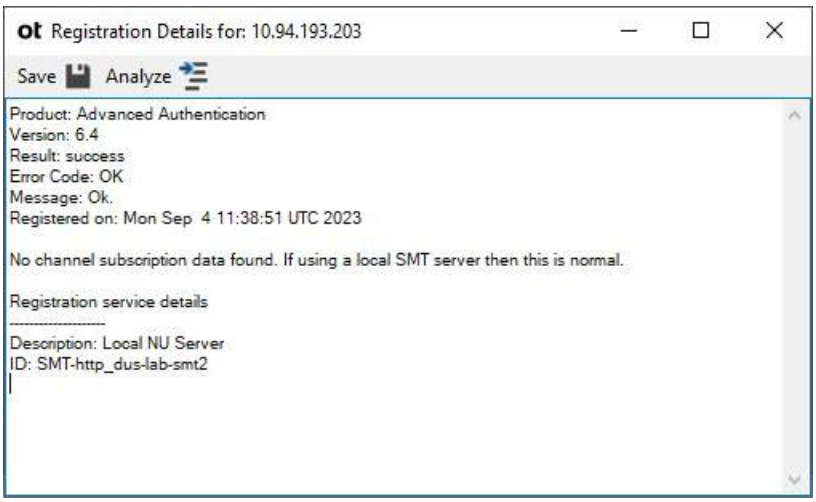
Check Registration

This option provides the ability to check the registration status of the appliance. This option requires an SSH session and SLAnalyzer will prompt for the SSH credentials. After connecting to the server via SSH the registration status will be displayed.

Registration status of a server registered to nu_novell_com:



Registration status of a server registered to a local SMT server:



Clear Registration

This option will clear any current registation so that the server can be registered again. Note that this option will require SSH access to the server. When executed this option will prompt for the SSH credentials. After connection via SSH, SLAnalyzer will remove the registration files on the server.

New Registration

This option will attempt to register the appliance with the registation service at nu_novell_com. This option requires SSH access to the server. When executed this option will prompt for the SSH credentials. After connection via SSH, SLAnalyzer will make the appropriate calls to the registration service to register the appliance.

Get zypper Information

This option will perform serveral different zypper commands to report on the status of the update service on the appliance. This option requires SSH access to the server. When selected the user will be prompted for their SSH credentials.

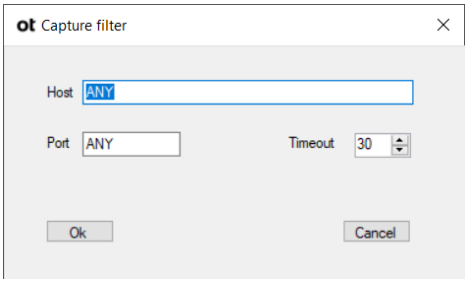
This option will report the following:

- Check for registration status.
- Report registered repositories - ls /etc/zypp/repos.d
- Report registered repository status - zypper lr
- Report installed zypper products - zypper search -i -t product
- Report installed zypper packages – zypper search -i -t package
- Report installed zypper patches - zypper search -i -t patch
- Report installed zypper patterns – zypper search -i -t pattern
- Report Available zypper updates - zypper lu
- Report Available zypper patches – zypper lp
- Check for consistency of requried dependencies - zypper ve

Capture packet trace

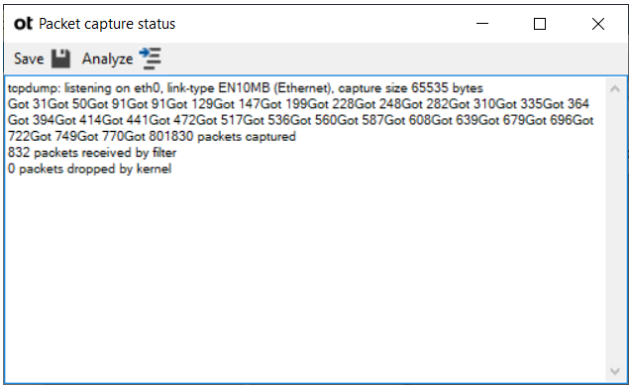
This option will capture a packet trace of the appliance. This option requires SSH access to the server. When selected the user will be prompted for their SSH credentials. After an SSH session is established then the user will be prompted for criteria for the packet capture.

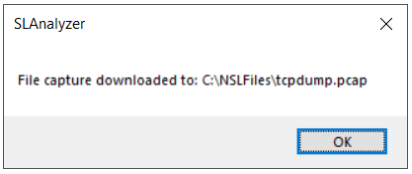
The user can limit the packet capture to a specific IP address or TCP port. By default, no filtering of the capture data is used. In addition to the filtering of packet data, the timeout value specifies the length of time the capture will be performed. The timeout value is in seconds.



After clicking Ok, the packet capture will be initiated on the common appliance host.

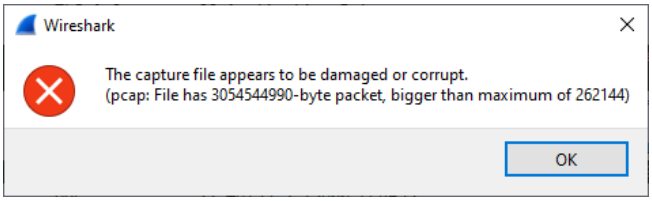
Once the packet capture has completed then the packet capture status window will display the number of packets captured. Also, a message indicating the location of the downloaded packet capture file will be displayed. Note that the packet capture file will be downloaded to the default SLAnalyzer report folder. (default c:\nslfiles). Also the filename of tcpdump.pcap is always used and the capture file will be overwritten if another packet capture is initiated. To retain the capture between capture sessions, rename the file tcpdump.pcap prior to running the trace again.

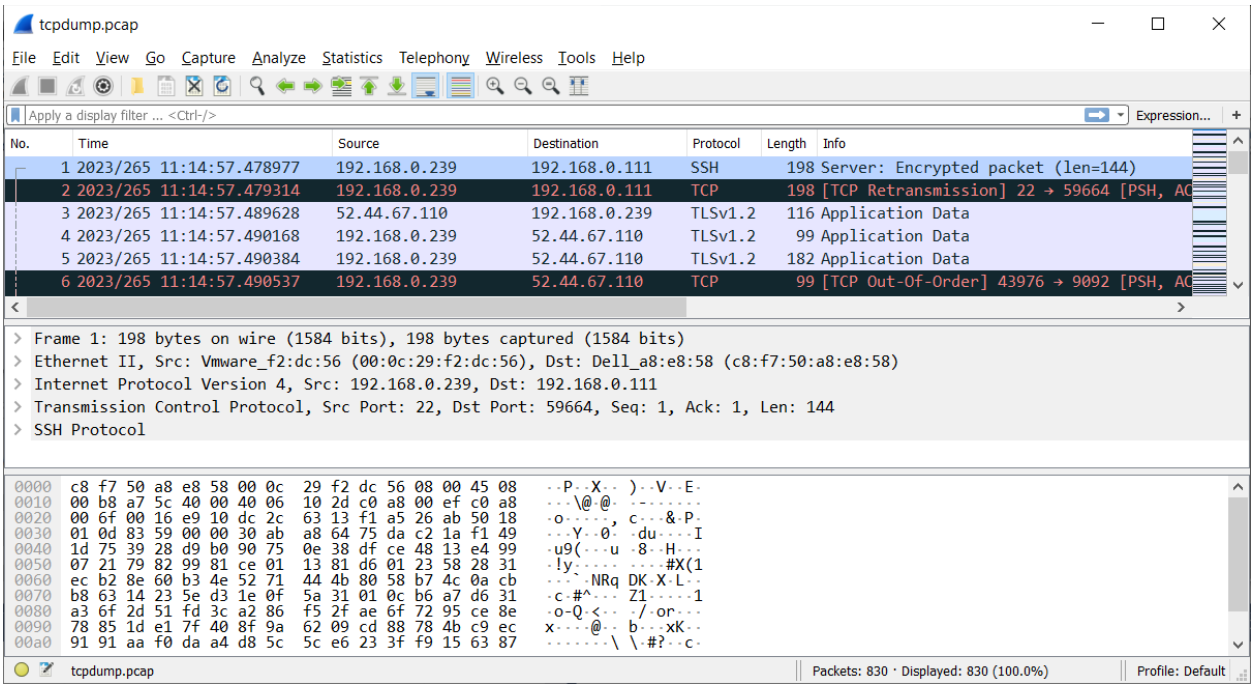




After successfully capturing the packet trace, open the trace file with Wireshark or other compatible trace utility.

Note that the packet trace is terminated while the trace utility is still capturing packets. It is normal to see an error similar to the one below when opening in Wireshark. This error message can be ignored.





It is important to understand that most of the traffic on a common appliance host will be encrypted. This is because the application running on top of the common appliance host is encrypting the data. Decryption of the traffic would have to be performed at the application layer and not at the common appliance host. The purpose of this option is to validate host connectivity and help in the troubleshooting of routing issues in the local network. It is not meant to provide analysis of the actual application running on top of the common appliance host.

Self Service Password Reset

This tools menu provides several options

1. REST Client – Tool to send REST calls to SSPR server for diagnostic and debugging purposes. Also provides links to common SSPR URL's.
2. Rights Validator – Tool to validate SSPR rights in the configured LDAP repository based upon the LDAPPermissionRecommendations.csv file or manually from the available user attributes found in the specified repository.
3. Command – This allows for administrative features like locking and unlocking the configuration on an SSPR server installed as an appliance or WAR deployment. This option will not function for a Windows deployment.

   There are several different options that can be selected.

   - Get App Version
   - Challenge Responses
     - Clear Local Responses
   - Configuration
     - Lock Configuration
     - Unlock Configuration
     - Set Configuration Password
     - Delete Configuration

SSPR REST Client

This option opens a window that will allow the testing of the SSPR REST API's.

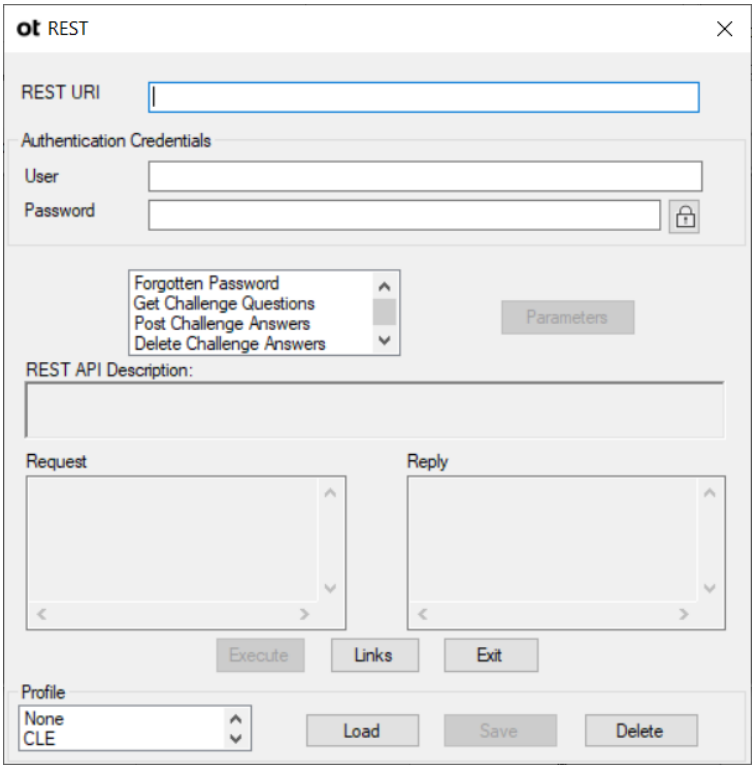


Figure 112 - SSPR REST Client

REST Client Window components

The REST Client window is composed of a number of different components.

- REST URI
- Authentication Credentials
- User
- Password
- REST Call Selection box
- Parameters button
- Request window
- Reply window
- Execute button
- Links button
- Exit button
- Profile data

Note: The SSPR server setting “Enable External Web Services” must be enabled for REST services to function properly.

REST URI

The REST URI is the full URL of the SSPR server including the path to the actual SSPR service.

For example
https://sspr.mydomain.microfocus.com:8443/sspr
Or
http://sspr.mydomain.microfocus.com:8080/sspr

Note: If CLE is installed on the workstation then the REST URI will be read from the CLE registry settings.

Authentication Credentials

Most of the REST calls made to SSPR require user credentials. The username and password provided in the authentication credentials are encrypted and included in the http header for authentication.

User

Any valid LDAP user on the SSPR server

Password

Password of the LDAP user on the SSPR server

REST Call Selection box

Listed in the selection box are the possible REST calls that can be made to a SSPR server. Each call has its own possible parameters and other requirements. Please refer to the documentation below for each possible REST call.

The possible REST calls are:

- Forgotten Password
- Get Challenge Questions
- Post Challenge Answers
- Delete Challenge Answers
- Post Check Password
- Get Health
- Get Profile
- Post Profile
- Get Random Password
- Post Random Password
- Post Set Password
- Get Statistics
- Get Status
- Post Verify OTP
- Post Verify Responses

Parameters button

The parameters button will become enabled when the selected REST call has additional parameters that can be passed or used in the request to the server. If there are no optional parameters then this button will be disabled.

REST API Description

This window will provide information about the REST call

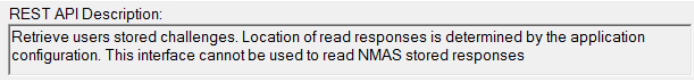


Figure 113 - REST API Description

Request window

The request window will show the syntax of the request being sent to the server.

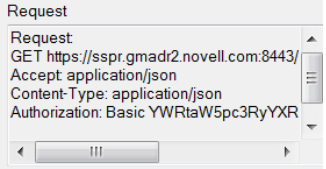


Figure 114 - REST Request window

Reply window

The reply window will show the response received from the SSPR server.

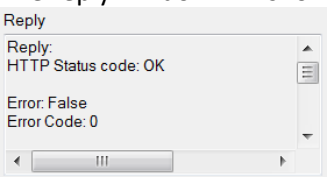


Figure 115 - REST Reply window

Execute button

The execute button will attempt to send the selected REST Call to the specified server. If the connection is encrypted then a window will popup providing the certificate details.

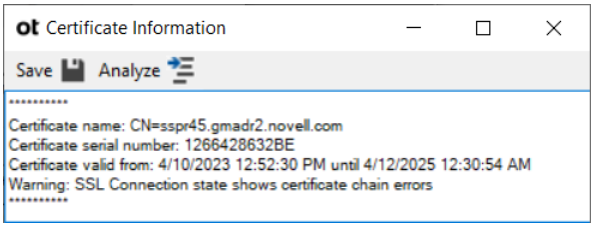


Figure 116 - Certificate details

Links button

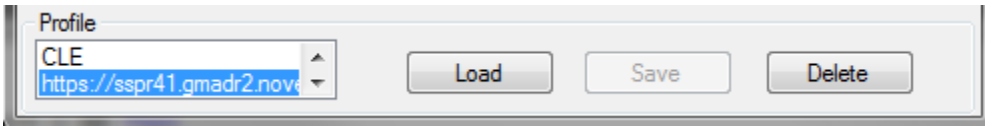
The Links button opens a window that displays common quick links to the SSPR server.

Exit button

The exit button will close the REST Client window and will return to the main SLAnalyzer window.

Profile data

The profile section allows the storing and retrieving of configuration information. The profile section has a Profile list selection box and 3 buttons (Load, Save, and Delete).



To store configuration information for the SSPR REST window, populate the fields within the window and then click the Save button.

For the SSPR REST client the fields REST URI and Authentication Credentials User are stored. The Authentication Credentials Password is not stored.

Profile data for the SSPR REST client is stored in the following location.
HKEY_CURRENT_USER\Software\MicroFocus\SLAnalyzer\SSPRRest
A new key will be created at thist location with the REST URI as the name. Within this key is a string value for Username.

To load a saved profile, scroll through the list of profiles and select the desired server profile. Then click the Load button. Note that if the Client Login Extension (CLE) client is detected then the Profile list will display the item CLE in the list. Selecting this option will populate the SSPR REST client with the REST URI configured for the CLE client.

To clear the current data in the CLE REST client fields, select the option “None” in the profile list box and then click the “Load” button.

To remove a stored profile, select the desired server item and click the Delete button. You cannot delete the Profile items “None” or “CLE”.

REST Calls

Forgotten Password

This REST call was implemented in SSPR version 4.6.

A multi-stage endpoint suitable for anonymous clients to implement a forgotten password module. Clients will call this service repeatedly until the process is completed. The following stages will be processed (some may be repeated or omitted based on policy and configuration):

- IDENTIFICATION
- METHOD_CHOICE
- TOKEN_CHOICE
- VERIFICATION
- ACTION_CHOICE
- NEW_PASSWORD
- COMPLETE

Each invocation of this service (except the first) requires a state parameter and form data. The state parameter is received from the previous invocation (or empty on the first call). It is the client's responsibility to maintain this state value throughout the process. If the state is invalid or expired, a new state will be generated by the server and the process restarted. The client can clear the state at any time to restart the sequence. Once the COMPLETE stage is reached, no further steps are possible and a new sequence will require discarding the state.

Each response from the service will include form data with one or more rows that will guide the client to create a UI for the user. Form fields are generally of type 'text' or 'select'. In the case of 'select' form fields, a 'selectOptions' value will include the possible values for the row. The next request to the server should include the state and the form data values for each form field. A form label and message is also included for display to the user.

The response from the service will include additional data of the 'stage' and 'method' (if appropriate). These values are informational and intended to aid the client in displaying an appropriate UI to the end user.

Errors can indicate syntax, operational, or internal errors. In most cases form data will also be included along with the error so that the user has an opportunity to attempt the operation again.

Stage 0 - Initial call

This request starts the forgotten password sequence. The request contains no parameter values.

Request:
POST https://sspr.example.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":null,"form":null}

The reply returns the information necessary for the forgotten password IDENTIFICATION stage.

Reply:
HTTP Status code: OK
Error? False
Error Code: 0
Stage: IDENTIFICATION
Label: Forgotten Password
Message: If you have forgotten your password, follow the prompts to reset your password.
Message detail:
Data name: sAMAccountName
Data Min Length: 1
Data Max Length: 64
Data Type: text
Data Required: True
Data label: Username
Data Select Options: {}

Stage IDENTIFICATION

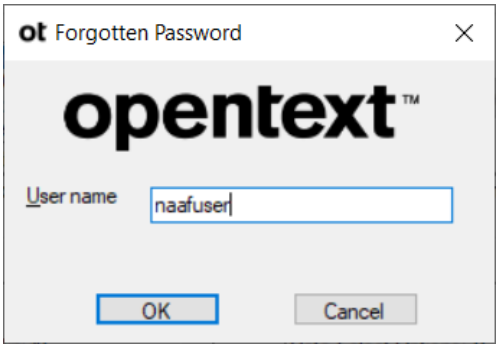
This stage identifies the user needing forgotten password. The request contains the user needing forgotten password. Included in the reply, the server will either return METHOD_CHOICE or VERIFICATION depending on the configuration.

If SSPR is configured for optional verification methods for forgotten password, then the next stage will be METHOD_CHOICE.
If SSPR is configured for mandatory verification methods, then the response will progress to the next stage of VERIFICATION for the first required verification method.

Request parameters are based upon the response from the previous response. An application can validate the information entered by the user using the previous response data.
IE….

Data name: sAMAccountName
Data Min Length: 1
Data Max Length: 64
Data Type: text
Data Required: True
Data label: Username
Data Select Options: {}

The user types in their username and then clicks the Ok button. SLAnalyzer sends the data to the server.



Request:
POST https://sspr45.gmadr2.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"Qi0zO9w2ytBzQmxFpGmJNaB2BR9nRyVJlh7zqxg2.H4sIAAAAAAAAAAEDAfz-dGpph832gDAQAA","form":{"sAMAccountName":"naafuser"}}

Reply:
HTTP Status code: OK
Error? False
Error Code: 0

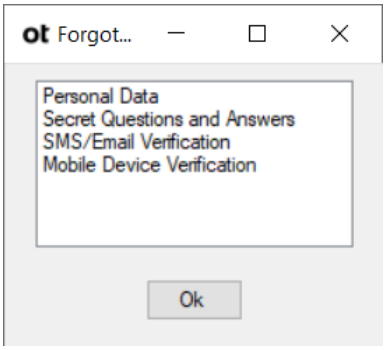
An invalid username will result in error 5008 being returned in the response.

Reply:
HTTP Status code: OK
Error? True
Error Code: 5006

Stage METHOD_CHOICE

This stage is repeated if multiple verification methods are set as optional.

SLAnalyzer now displays the list of verification methods to the user for selection. The list of verification methods was included in the response of the previous request. This could have been in response to an IDENTIFICATION or VERIFICATION stage. If a single verification method is defined, then this stage is not used. If multiple verification methods are defined, then the METHOD_CHOICE stage lists the possible user selections.



Stage VERIFICATION

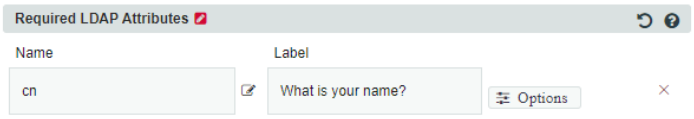
The VERIFICATION stage is the process of providing the information necessary to verify the user. Each verification method will require different information to complete the verification process. After sending the method choice to the server, the response will contain the required parameters for the verification stage of the selected method.

Supported Verification Methods

- LDAP Attributes
- Challenge Response
- Token SMS
- Token Email
- OTP Mobile Device Verification (Google Authenticator)

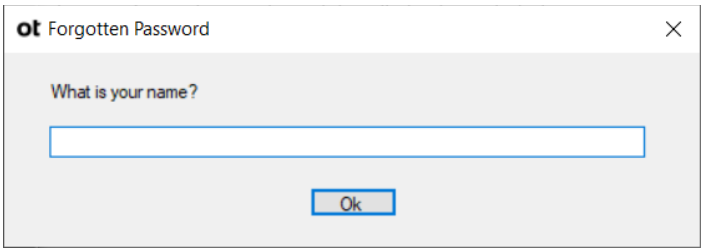
Verification Method LDAP Attributes

This verification method is defined in the SSPR configuration. It could be used to point to an attribute that contains information that the user would know. For example, their employee number. In this example we just defined the attribute cn for simplicity.



The previous reply specified the parameters for this verification method.

Data name: cn
Data Min Length: 0
Data Max Length: 255
Data Type: text
Data Required: False
Data label: What is your name?
Data Select Options: {}



When the user clicks the Ok button the attribute data is then sent to the server.

Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"bI8pyOrVBi6aFZj4okhZrBoQSBRXZhmHlhb1muyf.H4sIAAAAAAAAAAGuBVH6UFdNLkdDTTEQRoBEsJONk1A9FKnNPs
MybPeATdf_HNWMFds-zrtF- NE_boPk-MZacBXrgUAAA==","form":{"cn":"naafuser"}}

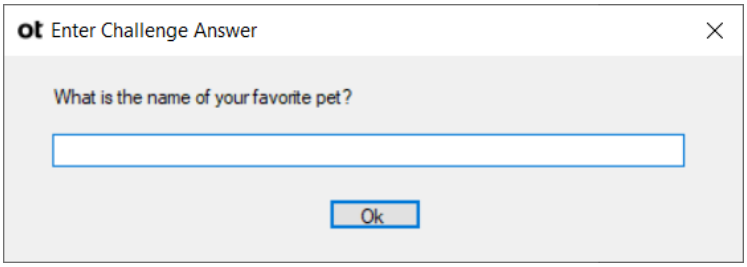
Reply:
HTTP Status code: OK
Error? False
Error Code: 0

Verification Method Challenge Response

The previous reply specified the parameters for this verification method.

Data name: PwmResponse_R_1
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: What is your favorite food?
Data Select Options: null
Data name: PwmResponse_R_2
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: What is the name of your favorite pet?
Data Select Options: null

SLAnalyzer will now prompt the user for each answer.



Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:

{"state":"FU2TJC4Aw6hU1Xoy7ki9X8ETmKMCzizklhb2omps.H4sIAAAAAAAAAAG2BUn6UFdNLkdDTTEQRoBEsJONk1A9FKnNPsMzc1yuPboFdYEALfrauMaJ8BDUh1dg0l41ux8DbLPYWv7Ckw0wRZoWJhFESX3vu1WbEX5iz4NhKqsq-2piv0FHBIyg0-FnroDn6cS4r9VVtgPe59XA27yKnHPzsn0Np7yA98kc71_o2S2BQAA","form":{"PwmResponse_R_1":"pizza","PwmResponse_R_2":"morris"}}

Reply:
HTTP Status code: OK
Error? False
Error Code: 0

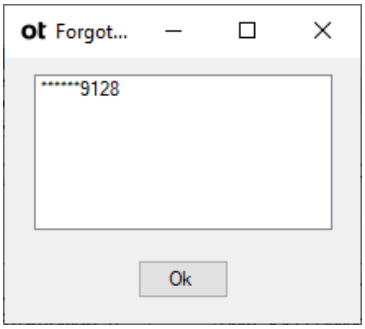
Verification Method TOKEN (SMS/Email)

This verification method is used for both SMS or Email tokens. The only real difference is that the server will return either a mobile number or an email address for user selection.

The previous reply specified the parameters for this verification method.

Data name: token
Data Min Length: 0
Data Max Length: 0
Data Type: select
Data Required: True
Data label: Select
Data Select Options:
{"49A19F4A553F4601883D7558DCB4B29AD878033BD1482EB258314B4BF8662363E4796421CEACC778EB15DFFF1BFE92E9D74EE302DC64F248C438E05D04459925":"******9128"}

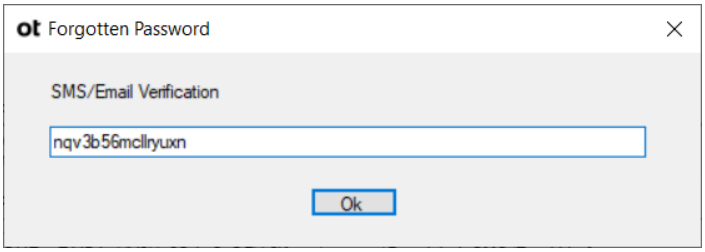
SLanalyzer will now prompt the user to select the account/number to send the token too.



Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"sXfYfh3iq6z3BvEswnrjfthwND4vogQwlhb2zv3l.H4sIAAAAAAAAAAGoBVf6UFdNLkdDTTEQRoBEsJONk1A9FKnNPsMzf6xtYrt9MIEUsgaDV3wCla7VgSKms4VCCGhaEGG1ApdxbyqIWa42o3C9YeIoy87rKgM1iGqVDIG6Rnxi-rKWnxMjlUe9QI6LB-kgkn6af5XVtsnB0NeWL_xLYJOor2K2TOmNuPuVD_w5DGtqAUAAA==","form":{"token":"49A19F4A553F4601883D7558DCB4B29AD878033BD1482EB258314B4BF8662363E4796421CEACC778EB15DFFF1BFE92E9D74EE302DC64F248C438E05D04459925"}}

Reply:
HTTP Status code: OK
Error? False
Error Code: 0
Stage: VERIFICATION
Label: Forgotten Password
Message: To verify your identity, a security code has been sent to you at ******9128. Please click the link in the email or copy and paste the security code here.
Message detail:
Data name: token
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: SMS/Email Verification
Data Select Options: null

The user receives the email or sms notification on their device and then type it into the prompt from SLAnalyzer.



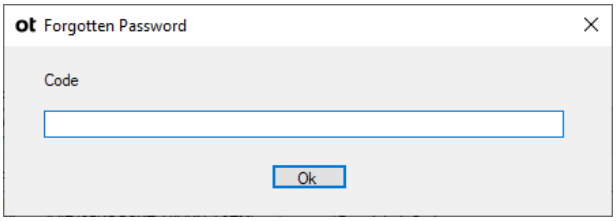
Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"sXfYfh3iq6z3BvEswnrjfthwND4vogQwlhb2zv3l.H4sIAAAAAAAAAAGABn_5UFdNLkdDTTEQRoBEsJONk1A9FKnNPsM0A
XsvzRTa44mOOcK-JDE_ScbPB2rMN3DgOZzzFJXW3jgeISdzrSB6GCsHG0zYYN9xiey1c_-oyARh2ChuG7Rv-
HQKRkKX9kO4gAYAAA==","form":{"token":"nqv3b56mcllryuxn"}}

Reply:
HTTP Status code: OK
Error? False
Error Code: 0

Verification Method OTP (Mobile device verification)

The previous reply specified the parameters for this verification method.

Data name: otpToken
Data Min Length: 0
Data Max Length: 0
Data Type: text
Data Required: True
Data label: Code
Data Select Options: null



Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"TZx3Z0T1iRxwt9xehGCt2hlpMjGjRFKrlhb3hzcv.H4sIAAAAAAAAAAGnBVj6UFdNLkdDTTEQRoBEsJONk1A9FKnNPsM0CmxE5CJJfOF_Jsb9aCCkFZpS8X_-cw4xC0G10z5lPLYaHs83JK7ufn9LcshwyipKr504XYnZqokodpb34UxS8b_shYYB-MT17q1QjWPEiuj5_yRND5Gp2tcTpQ3CEcBsJy_CJV9-zv5E51aRvlxxflpfR5yuLCwZWoFU3xEAkDn_B3TulyxzRUTfk-Ay0IT3_iNVs4OrYnKnOdfwSy5Znbwt-4Oom3e4R-vt__pSO4b20Uc69zBCgCnBQAA","form":{"otpToken":"390345"}}

Reply:
HTTP Status code: OK
Error? False
Error Code: 0

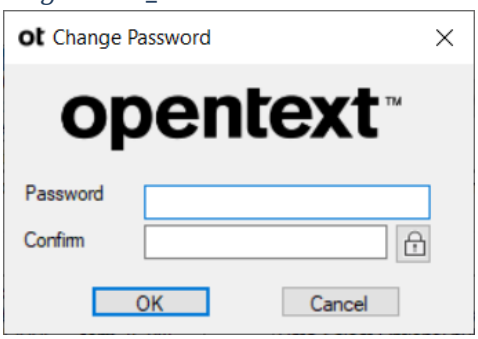
If there is an error processing the user input, the server just repeats the same stage. This means that SLAnalyzer will just redisplay the same window waiting on valid user data. There is no indication of a failure in the server response.

If the method succeeds, then the server will return the next stage.

The next stage would be on of the following:

1. Prompt the user for selection of another verification method with METHOD_CHOICE.
2. Force another verification method with VERIFICATION.
3. Proceed to the final stage of NEW_PASSWORD.

Stage: NEW_PASSWORD



Label: Change Password
Message: Please change your password. Keep your new password secure. After you type your new password, click the Change Password button. Your new password must meet the following requirements:
Message detail: Password is case sensitive.
Must be at least 7 characters long.
Must not include any of the following values: password test
Must not include part of your name or user name.
Must not include a common word or commonly used sequence of characters.
Data name: password1
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: Password
Data Select Options: null
Data name: password2
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: Confirm Password
Data Select Options: null
Stage NEW_PASSWORD

Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"Qi0zO9w2ytBzQmxFpGmJNaB2BR9nRyVJlh7zqxg2.H4sIAAAAAAAAAAHJBTb6UFdNLkdDTTEQRoBEsJONk1A9FKnNPsMqe8gOUrP04gQJMBavDC8lZhNC4Zhe-Gu4qEtTt5IMdTvBHfXK3Zyt9d7ZMyu3mTJU-uHnT8_aKp8EKvbCB2pJUa8lV1Gb7e6xoLVp2GN_WH3bjqf3cazyARup9_kWIhyQUAAA==","form":{"password1":"Password","password2":"Password"}}

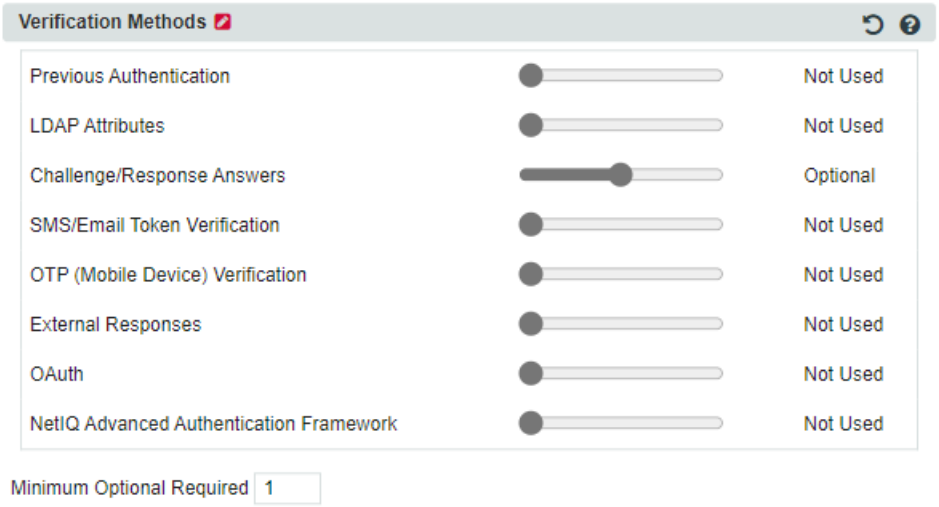
Reply:
HTTP Status code: OK
Error? False
Error Code: 0
Stage: COMPLETE
Label: Change Password
Message: The password has been changed successfully.
Message detail:

Example workflows

The following examples demonstrate how this REST call functions under different configurations.

Single mandatory verification method

In this example the SSPR server is configured for 1 verification method (Challenge Response Answers). Since the Minimum Optional Required is set to 1 then this method will always be required for forgotten password.



Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"mxamXfivNoYW2RGnfd4AdnOUqOLYYnd3lh9lfs4c.H4sIAAAAAAAAAAEDAfz-UFdNLkdDTTEQRoBEsJONk1A9FKnNPsMsBcXPW4_XwllZIbVp60ZO_-yrKcnTAWFqGkaGJ1-f6aOPQfj7dvb7xaw_wWG8eYirDHI29nFd4n8k_TlA7DQ1Fe5f1HHmMMABzL73slIdXyW8DAQAA","form":{"sAMAccountName":"naafuser"}}

Reply:
HTTP Status code: OK
Error? False
Error Code: 0
Stage: VERIFICATION
Label: Forgotten Password
Message: Please answer the following questions. If you answer these questions correctly, you will then be able to reset your password.
Message detail:
Data name: PwmResponse_R_1
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: What is the name of your favorite pet?
Data Select Options: null
Data name: PwmResponse_R_2
Data Min Length: 0

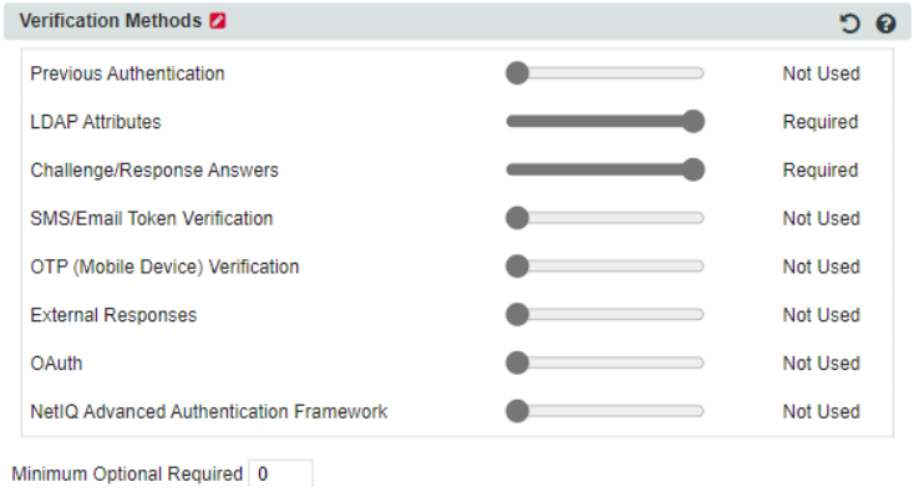
Data Max Length: 0
Data Type: password
Data Required: True
Data label: What was your favorite show as a child?
Data Select Options: null

Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"mxamXfivNoYW2RGnfd4AdnOUqOLYYnd3lh9lfs4c.H4sIAAAAAAAAAAGhBV76UFdNLkdDTTEQRoBEsJONk1A9FKnNPsMsC5kS0bBWk8W4y6ubMEqcZqDqaze-fWvGr_oJdtlehG4ajzwmNtDrwn4y58f0RbhbqQ466dSb6pohVftxrhPMqvSlBbndrjN4G5WmhBQAA","form":{"PwmResponse_R_1":"morris","PwmResponse_R_2":"star trek"}}

Reply:
HTTP Status code: OK
Error? False
Error Code: 0
Stage: NEW_PASSWORD
Label: Change Password
Message: Please change your password. Keep your new password secure. After you type your new password, click the Change Password button. Your new password must meet the following requirements:
Message detail: Password is case sensitive.
Must be at least 7 characters long.
Must not include any of the following values: password test
Must not include part of your name or user name.
Must not include a common word or commonly used sequence of characters.
Data name: password1
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: Password
Data Select Options: null
Data name: password2
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: Confirm Password
Data Select Options: null

Multiple required verification methods

In this example the SSPR server is configured for 2 required verification methods.



Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"RFMwznyfksfUAV1KNbKyhQUckt2iRfVGlh9m6ewo.H4sIAAAAAAAAAAEDAfz-UFdNLkdDTTEQRoBEsJONk1A9FKnNPsMtF9qT1Jw3G4ZuJFfXWDAz9Io6rwykZVA48B79Rno1nxbh5y_PjMXgWHhReRgs5iCVBnQwFBCbNiOPFRaKMX3Lv-0IDAQAA","form":{"sAMAccountName":"naafuser"}}

Reply:
HTTP Status code: OK
Error? False
Error Code: 0
Stage: VERIFICATION
Label: Forgotten Password
Message: Please answer the following questions. If you answer these questions correctly, you will then be able to reset your password.
Message detail:
Data name: cn
Data Min Length: 0
Data Max Length: 255
Data Type: text
Data Required: False
Data label: What is your name?
Data Select Options: {}

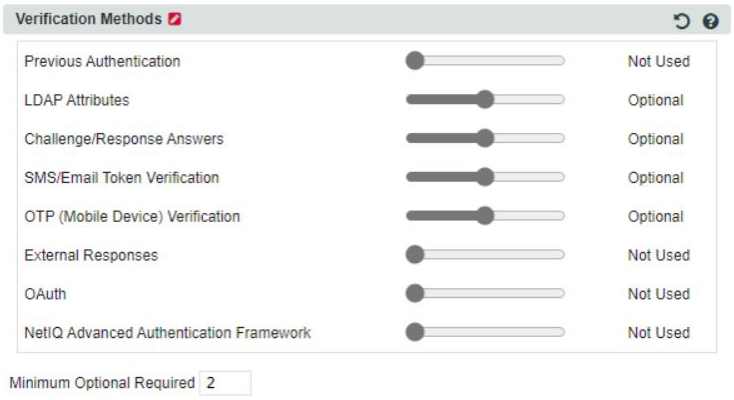
Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"RFMwznyfksfUAV1KNbKyhQUckt2iRfVGlh9m6ewo.H4sIAAAAAAAAAAGnBVj6UFdNLkdDTTEQRoBEsJONk1A9FKnNPsMtG92VNTj2PkGJM1nPRoceabn1ci4kFAtNP7G4ew1h4r9qwhfRi3gs-6CwxrS6jvZBoUTlf4_2FkwypVKGU1GXApOYyah65vYiynBQAA","form":{"cn":"naafuser"}}

Reply:
HTTP Status code: OK
Error? False
Error Code: 0
Stage: VERIFICATION
Label: Forgotten Password
Message: Please answer the following questions. If you answer these questions correctly, you will then be able to reset your password.
Message detail:
Data name: PwmResponse_R_1
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: What is the name of your favorite pet?
Data Select Options: null
Data name: PwmResponse_R_2
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: What was your favorite show as a child?
Data Select Options: null

Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"RFMwznyfksfUAV1KNbKyhQUckt2iRfVGlh9m6ewo.H4sIAAAAAAAAAAG-BUH6UFdNLkdDTTEQRoBEsJONk1A9FKnNPsMtHUCMqFMuwZ1HifruC-gA5d-WRFlAqEYb4FAAA=","form":{"PwmResponse_R_1":"morris","PwmResponse_R_2":"star trek"}}

Reply:
HTTP Status code: OK
Error? False
Error Code: 0
Stage: NEW_PASSWORD
Label: Change Password
Message: Please change your password. Keep your new password secure. After you type your new password, click the Change Password button. Your new password must meet the following requirements:
Message detail: Password is case sensitive.
Must be at least 7 characters long.
Must not include any of the following values: password test
Must not include part of your name or user name.
Must not include a common word or commonly used sequence of characters.
Data name: password1
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: Password
Data Select Options: null
Data name: password2
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: Confirm Password
Data Select Options: null

Multiple optional verification methods



Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"1jLGAlYc1uVx9eC8lJQR0VbDk3EpE14Nlhawfkaw.H4sIAAAAAAAAAAEDAfz-UFdNLkdDTTEQRoBEsJONk1A9FKnNPsMuUAXtB2-5IXnEdd6K_6lKcqifeTlcCJkCmjpXuucCsdy9VAcRD_cXgp93Vs4Aaowo3B3WppezfgFhyPqF3oj9DnMzTe3tkH6AWvvNc9i2zyQt6GHWQshoUibwNaagH5bp5n_IrjBUCLhGCL7W8fTzn76ICKl0PdRb-yBhh4lkMuISCuyPA00FLS0rGvu2167Ygsj1b-x6QKGOxbyV6cJUfl-7F-WZy4dOUQmfCxU-GERlVWtAAoR3Uq2-3RJplVtQdbXSpI2ztkEDtH87NMGCPXYdhqIgtZC_kxH0FNgRureyk4vrLHo5mUSrhbEW6VkDAQAA","form":{"sAMAccountName":"naafuser"}}

Reply:
HTTP Status code: OK
Error? False
Error Code: 0
Stage: METHOD_CHOICE
Label: Forgotten Password
Message: Please select one of the following methods to verify your identity. Note: If your administrator requires multiple forms of verification, you will be redirected back to this page until all verification criteria is met.
Message detail:
Data name: methodChoice
Data Min Length: 0
Data Max Length: 255
Data Type: select
Data Required: True
Data label: Select
Data Select Options: {"ATTRIBUTES":"Personal Data","CHALLENGE_RESPONSES":"Secret Questions and Answers","TOKEN":"SMS/Email Verification","OTP":"Mobile Device Verification"}

Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"1jLGAlYc1uVx9eC8lJQR0VbDk3EpE14Nlhawfkaw.H4sIAAAAAAAAAAGkBVv6UFdNLkdDTTEQRoBEsJONk1A9FKnNPs

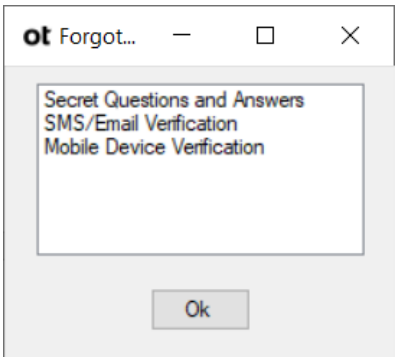
MuVhNIAI87clNNhc7_hWsahff0xyXtuKL8Uhc-Jeko887flzklgBzoBHNC7xMQN2rVPpwgDG7rvOkBQAA","form":{"methodChoice":"ATTRIBUTES"}}

Reply:
HTTP Status code: OK
Error? False
Error Code: 0
Stage: VERIFICATION
Label: Forgotten Password
Message: Please answer the following questions. If you answer these questions correctly, you will then be able to reset your password.
Message detail:
Data name: cn
Data Min Length: 0
Data Max Length: 255
Data Type: text
Data Required: False
Data label: What is your name?
Data Select Options: {}

Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"1jLGAlYc1uVx9eC8lJQR0VbDk3EpE14Nlhawfkaw.H4sIAAAAAAAAAAG5BUb6UFdNLkdDTTEQRoBEsJONk1A9FKnNPsMuVwkP6Bw6mkbPkXRLwZu5kJtIXpWqYb1OCsfzmUgbGhkKWUDPpE7l7zwXxGNabLE_YS3tApgPZecFhUu9mqLTPUuC0ke637I9fu_0UHDqJ41cJSKQzR3zlHKgTxBCOZMe-12saJYcBJP-Vv9KANlJw6m38fhGxaOLhYOuDLFthXBDOhXNIKc_miou5BQAA","form":{"cn":"naafuser"}}

Reply:
HTTP Status code: OK
Error? False
Error Code: 0
Stage: METHOD_CHOICE
Label: Forgotten Password
Message: Please select one of the following methods to verify your identity. Note: If your administrator requires multiple forms of verification, you will be redirected back to this page until all verification criteria is met.
Message detail:
Data name: methodChoice
Data Min Length: 0
Data Max Length: 255
Data Type: select
Data Required: True
Data label: Select
Data Select Options: {"CHALLENGE_RESPONSES":"Secret Questions and Answers","TOKEN":"SMS/Email Verification","OTP":"Mobile Device Verification"}

SLAnalyzer then prompts the user to select a second method



Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"1jLGAlYc1uVx9eC8lJQR0VbDk3EpE14Nlhawfkaw.H4sIAAAAAAAAAAGyBU36UFdNLkdDTTEQRoBEsJONk1A9FKnNPsMuWJb9l8gPDu049Q1VjK_vzqiyMhmLNYdQSiIxvGHe4jGtSFqMfUD7xD3kao6KQq2HGcY7CDRiPUhf76Oz8VwOV5d6j7sEdjlEyzdMRZNKm6145BkJKc29kQtRr7S3FxbcMNrIFAAA=","form":{"methodChoice":"CHALLENGE_RESPONSES"}}

Reply:
HTTP Status code: OK
Error? False
Error Code: 0
Stage: VERIFICATION
Label: Forgotten Password
Message: Please answer the following questions. If you answer these questions correctly, you will then be able to reset your password.
Message detail:
Data name: PwmResponse_R_1
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: What is the name of your favorite pet?
Data Select Options: null
Data name: PwmResponse_R_2
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: What was your favorite show as a child?
Data Select Options: null

Request:
POST https://sspr.novell.com/sspr/public/rest/forgottenpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Params:
{"state":"1jLGAlYc1uVx9eC8lJQR0VbDk3EpE14Nlhawfkaw.H4sIAAAAAAAAAAHQBS_6UFdNLkdDTTEQRoBEsJONk1A9FKnNPsMuWdrl6AFA341S943i-3UYdAwyVGOe7NakXyle6UBQAoBAfSFOpuk8ZmbFCS8hbSGtbjG227Hv2xhdkkf1tUZbEy8p69tEA-nkHtvDpq8U4Q0PVFhjJng_HrkkZNo-a4q-FH7LaXnCZ7GhsRGm6KSSEFY2jhYx-i1vqOzVrZTqPMNNHkEBVOZPjb_htAFAAA=","form":{"PwmResponse_R_1":"morris","PwmResponse_R_2":"star trek"}}

Reply:
HTTP Status code: OK
Error? False
Error Code: 0
Stage: NEW_PASSWORD
Label: Change Password
Message: Please change your password. Keep your new password secure. After you type your new password, click the Change Password button. Your new password must meet the following requirements:
Message detail: Password is case sensitive.
Must be at least 7 characters long.
Must not include any of the following values: password test
Must not include part of your name or user name.
Must not include a common word or commonly used sequence of characters.
Data name: password1
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: Password
Data Select Options: null
Data name: password2
Data Min Length: 0
Data Max Length: 0
Data Type: password
Data Required: True
Data label: Confirm Password
Data Select Options: null

Note: SSPR does not currently validate if the verification method is valid for the specified user. For example, if OTP is selected by the user but they have not enrolled their smartphone with google authenticator, the verification will fail. Or if the user selects SMS/Email Token verification but they do not have a valid email or mobile number set in the LDAP repository then these methods will fail as well.

Get Challenge Questions

Retrieve user's stored challenges. Location of read responses is determined by the application configuration. This interface cannot be used to read NMAS stored responses.

This REST call requires user authentication so the username and password field must be set. Once selected the Parameters button is enabled. Clicking on the Parameters button gives the following optional parameters.

Parameters

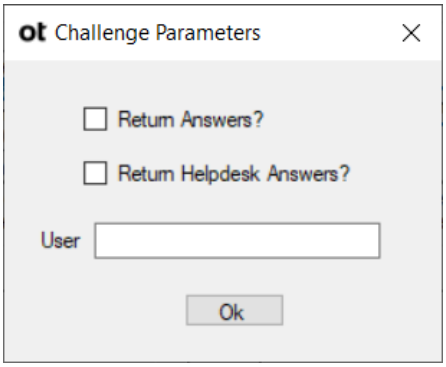


Figure 117 - Get Challenge Questions Parameters

- Return Answers? - Will return the encrypted answers currently stored in the database. These really have no value for testing purposes since they are not readable. The SSPR server setting "Allow Web Services to Read Answers" must be enabled.
- Return Helpdesk Answers? - Will return the encrypted helpdesk answers. Like the option previous these really have no value in testing. The SSPR server setting "Allow Web Services to Read Answers" must be enabled. Also, a helpdesk profile also needs to be enabled.
- User – This optional field specifies that this operation is to be on this user object and not on the user being authenticated. Note that the user specified on the main window for authentication must have the necessary rights to modify other users in the LDAP directory. The SSPR server setting "Web Services Third Party Permissions" must succeed to use this parameter.

Click the execute button to send this REST call to the SSPR server.

Sample request

GET https://sspr.novell.com:8443/sspr/public/rest/challenges HTTP/1.1
Accept: application/json
Content-Type: application/json
Authorization: Basic YWRtaW5pc3RyYXRvcjpDbGlwcGVyMQ==

Sample reply

HTTP Status code: OK

Error: False
Error Code: 0
username: default
Answered challenge questions
Question What was your favorite show as a child?
Min Length: 4
Max Length: 200
Admin Defined: True
Required: False
Max Question Chars: 0
Enforce Word List: False
Minimum Randoms: 1

Defined challenge questions:
Question What is the name of the main character in your favorite book?
Min Length: 4
Max Length: 200
Admin Defined: True
Required: False
Max Question Chars: 3
Enforce Word List: True

Question What is the name of your favorite teacher?
Min Length: 4
Max Length: 200
Admin Defined: True
Required: False
Max Question Chars: 3
Enforce Word List: True

Minimum Randoms: 2

Post Challenge Answers

Set users stored challenge/response set.

Before you can issue the Post Challenge Answers you must first issue the call Get Challenge Questions. The challenge set information returned from the server will provide the data necessary to issue this call. Click the parameters button to list all the possible questions.

Parameters

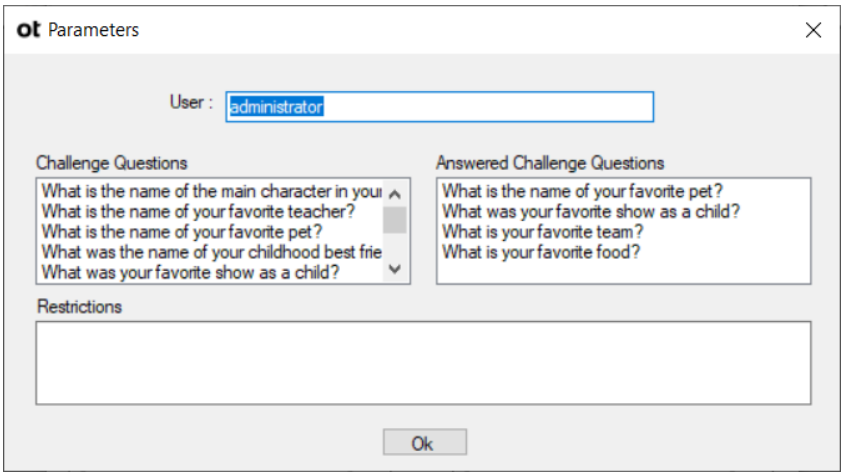


Figure 118 - Post Challenge Answers Parameters

If there were any questions answered previously by this user, then those questions will appear in the Answered Challenge Questions window. Notice that the questions answered still appear in the list of possible Challenge Questions.

When submitting this call the server, the server will set the answers to the questions defined here. If there are questions listed in the Answered Challenge Questions list but you do not provide the answer to that question, then that answered question will be deleted from the server when you submit this new set of answers.

For example, if you have previously answered question 1 and question 2, but then issue this call and only provide answer 1, then only answer 1 will be defined. The challenge answer for question 2 will no longer be valid. The next time you issue a Get Challenge Answers only question 1 will be listed in the Answered Challenge Question list.

Selecting a question

To select a question, click on one of the entries in the Challenge Questions list. The Restrictions window will display the policy restrictions that must be matched by the answer.

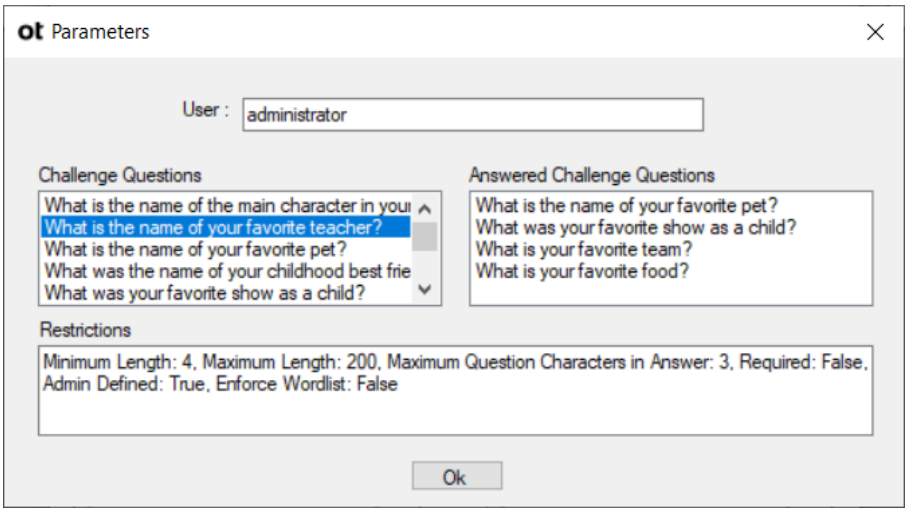


Figure 119 - Challenge Answer Restrictions

Entering a new answer to a challenge question

Double clicking on one of the entries in the Challenge Questions list will allow the user to enter an answer for that entry. The answer entered must meet the restrictions that were listed.

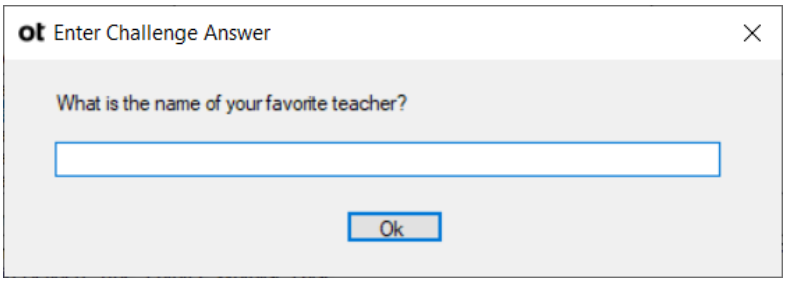


Figure 120 - Entering a Challenge Answer

After entering an answer press the Ok button.

SLAnalyzer will evaluate the answer provided when you press the Ok button against the restrictions. If the answer fails, the evaluation then a message will be displayed to the user to try again.

After entering the answer and pressing the Ok button the answered question will now be listed in the Answered Challenge Questions box.

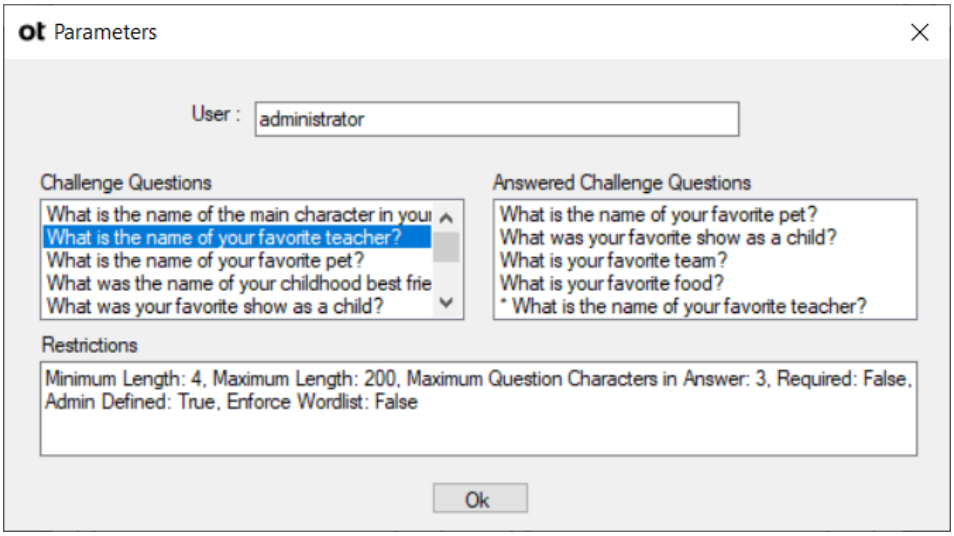


Figure 121 - Answered question updated

If you click the Ok button on the parameters window you will be notified if you have not defined any answers. Note that this does not tell you if there are incomplete answers.

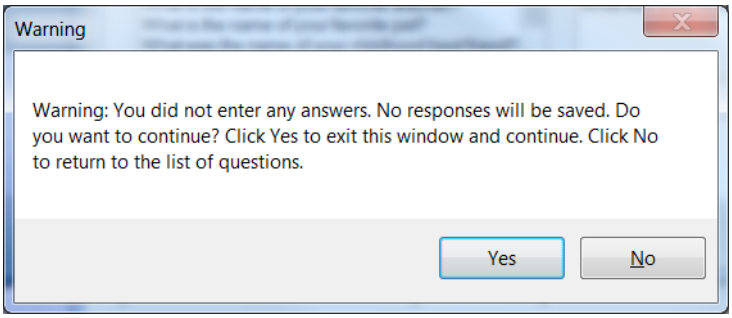


Figure 122 - Prompt for no answers defined

After defining the answers to the challenge questions then click the execute button to send this call to the server. If you did not enter any answers, then SLAnalyzer will display an error message.

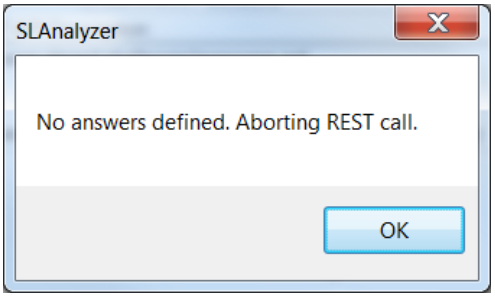


Figure 123 - No answers aborting call.

Sample request

POST https://sspr.novell.com:8443/sspr/public/rest/challenges HTTP/1.1
Accept: application/json
Content-Type: application/json
Authorization: Basic YWRtaW5pc3RyYXRvcjpDbGlwcGVyMQ==
{
"username":"administrator",

{"challenges":[{"challengeText":"What was your favorite show as a
child?","minLength":4,"maxLength":200,"adminDefined":true,"required":false,"answer":{"answerText":"brit"}},{"challengeText":"What was
your favorite show as a child?","minLength":4,"maxLength":200,"adminDefined":true,"required":false,"answer":{"answerText":"star
trek"}}],"minimumRandoms":2,"username":""}

Sample reply

HTTP Status code: OK

{"error":false
"errorCode":0
"successMessage":"Thank you. Your secret questions and answers have been successfully saved. If you ever forget your password you can use
the answers to these questions to reset your password."}

Post Verify Responses

Validate supplied challenge response answers against a user's stored responses. Note this service will not work properly if the user's responses are stored only in the NMAS repository.

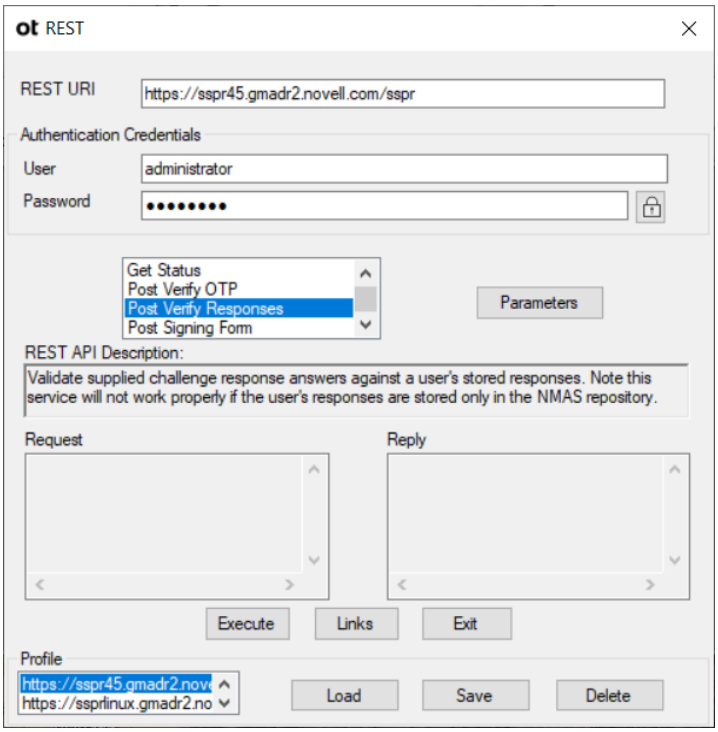


Figure 124 - Post Verify Responses

Requires authentication so the Authentication Credentials must be provided.

This call utilizes the challenge question and answer set retrieved with the Get Challenge Questions REST call. The user must first execute the Get Challenge Questions call prior to calling Post Verify Responses.

Parameters

Provides the details on what answers have been defined for this user.

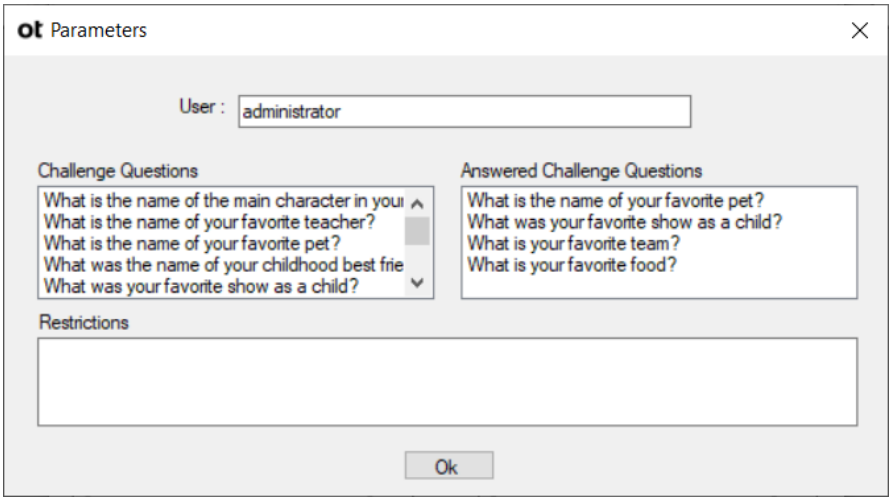


Figure 125 - Post Verify Responses Parameters

Click the execute button to submit this call to the SSPR server. SLAnalyzer will now prompt the user for each answer.

Challenge prompt

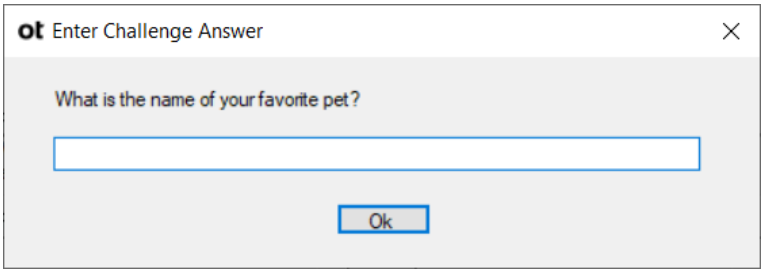


Figure 126 - Verify Responses Challenge Prompt

The user must provide each answer exactly. This is character case sensitive.

Sample request

POST https://sspr.novell.com:8443/sspr/public/rest/verifyresponses HTTP/1.1
Accept: application/json
Content-Type: application/json
Authorization: Basic YWRtaW5pc3RyYXRvcjpDbGlwcGVyMQ==

{"username":"administrator","challenges":[{"challengeText":"What was your favorite show as a child?","minLength":4,"maxLength":200,"adminDefined":true,"required":false,"answer":{"answerText":"star trek"}}]}

Sample reply

HTTP Status code: OK

{"error":false
"errorCode":0
"successMessage":"The operation has been successfully completed."
"data":true}
Responses Matched.

Delete Challenge Answers

Clear users saved challenge responses.

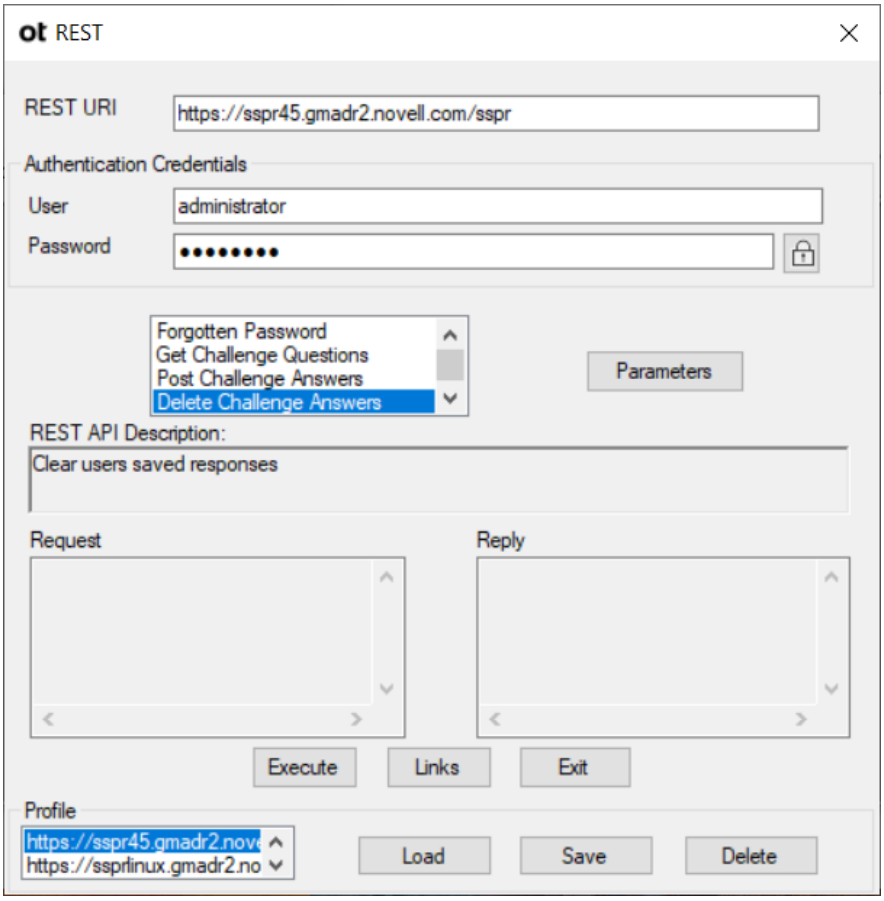
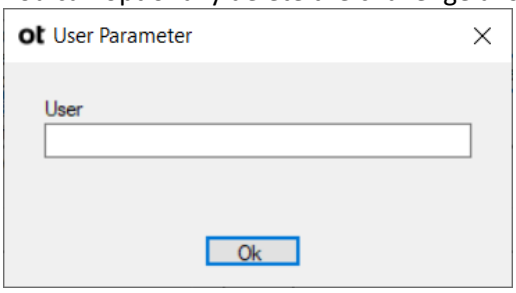


Figure 127 - Delete Challenge Answers

Parameters

You can optionally delete the challenge answers on a different user.



Click the execute button to send the call to the server.

Sample request

```
DELETE https://sspr.novell.com:8443/sspr/public/rest/challenges HTTP/1.1
Accept: application/json
Content-Type: application/json
Authorization: Basic YWRtaW5pc3RyYXRvcjpDbGlwcGVyMQ==
```

Sample reply

HTTP Status code: OK


```
{"error":false
"errorCode":0
"successMessage":"The operation has been successfully completed."}
```

Post Check Password

Check a password value(s) against user policy

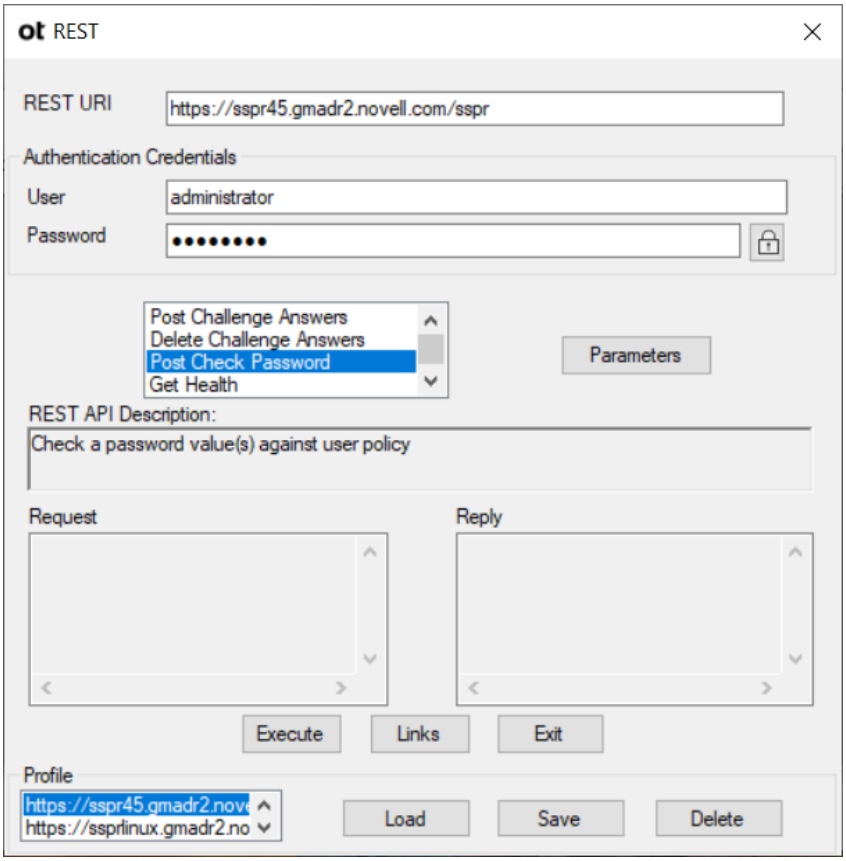


Figure 128 - Post Check Password

Parameters

Prior to making this call, the user must specify the password to verify. The user can optionally specify a different user object to verify the password against.

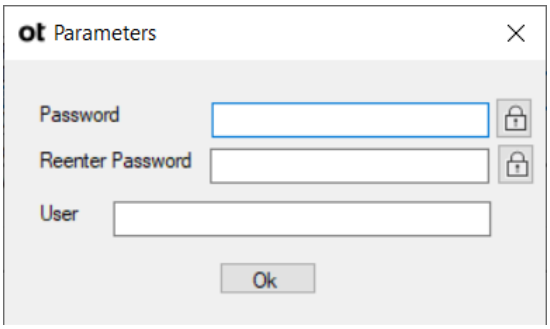


Figure 129 - Post Check Password Parameters

Click the execute button to submit the call to the SSPR server. If the password fails, the password policy an error will be returned indicating why the password failed.

Sample request

```
POST https://sspr.novell.com:8443/sspr33build96/public/rest/checkpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Authorization: Basic YWRtaW5pc3RyYXRvcjpDbGlwcGVyMQ==
{
"username":"administrator",
"password1":"NewPWD123",
"password2":"NewPWD123"
}
```

Sample reply

HTTP Status code: OK


```
{"error":false
"errorCode":0
"data":{"version":2
"strength":56
"match":"MATCH"
"message":"New password accepted please click change password"
"passed":true
"errorCode":0}}
```

Get Health

Gets the health of the SSPR server

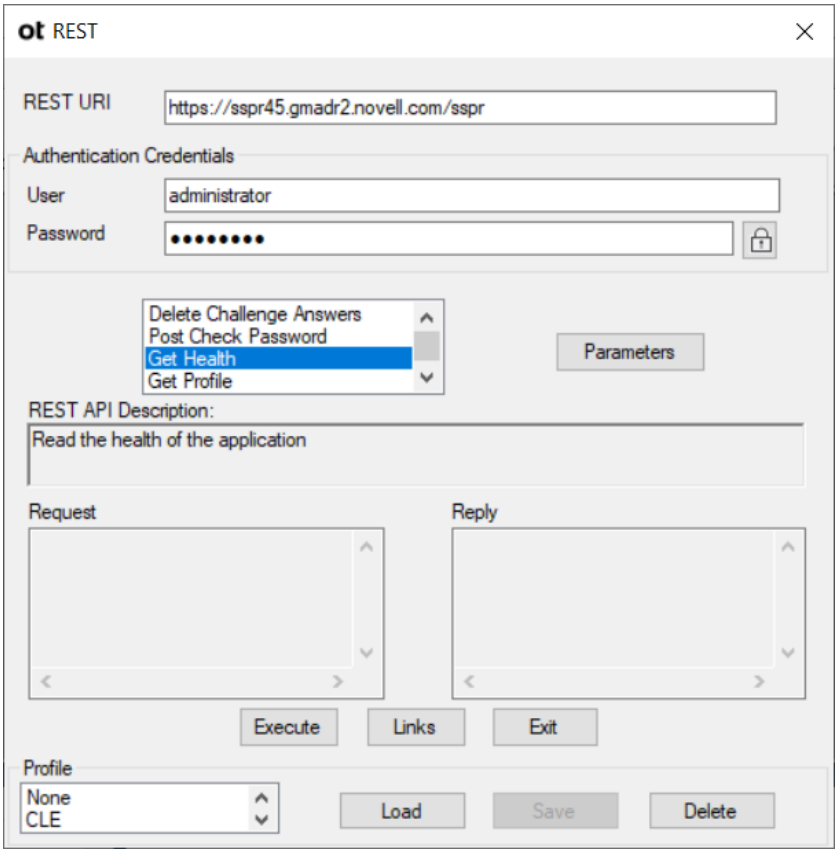


Figure 130 - Get Health

Parameters

There is only one parameter for this REST call.

If the Refresh Immediately checkbox is checked then the SSPR server will refresh prior to send the health information.

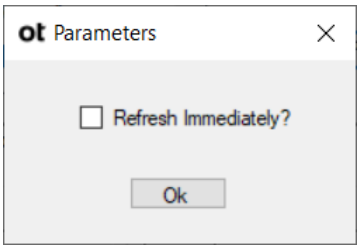


Figure 131 - Get Health Parameters

Click the execute button to submit this call to the SSPR server.

The information returned by this call is the same information as seen on the health screen in the administration console.



Figure 132 - Server Health

Note that the SSPR server setting “Enable Public Health and Statistics Web Service” must be enabled.

Sample request

GET https://sspr.novell.com:8443/sspr/public/rest/health HTTP/1.1
Accept: application/json
Content-Type: application/json
Authorization: Basic YWRtaW5pc3RyYXRvcjpDbGlwcGVyMQ==

Sample reply

HTTP Status code: OK

Server Response:
{"error":false
"errorCode":0
"data":{"timestamp":"2015-07-24T17:26:20Z"
"overall":"CONFIG"
"records":[{"status":"CONFIG"
"topic":"Configuration"
"detail":"AppProperty ⇨ ldap.promiscuousEnable setting should be set to false for proper security"}
{"status":"CONFIG"
"topic":"Configuration"
"detail":"LDAP ⇨ LDAP Directories ⇨ default ⇨ LDAP Proxy Password strength of password is weak (33/100); increase password length/complexity for proper security"}
{"status":"CONFIG"
"topic":"Configuration"
"detail":"Settings ⇨ Security ⇨ Web Security ⇨ Require HTTPS setting should be set to true for proper security"}
{"status":"GOOD"
"topic":"LDAP"
"detail":"All configured LDAP servers are reachable"}
{"status":"GOOD"
"topic":"LDAP"
"detail":"LDAP test user account is functioning normally for profile default"}
{"status":"GOOD"
"topic":"LocalDB"
"detail":"LocalDB and related services are operating correctly"}
{"status":"GOOD"
"topic":"Platform"
"detail":"Java platform is operating normally"}]}}

Get Profile

Returns profile information on a user

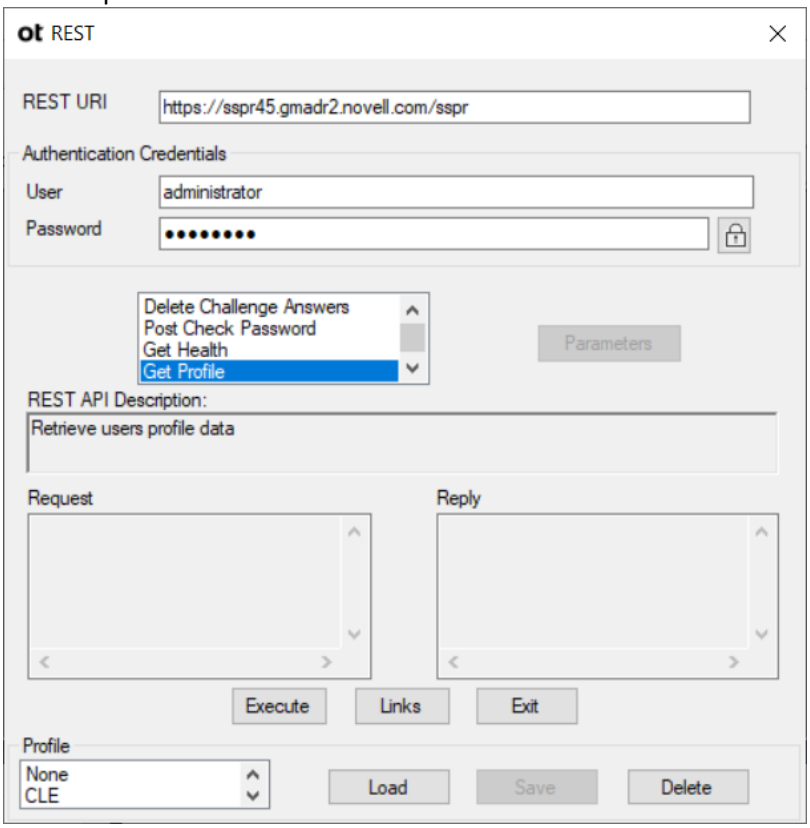


Figure 133 - Get Profile

There are no optional parameters for this call. This call requires authentication and the profile information returned will apply to the authentication user.

The information returned for this API is defined in the SSPR configuration under Modules/Update Profile

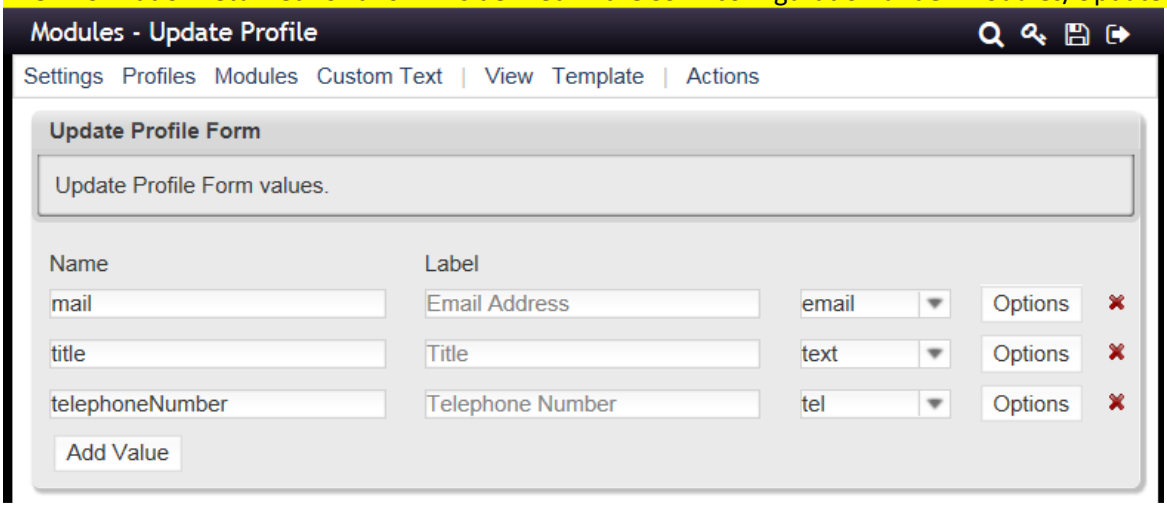


Figure 134 - Server profile settings

Sample request

GET https://sspr.novell.com:8443/sspr/public/rest/profile HTTP/1.1
Accept: application/json
Authorization: Basic YWRtaW5pc3RyYXRvcjpDbGlwcGVyMQ==

Sample reply

HTTP Status code: OK

Server Response:
{"error":false,"errorCode":0,"data":{"profile":{"telephoneNumber":"918-555-1212","mail":"testuser@gmail.com","givenName":"Testme","title":"Domain administrator for gmadr2 domain"},"formDefinition":[{"name":"mail","minimumLength":1,"maximumLength":64,"type":"email","required":true,"confirmationRequired":false,"readonly":false,"unique":true,"labels":{"":"Email Address"},"regexErrors":{"":""},"description":{"":""},"selectOptions":{}},{"name":"title","minimumLength":1,"maximumLength":64,"type":"text","required":false,"confirmationRequired":false,"readonly":false,"unique":false,"labels":{"":"Title"},"regexErrors":{"":""},"description":{"":""},"selectOptions":{}},{"name":"telephoneNumber","minimumLength":1,"maximumLength":64,"type":"tel","required":false,"confirmationRequired":false,"readonly":false,"unique":false,"labels":{"":"Telephone Number"},"regexErrors":{"":""},"description":{"":""},"selectOptions":{}},{"name":"givenName","minimumLength":0,"maximumLength":255,"type":"text","required":false,"confirmationRequired":false,"readonly":false,"unique":false,"labels":{"":"givenName"},"regexErrors":{"":""},"description":{"":""},"selectOptions":{}}]}}

{"error":false
"errorCode":0
"data":{"profile":{"telephoneNumber":"918-555-1212"
"mail":"testuser@gmail.com"
"givenName":"Testme"
"title":"Domain administrator for gmadr2 domain"}
"formDefinition":[{"name":"mail"
"minimumLength":1
"maximumLength":64
"type":"email"
"required":true
"confirmationRequired":false
"readonly":false
"unique":true
"labels":{"":"Email Address"}
"regexErrors":{"":""}
"description":{"":""}
"selectOptions":{}}]}}

Post Profile

Sets Profile data on a user

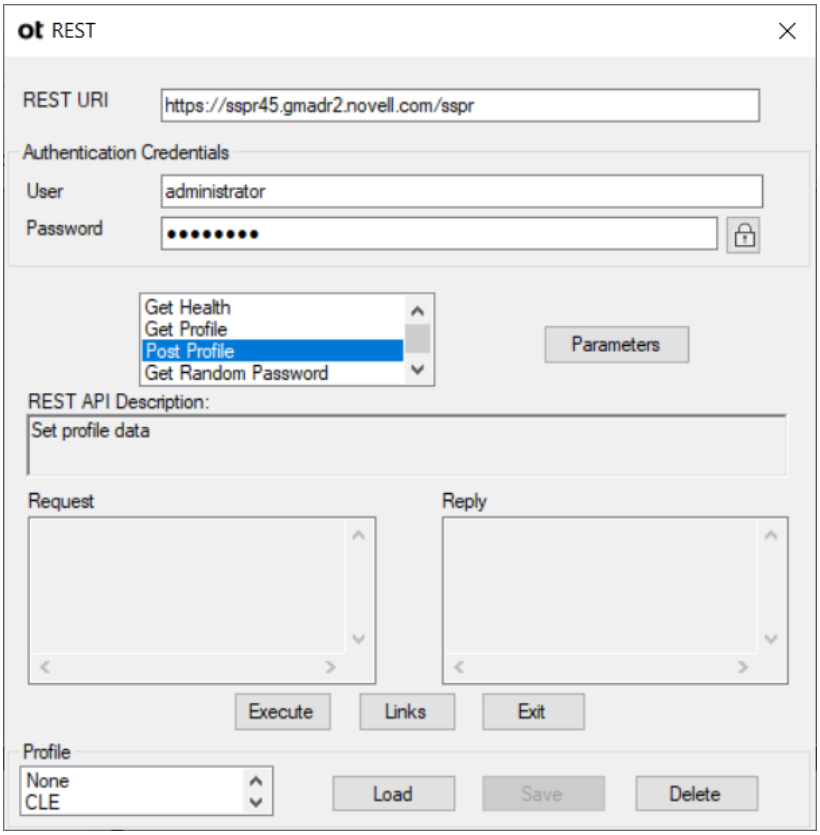


Figure 135 - Post Profile

This call requires information returned by the Get Profile call. First execute a Get Profile request to populate the optional parameters for this call.

Parameters

The parameters will display the profile data read from the server with the Get Profile call

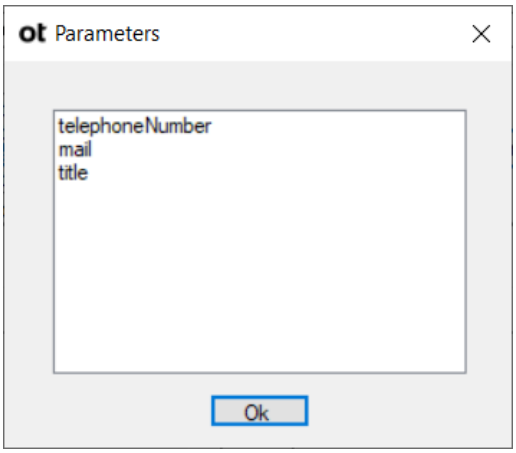


Figure 136 - Post Profile Parameters

Modifying profile data

To view or modify data within the profile, highlight and then double click on the entry.

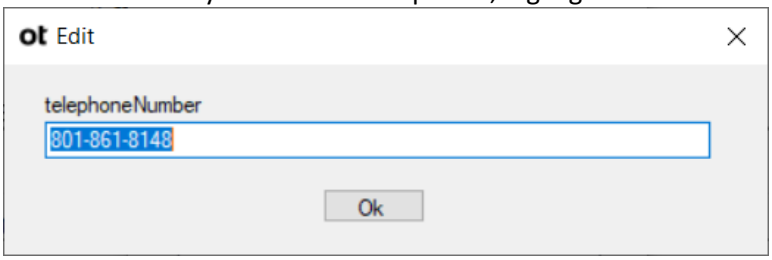


Figure 137 - Modifying profile data

Edit the information and click the Ok button to return to the parameters window.
Click the execute button to send this call to the SSPR server.

Sample request

```
POST https://sspr.novell.com:8443/sspr/public/rest/profile HTTP/1.1
Accept: application/json
Content-Type: application/json
Authorization: Basic YWRtaW5pc3RyYXRvcjpDbGlwcGVyMQ==
{
"profile":{
"telephoneNumber":"918-555-1212",
"mail":"testuser@gmail.com",
"givenName":"Testme",
"title":"Domain administrator for gmadr2 domain"
}}
```

Sample reply

HTTP Status code: OK

```
{"error":false
"errorCode":0
"successMessage":"Your user information has been successfully updated."}
```

Get Random Password

Gets a random password based upon user's password policy and other criteria.

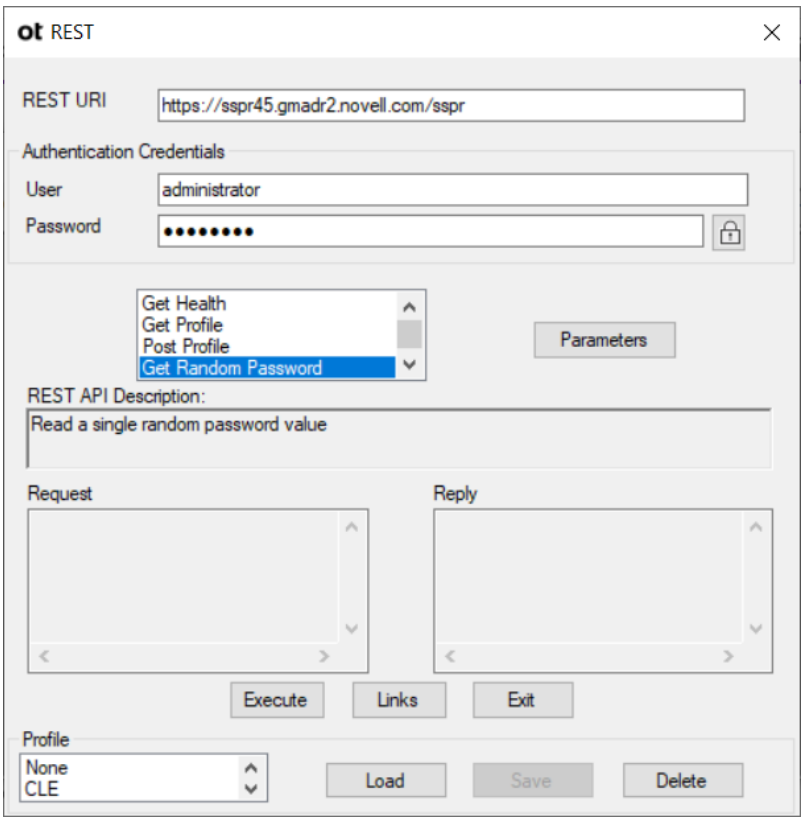


Figure 138 - Get Random Password

Parameters

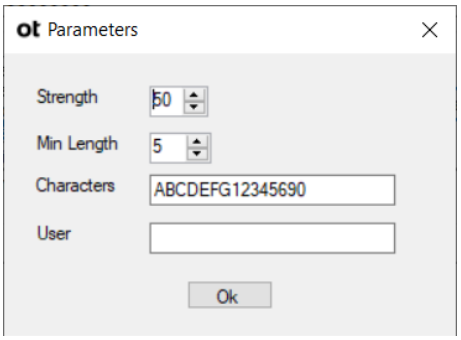


Figure 139 - Get Random Password Parameters

- Strength should be set to the desired strength/complexity of the generated password. (default is 50)
- Min Length is the minimum length of the generated password. (default 5)
- User is the optional user object.

If successful a random password will be returned that matches the defined criteria.

Sample request

```
GET https://sspr.novell.com:8443/sspr/public/rest/randompassword HTTP/1.1
Accept: text/plain
Authorization: Basic YWRtaW5pc3RyYXRvcjpDbGlwcGVyMQ==
```

Sample reply

```
HTTP Status code: OK
Password: YFla9Rger
```

Post Random Password

Posts a random password

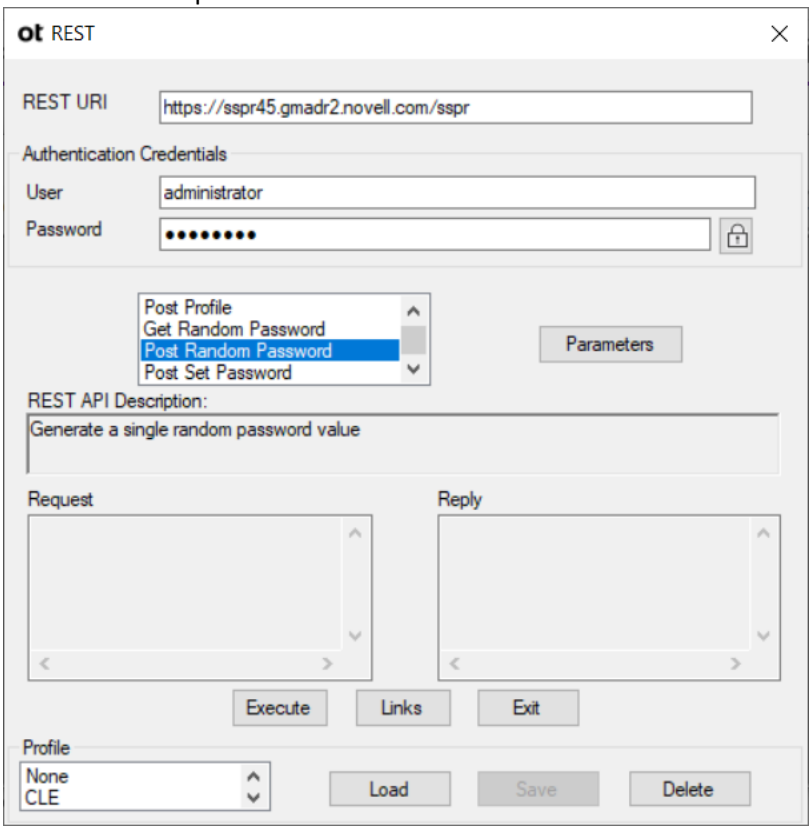


Figure 140 - Post Random Password

Parameters

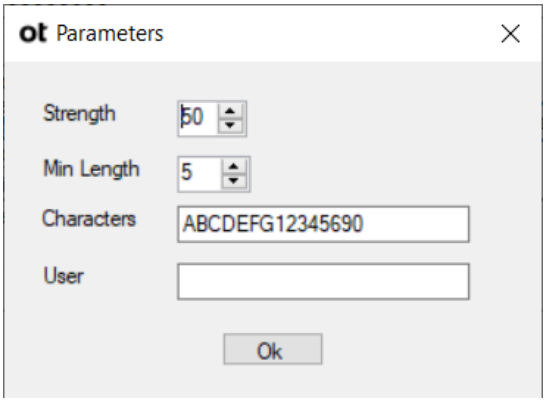


Figure 141 - Post Random Password Parameters

- Strength should be set to the desired strength/complexity of the generated password. (default is 50)
- Min Length is the minimum length of the generated password. (default 5)
- User is the optional user object.

If successful a random password will be returned that matches the defined criteria.

Sample request

```
Post https://sspr.novell.com:8443/sspr/public/rest/randompassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Authorization: Basic YWRtaW5pc3RyYXRvcjpDbGlwcGVyMQ==
{
"strength":"50",
"minLength":"5",
"chars":"ABCDEFG12345690"
}
```

Sample reply

HTTP Status code: OK

```
{"error":false
"errorCode":0
"data":{"password":"4=d8C5"}}
```

Post Set Password

Sets/Changes the password for a user

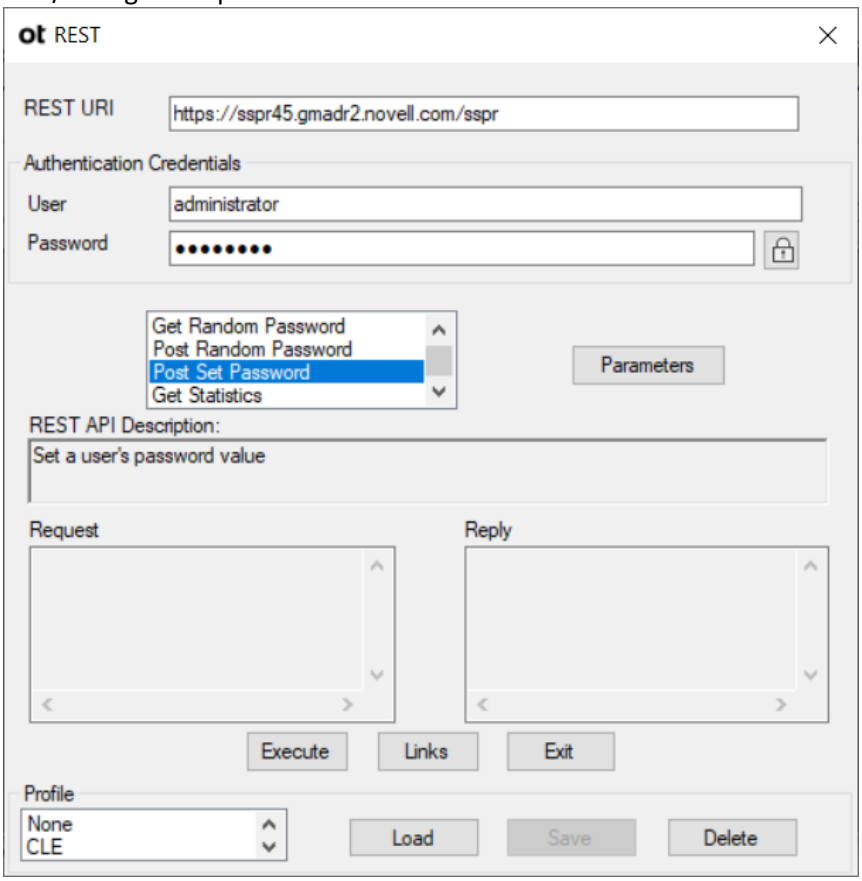


Figure 142 - Post Set Password

This call requires user authentication.

The password that will be changed is the user specified in the Authentication Credentials portion of this window unless the optional user is specified in the parameters window.

Parameters

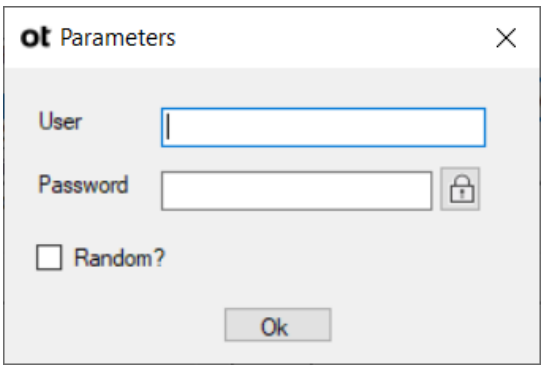


Figure 143 - Post Set Password Parameters

User is the optional user to set the new password on. Note that the authentication user must have rights to change the password on this user. Also, the HelpDesk profile must also be enabled in the SSPR settings.

Password is the new password.

The checkbox Random? is to specify that the SSPR server should generate a random password. Note that if the checkbox Random? is checked then no password value should be defined in the Password field.

If successful, the password will be changed on the specified user or the authentication user if no user was entered into the parameters window. The password is set in the directory and not in SSPR itself. SSPR does not store passwords.

Sample request

```
Post https://sspr.novell.com:8443/sspr/public/rest/setpassword HTTP/1.1
Accept: application/json
Content-Type: application/json
Authorization: Basic YWRtaW5pc3RyYXRvcjpDbGlwcGVyMQ==
{
"password":"TestPassword123"
}
```

Sample reply

HTTP Status code: OK

```
{"error":true
"errorCode":4034
"errorMessage":"New password is using a value that is not allowed"}
```

Get Statistics

Gets the current SSPR statistics

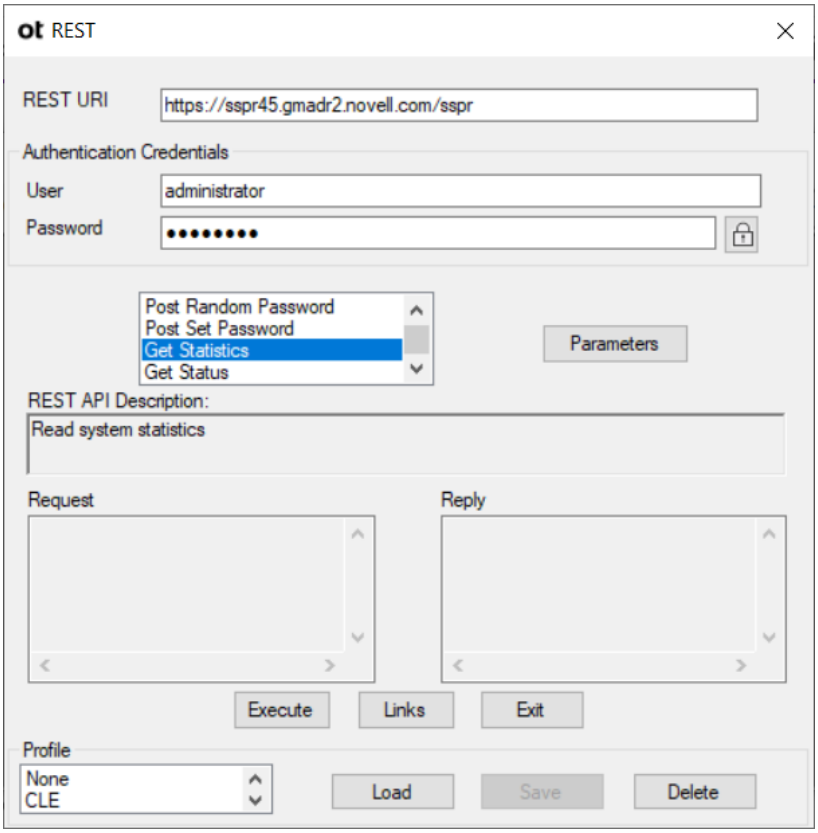


Figure 144 - Get Statistics

User authentication is not required for this API.
Note that the SSPR server setting “Enable Public Health and Statistics Web Service” must be enabled.

Parameters

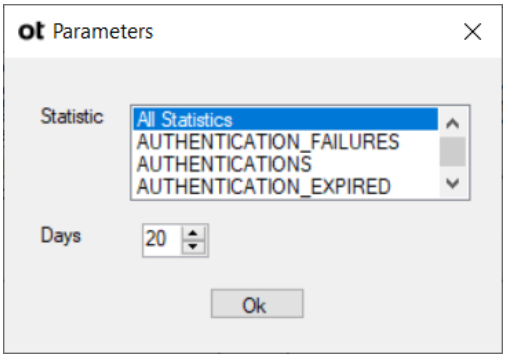


Figure 145 - Get Statistics Parameters

The table “Statistics” allows the selection of “All Statistics” (default) or a specific statistic.
Days indicates the number of days to include in the statistics.

Sample request

GET https://sspr.novell.com:8443/sspr/public/rest/statistics?days=20 HTTP/1.1
Accept: application/json
Authorization: Basic YWRtaW5pc3RyYXRvcjpDbGlwcGVyMQ==

Sample reply

HTTP Status code: OK

Server Response:
{"error":false
"errorCode":0
"data":{"EPS":{"AUTHENTICATION_DAY":"0.001"
"AUTHENTICATION_HOUR":"0.001"
"AUTHENTICATION_MINUTE":"0.001"
"DB_READS_DAY":"0.000"
"DB_READS_HOUR":"0.000"
"DB_READS_MINUTE":"0.000"
"DB_WRITES_DAY":"0.000"
"DB_WRITES_HOUR":"0.000"
"DB_WRITES_MINUTE":"0.000"
"INTRUDER_ATTEMPTS_DAY":"0.000"
"INTRUDER_ATTEMPTS_HOUR":"0.000"
"INTRUDER_ATTEMPTS_MINUTE":"0.000"
"PASSWORD_CHANGES_DAY":"0.000"
"PASSWORD_CHANGES_HOUR":"0.000"
"PASSWORD_CHANGES_MINUTE":"0.000"
"PWMDB_READS_DAY":"0.014"
"PWMDB_READS_HOUR":"0.132"
"PWMDB_READS_MINUTE":"0.144"
"PWMDB_WRITES_DAY":"0.059"
"PWMDB_WRITES_HOUR":"0.485"
"PWMDB_WRITES_MINUTE":"0.346"}
"keyData":{"ActivatedUsers":"0"
"AuthenticationFailures":"0"
"Authentications":"7"
"Authentications_Expired":"0"
"Authentications_ExpiredWarning":"0"
"Authentications_PreExpired":"0"
"AvgAuthenticationTime":"421"
"AvgLdapSearchTime":"101"
"AvgPasswordStrength":"0"
"AvgPasswordSyncTime":"0"
"CaptchaFailures":"0"
"CaptchaPresentations":"0"
"CaptchaSuccessess":"0"

Get Status

Get the status of a user

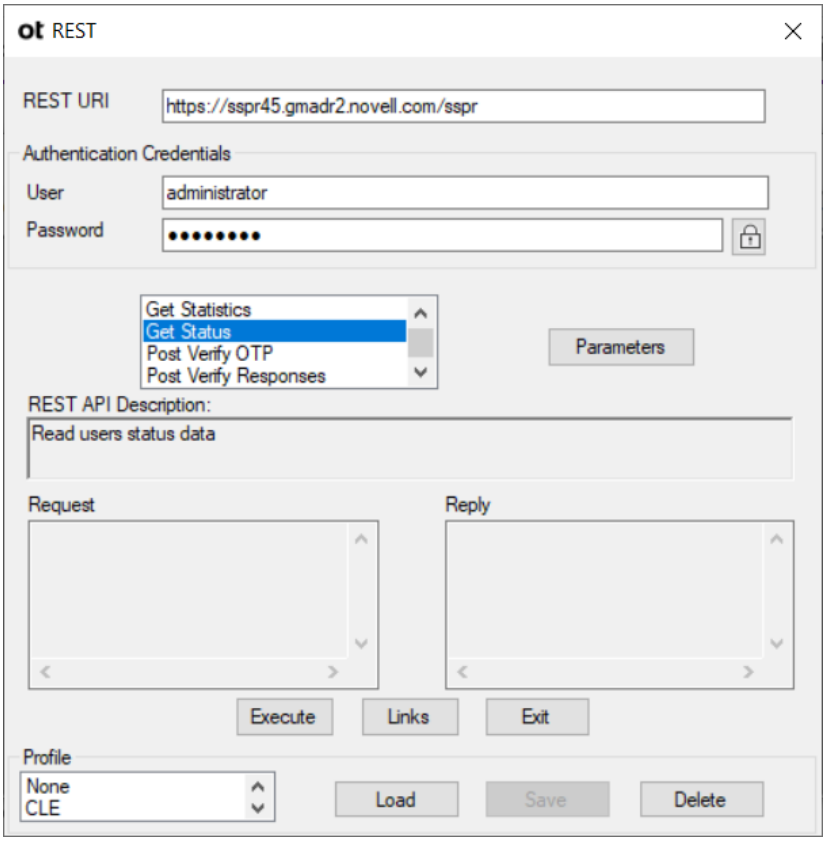


Figure 146 - Get Status

Parameters

The only optional parameter is User. Specify this value if you want to report the Status of a user other than the authentication user.

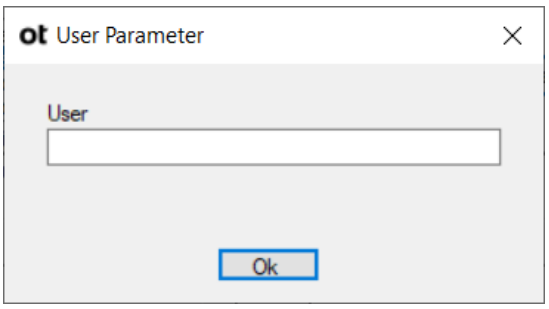


Figure 147 - Get Status Parameters

Sample request

GET https://sspr.gmadr2.novell.com:8443/sspr/public/rest/status HTTP/1.1
Accept: application/json
Authorization: Basic YWRtaW5pc3RyYXRvcjpDbGlwcGVyMQ==

Sample reply

HTTP Status code: OK

Server Response:
{"error":false
"errorCode":0
"data":{"userDN":"CN=Administrator
CN=Users
DC=gmadr2
DC=novell
DC=com"
"ldapProfile":"default"
"userID":"Administrator"
"userEmailAddress":"testuser@gmail.com"
"passwordExpirationTime":"2015-08-28T18:18:53Z"
"passwordLastModifiedTime":"2015-07-17T18:18:53Z"
"requiresNewPassword":false
"requiresResponseConfig":false
"requiresUpdateProfile":false
"requiresInteraction":false
"passwordStatus":{"expired":false
"preExpired":false
"violatesPolicy":false
"warnPeriod":false}
"passwordPolicy":{"DisallowCurrent":"true"
"MinimumNumeric":"0"
"AllowNumeric":"true"
"MaximumSpecial":"0"
"AllowLastCharSpecial":"true"
"CharGroupsValues":".*[0-9]\n.*[^A-Za-z0-9]\n.*[A-Z]\n.*[a-z]"
"MinimumLength":"5"
"EnforceAtLogin":"false"
"AllowFirstCharNumeric":"true"
"MaximumUpperCase":"0"
"MinimumLowerCase":"0"
"UniqueRequired":"false"
"AllowAdminChange":"true"
"PolicyEnabled":"true"
"ADComplexityMaxViolations":"2"
"MaximumLength":"64"
"DisallowedValues":"password\ntest"

Post Verify OTP

Validate supplied one time password against a user's stored secret.

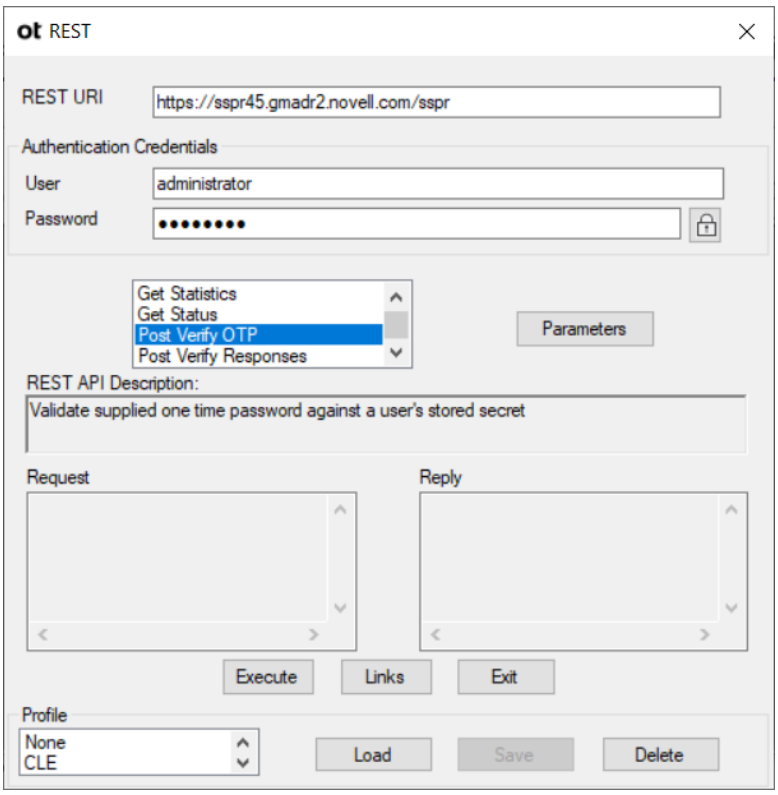


Figure 148 - Post Verify OTP

This REST call is only valid in SSPR version 3.3 or higher.

Parameters

The only optional parameter is User. Specify this value if you want to report the Status of a user other than the authentication user.

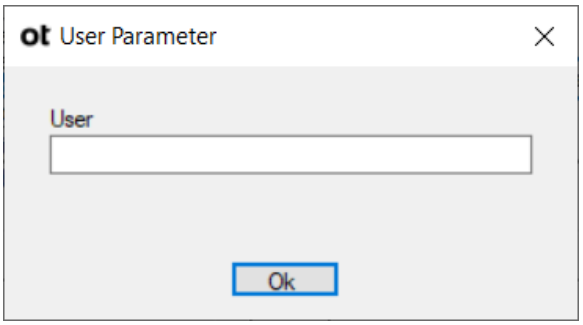


Figure 149 – Post Verify OTP Parameters

Smart Phone Setup

For this call to work correctly, One Time Password (OTP) must be enabled and configured in the SSPR configuration settings. Either force setup and/or force with user option.

Then the user must register their smartphone.

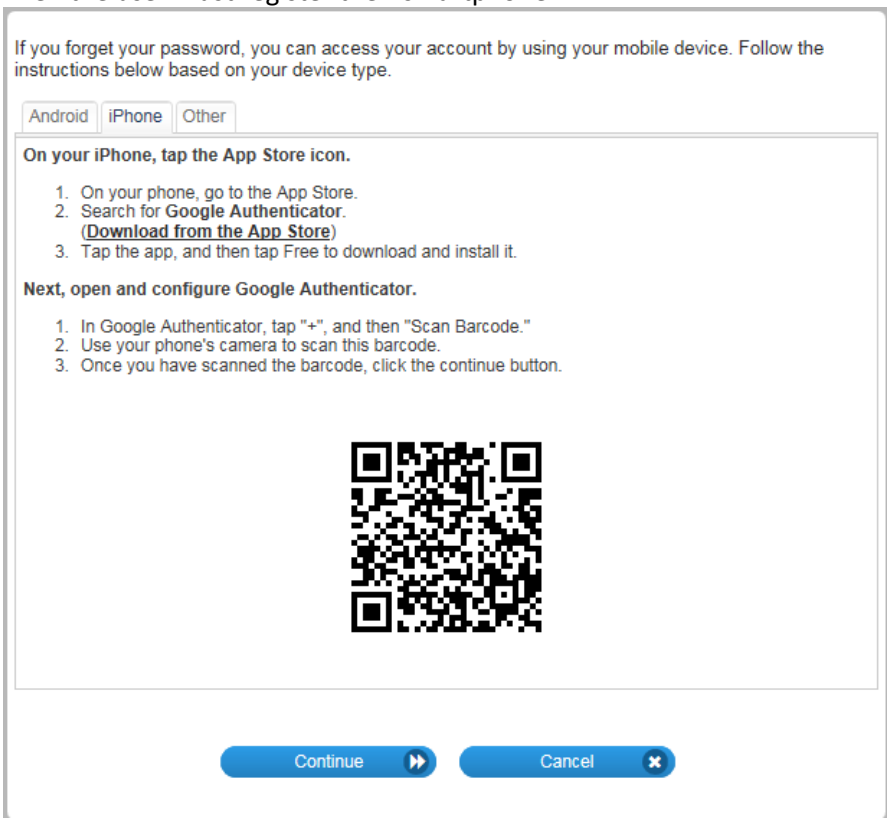


Figure 150 - Setup Mobile App Authentication

Testing

When clicking the Execute button the user will be prompted to enter a token. The token is displayed in the Google Authenticator app.

Sample request

```
Post http://sspr.novell.com:8080/sspr33build96/public/rest/verifyotp HTTP/1.1
Accept: application/json
Content-Type: application/json
Authorization: Basic YWRtaW5pc3RyYXRvcjpDbGlwcGVyMQ==
{"token":564560}
```

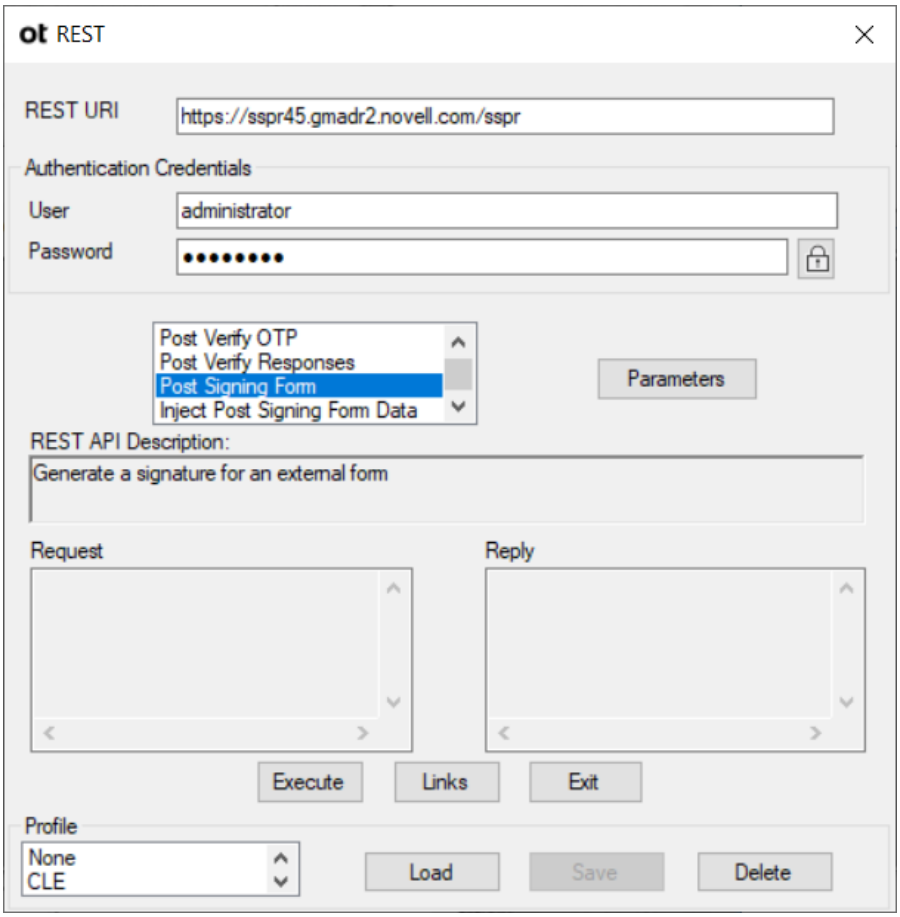
Sample reply

HTTP Status code: OK


```
{"error":false
"errorCode":0
"successMessage":"The operation has been successfully completed."
"data":true}
```

Post Signing Form

This REST call is used to generate signed form data for use with the Inject Post Signing Form. Used for automating the new user registration.



Parameters

The parameter for this REST call is a single string value. This string can be a JSON or urlencoded formatted string.

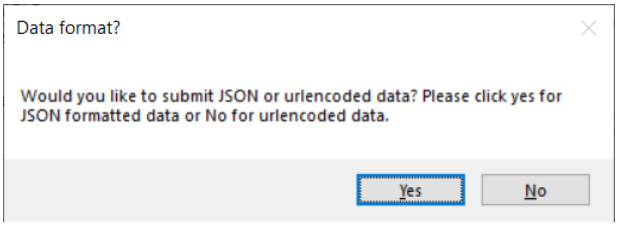
For example…

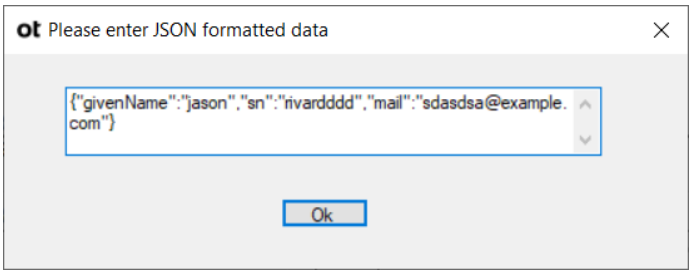
JSON string

{"givenName":"jason","sn":"rivardddd","mail":"sdasdsa@example.com"}

URLencoded string

Source string: {"givenName":"jason"&"sn":"rivardddd"&"mail":"sdasdsa@example.com"}
Converted string:
%7B%22givenName%22%3A%22jason%22%26%22sn%22%3A%22rivardddd%22%26%22mail%22%3A%22sdasdsa%40example.com%22%7D





For more details see this Technical Information Document (TID)
[How to setup and use the Signing Form REST API (microfocus.com)]

Sample request

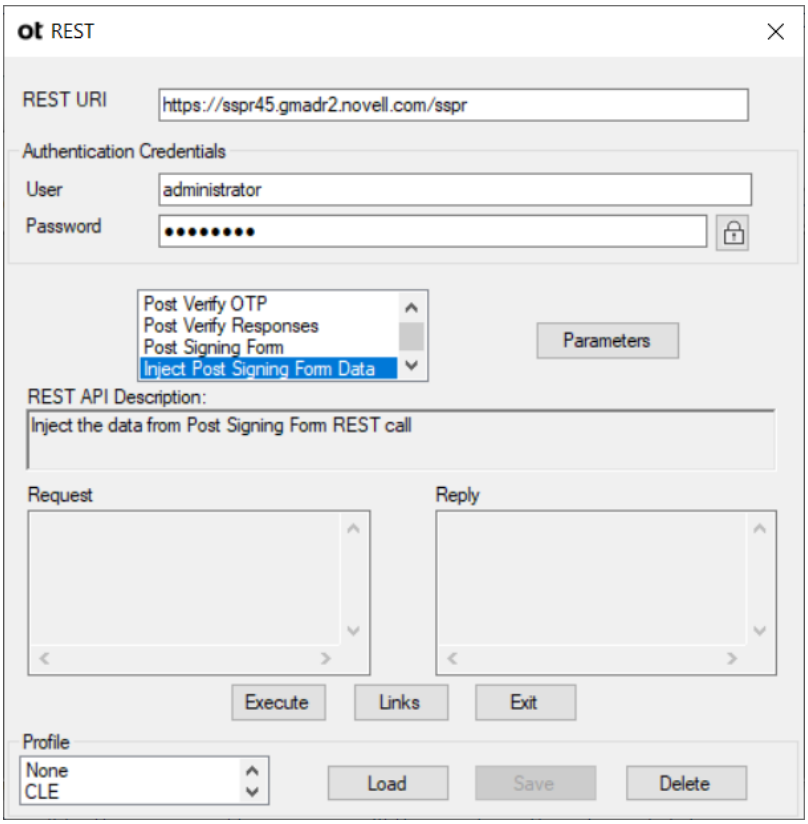
Request:
Post https://sspr.novell.com/sspr/public/rest/signing/form HTTP/1.1
Accept: application/json
Content-Type: application/json
Authorization: Basic YWRtaW5pc3RyYXRvcjpDbGlwcGVyMQ==
{"givenName":"jason","sn":"rivardddd","mail":"sdasdsa@example.com"}

Sample reply

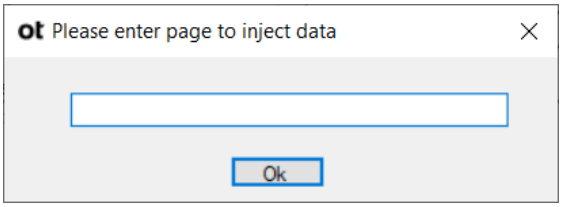
Reply:
HTTP Status code:
{"error":false
"errorCode":0
"data":"H4sIAAAAAAAAAAGcAGP_UFdNLkdDTTEQRoBEsJONk1A9FKnNPsM0au6dGqnw9tvjMREAJVmLEp9b0ccjtXVg3hy2XRlGvihOkZHwS8OIOeq43XARvoxJZnzaWgmWjY_sSoJrCFRHq4Ryn-1FhWCbrdzCyMkTyeIfut1QZLuVxieZ_q2CK5w5jbsoFOj7fhHbaTDOkOWVq-UMguPSc9BS02_blHA8t3hGls28ywx_-5wAAAA="}

Inject Post Signing Form Data

This REST call takes its input from the Post Signing Form REST call. The purpose of this API is to inject the form data needed to automate the new user registration module.



Parameters:



This API accepts a single string parameter. The string is a combination of the server URL and the signed data returned from the Post Signing Form API.

<server URL>/sspr/public/newuser/profile/guest?signedForm=<output from signedformdata rest call>

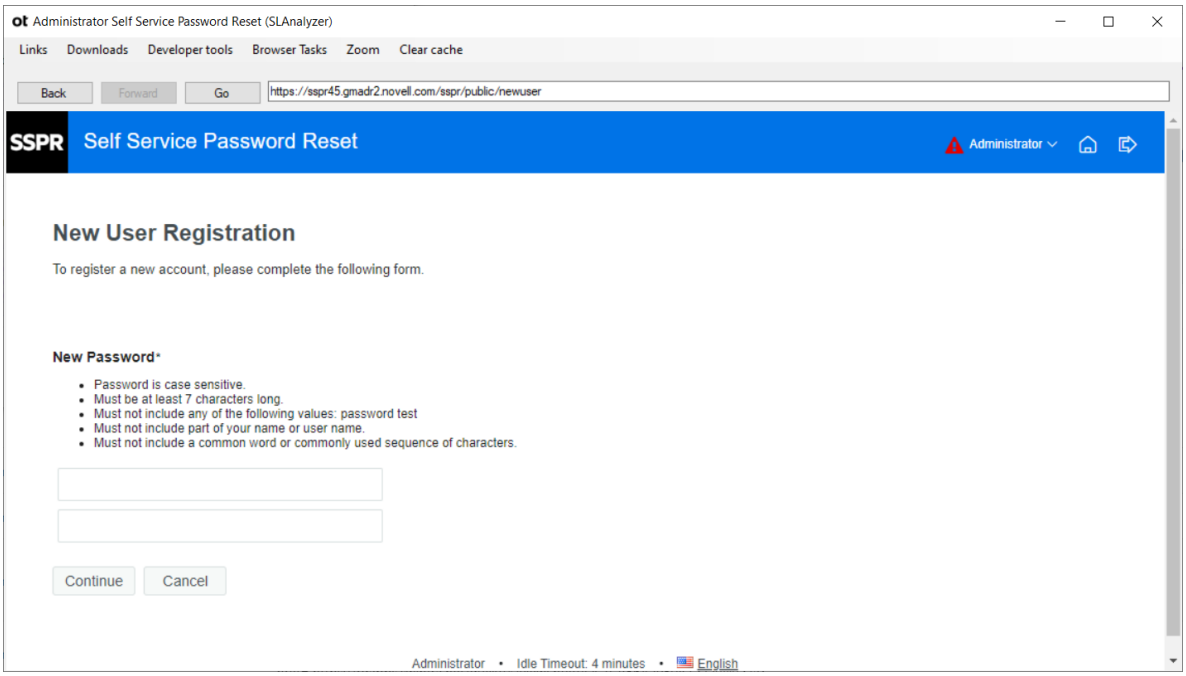
For example:

https://sspr.novell.com/sspr/public/newuser/profile/guest?signedForm=
H4sIAAAAAAAAAAGcAGP_UFdNLkdDTTEQRoBEsJONk1A9FKnNPsM0au6dGqnw9tvjMREAJVmLEp9b0ccjtXVg3hy2XRlGvihOkZHwS8OIOeq43XAR
voxJZnzaWgmWjY_sSoJrCFRHq4Ryn-1FhWCbrdzCyMkTyeIfut1QZLuVxieZ_q2CK5w5jbsoFOj7fhHbaTDOkOWVq-
UMguPSc9BS02_blHA8t3hGls28ywx_-5wAAAA=

If SLAnalyzer detects that the input is invalid, it will display the following error message.



If the injection is successful, then the new user should be redirected to the set password page.



For more information, please see this Techinical Information Document (TID)
[How to setup and use the Signing Form REST API (microfocus.com)]

SSPR Quick Links

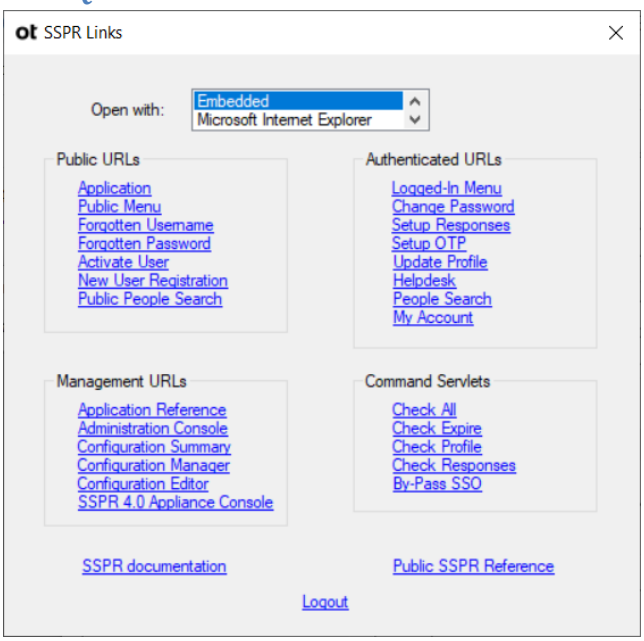


Figure 151 - SSPR Quick Links

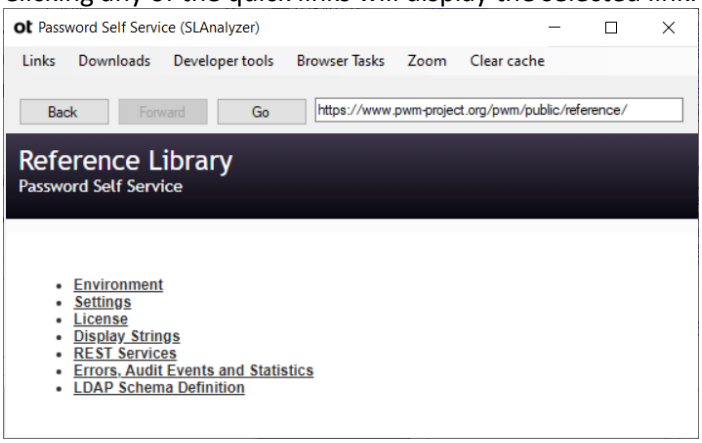
Open with:

This selection box allows the user to specify how the selected link will be processed. By default, SLAnalyzer will attempt to open the selected link in the SLAnalyzer embedded IE window. By selecting a different browser SLAnalyzer will attempt to open the link in the specified browser.
Support browsers:

- Embedded
- Microsoft Internet Explorer
- Microsoft Edge
- Mozilla FireFox
- Google Chrome

Note that SLAnalzyer will attempt to validate that the selected browser is installed on the workstation after clicking a specified link.

Clicking any of the quick links will display the selected link.



SSPR Rights Validator

This feature provides a mechanism to communicate with the underlying LDAP directory configured with SSPR. SSPR requires specific rights to be assigned to the proxy user so that it can perform password changes and other activities on behalf of the user.

Note: Although this feature is designed for validation of SSPR rights, it can be used to validate any object rights to another object. Test user is the destination object and proxy user is the source object. The only limitation here is that SLAnalyzer requires a password for the destination object (test user) if testing against a non-user object, or simply another object that you don't know the password for, then just enter any text in the password field. When the import button is clicked then an error will be reported that SLAnalyzer cannot login as the test user, but the table will be populated with the attribute data and rights found for the source user against the destination user.

The SSPR validator has 4 methods of operation

1. AD (Active Directory) – Using the Microsoft client access AD attribute data.
2. eDirectory – Using the Novell client access eDir attribute data.
3. LDAP – Using LDAP access attribute data over a non-secure connection. Note destination server can be AD, eDir or any other LDAP v3 compliant server.
4. LDAPS – Using LDAP access attribute data over a secure connection. Note destination server can be AD, eDir or any other LDAP v3 compliant server.

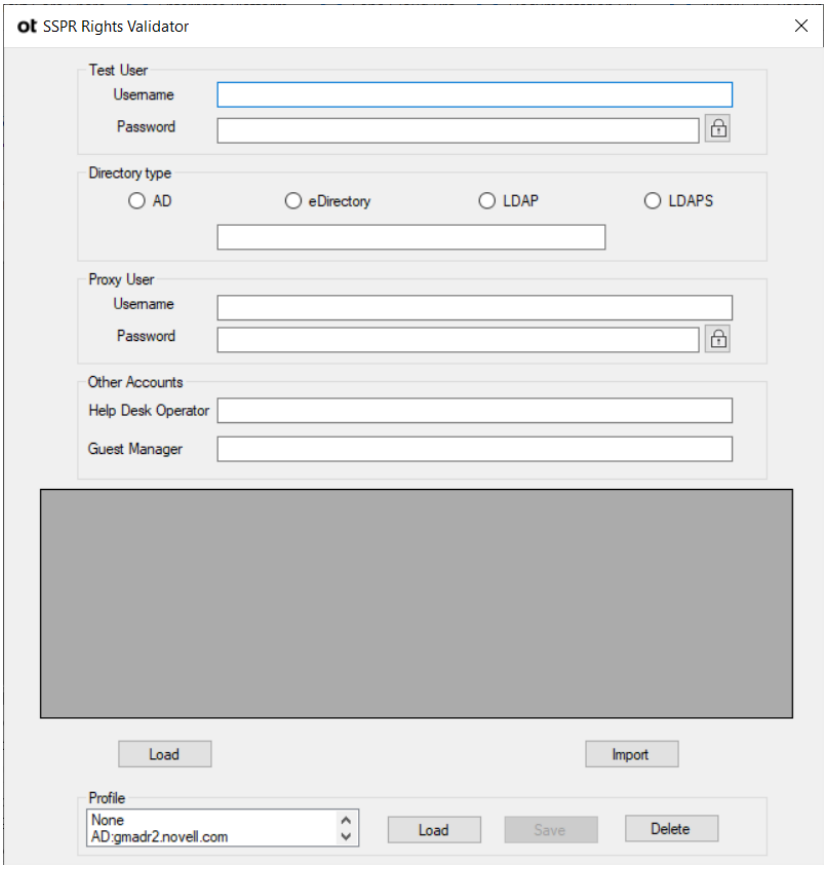


Figure 152 - SSPR Rights Validator

Window components:

The SSPR Rights Validator window has the following fields.

- Test User Credentials – Enter the username and password of the destination (test) user
- Directory type – Select AD, eDirectory, LDAP, or LDAPS
- Proxy User Credentials – Enter the username and password of the source (proxy) user
- Other Accounts – Optionally specify the credentials for help desk or guest manager user objects. When clicking on one of the Other Accounts field the user will be prompted for objects credential data.
- Data Table – This table is loaded by clicking the Load or Import buttons
- Load button – Loads the data table with the information from an sspr permissions file (LDAPPermissionRecommendations.csv). This file can be exported from an SSPR 4.x manager page or can be obtained from a downloaded 4.x support bundle. This file is not available from older versions of SSPR.
- Import button – Queries the configured directory for attribute information and populates the table with a listing of all available attributes and their respective rights.
- Report window – Lists detailed information about actions taken within the SSPR Rights Validator window.
- Profile data – Allows the storing and retrieving of configuration information of the SSPR Rights Validator window. For general information regarding the use of the profile options refer to the profile data section of the SSPR REST client section of this document. Data stored with this option will be saved to: HKEY_CURRENT_USER\Software\MicroFocus\SLAnalyzer\SSPRRights.

Data table:

Line	Column 1	Column 2	Column 3	Column 4
1	Proxy User ➪ All	CN	read	LDAP ➪ LDAP Directori...
2	Proxy User ➪ All	pwmLastPwdUpdate	write	LDAP ➪ LDAP Directori...
3	Proxy User ➪ All	mail	read	Settings ➪ Email ➪ Email ...
4	Proxy User ➪ All	cn	read	Policies ➪ Password Poli...
5	Proxy User ➪ All	givenName	read	Policies ➪ Password Poli...
6	Proxy User ➪ All	sn	read	Policies ➪ Password Poli...
7	Proxy User ➪ All	pwmEventLog	write	Settings ➪ Auditing ➪ Us...

When the data table is first loaded or imported it is not colorized. As tests are performed the table is colorized to indicate the results of the attribute test.

Yellow – Attribute contains no data or source user is unable to read
Green – Successfully tested Read or Write access
Red – Some type of error condition occurred while attempting to access/test attribute access

Report window:

After clicking the Import or Load buttons the report window is displayed to show detailed information about the rights found on the specified attributes within the table.

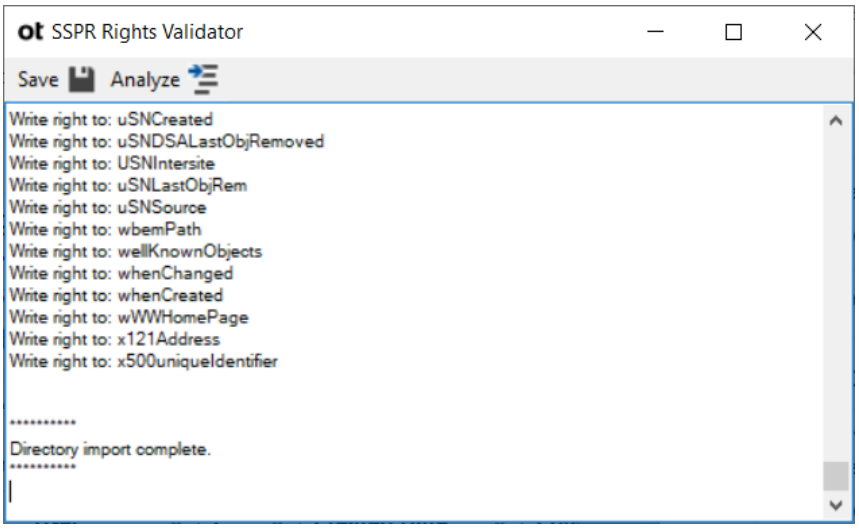


Figure 153 - SSPR Rights Validator report

AD and eDirectory Data table menu:

After a table is loaded then the following context menu is available. Right click anywhere within the data table to display the context menu.

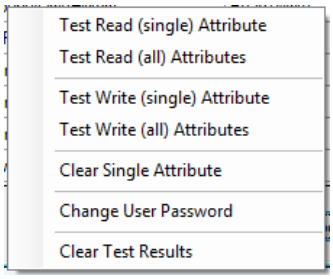


Figure 154- SSPR Rights Validator AD/eDirectory data table menu

LDAP and LDAPS Data table menu:

After a table is loaded then the following context menu is available. Right click anywhere within the data table to display the context menu.

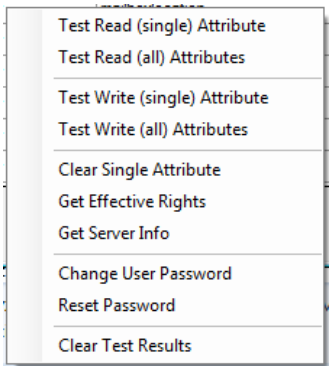


Figure 155 - SSPR Rights Validator LDAP data table menu

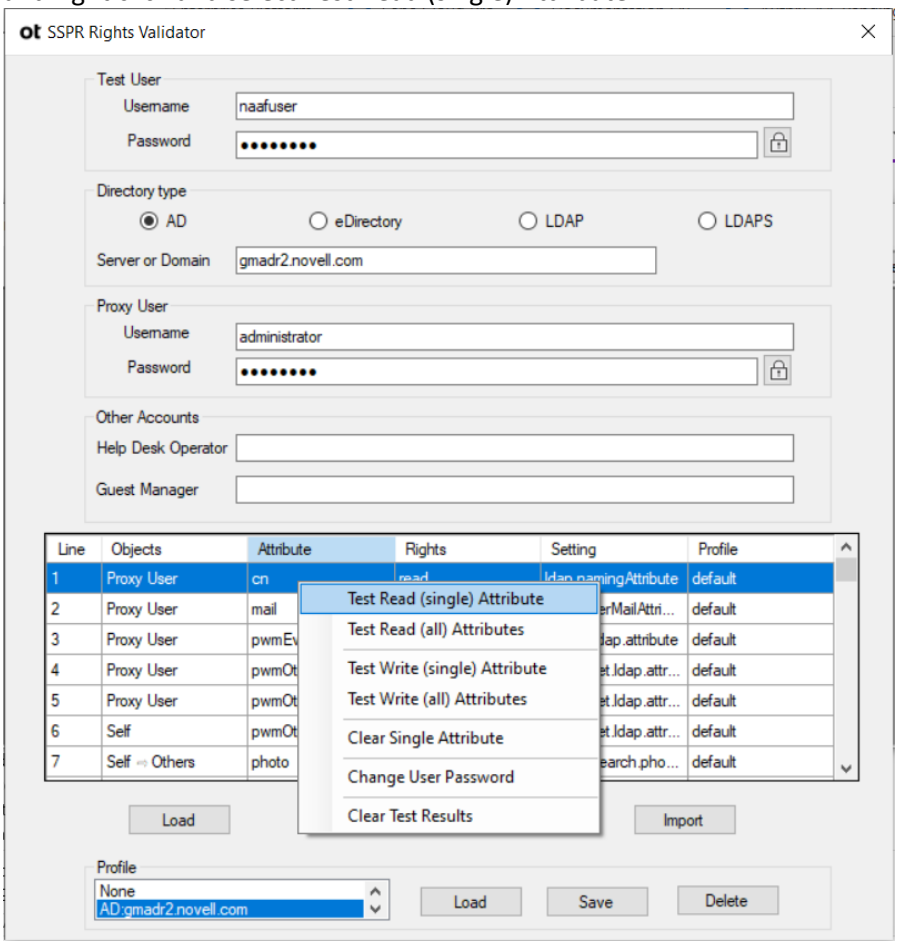
Data table menu items:

- Test Read (single) Attribute – Will attempt to read the selected attribute from the table. (Available in both table menus)
- Test Read (all) Attributes – Will attempt to read all attributes listed in the table with Read rights. (Available in both table menus)
- Test Write (single) Attribute – Will attempt to write to the selected attribute from the table. If the attribute is defined and there is a current value, then SLAnalyzer will read the current value, delete the value, and then attempt to write the original value back to the selected attribute. If the attribute is not already defined, then the user will be prompted if they want to add an entry. If they reply yes, then SLAnalyzer will attempt to add a new value to this attribute on the test user object. Please note that the recommended method of adding an attribute value is with the manufacturers provided management tool. Once the attribute is defined and contains a valid value then SLAnalyzer will use this formatted value to perform this write test. (Available in both table menus)

- Test Write (all) Attributes – Will attempt to write to all attributes that already contain a value. If the attribute is not set, then SLAnalyzer will not attempt to write to the attribute. Only attributes that contain values will be tested. If an attribute that is not set is desired to be tested for write access, first use the Test Write (single) Attribute option to define a new value. When this option is selected, SLAnalyzer will first read the current value, delete the value, and then attempt to write back the original value. Typically, if there is a problem with write access to the attribute then the attempt to delete the value will fail. (Available in both table menus)
- Clear Single Attribute – Will attempt to delete the value of the selected attribute. (Available in both table menus)
- Get Effective Rights – Will attempt to query the LDAP server for effective rights information on the selected attribute. Note that Active Directory servers do not support this LDAP query. Also, this option utilizes the Novell LDAP library. (Available only with eDirectory LDAP servers)
- Get Server Info – Will attempt to read information about the LDAP server. (Available only in the LDAP tables)
- Change User Password – Will attempt to change the test user's password with the selected source user from the table. For example, selecting Proxy User -> All will attempt to change the test users password while logged in as the Proxy User. This option is for the testing of other objects changing the password of the test user. If you select a Self object from the table a message will be displayed that this is not supported. The only valid options are Proxy User, Help Desk, and Guest Manager. (Available in both table menus)
- Reset Password – Will attempt to reset the users' password. For LDAP directories reset password does not use the old password value and requires specific rights for changing another objects password value. (Available only in the LDAP tables)
- Clear Test Results – Clears any test results from the report window and colorization in the table. (Available in both table menus)

Read single attribute value

To test the ability to read the value of an attribute of the test user, select the desired line from the table and right click and select Test Read (single) Attribute.



For this example, SLAnalyzer will login as the proxy user with the credentials provided and then attempt to read the attribute designated in Column 2 (CN).
The report window shows:

******
Read attribute data.
******
Attribute selected: cn
Attribute value: SSPR LDAP

Read all attribute values

To test the ability to read all the currently populated attributes of the test user, right click on the table and select the option Test Read (all) Attributes.

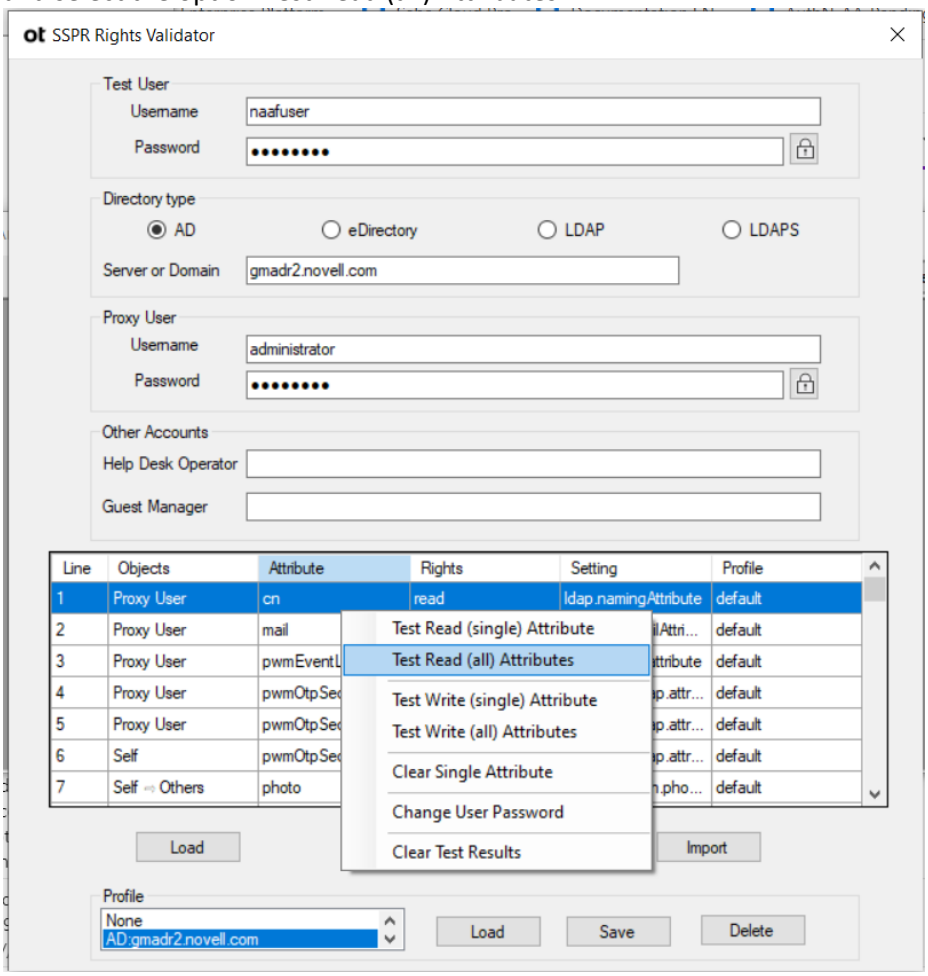


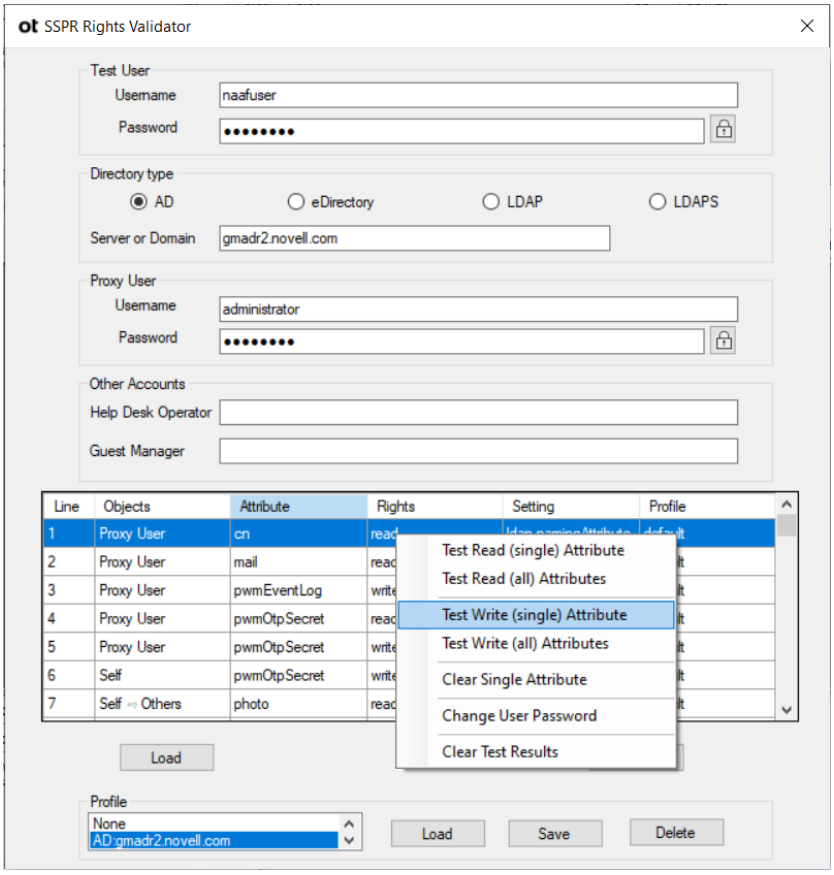
Figure 156 - AD Read all attribute values

Line	Column 1	Column 2	Column 3	Column 4
1	Proxy User ⇨ All	CN	read	LDAP ⇨ LDAP Directori...
2	Proxy User ⇨ All	pwmLastPwdUpdate	write	LDAP ⇨ LDAP Directori...
3	Proxy User ⇨ All	mail	read	Settings ⇨ Email ⇨ Email ...
4	Proxy User ⇨ All	cn	read	Policies ⇨ Password Poli...
5	Proxy User ⇨ All	givenName	read	Policies ⇨ Password Poli...
6	Proxy User ⇨ All	sn	read	Policies ⇨ Password Poli...
7	Proxy User ⇨ All	pwmEventLog	write	Settings ⇨ Auditing ⇨ Us...

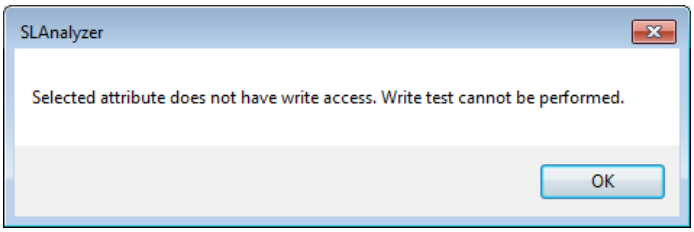
******
Read All Active Directory attributes.
******
Attribute selected: cn
Attribute selected: givenname
Attribute selected: samaccountname

Write single attribute value:

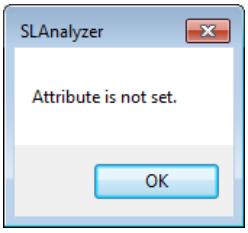
To test the ability to write a value of an attribute of the test user, select the desired line from the table and right click and select Test Write (single) Attribute.



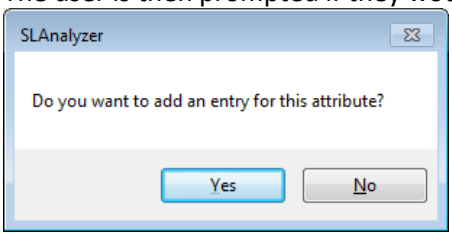
This option first checks the value of Column 3 to see the rights listed. If the rights are not Write then an error message is displayed to the user.



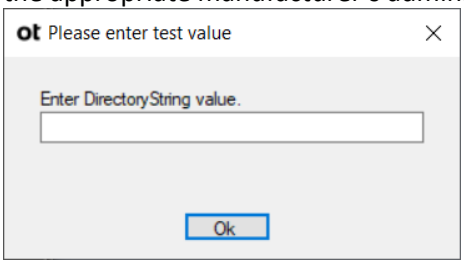
When Column 3 includes the right read then SLAnalyzer will first attempt to read the current value of the attribute selected. If the attribute contains no value then SLAnalyzer will return a message.



The user is then prompted if they would like to add a new value.



If the user selects “No” then the process is aborted. If the user selects “Yes” then SLAnalyzer prompts the user for the value. SLAnalyzer does not always attempt to format the value properly for the attribute type. For example, if the value of the attribute is expected to be a number but the user enters a word then the new value addition will fail. It is recommended that populating attribute values be done with the appropriate manufacturer’s administration tool.



If the user enters no value, then the process is aborted. If the user enters some value, then the data entered is submitted to the directory. The directory will validate the data and either accept or deny the value. SLAnalyzer will display the return status and colorize the table item accordingly.

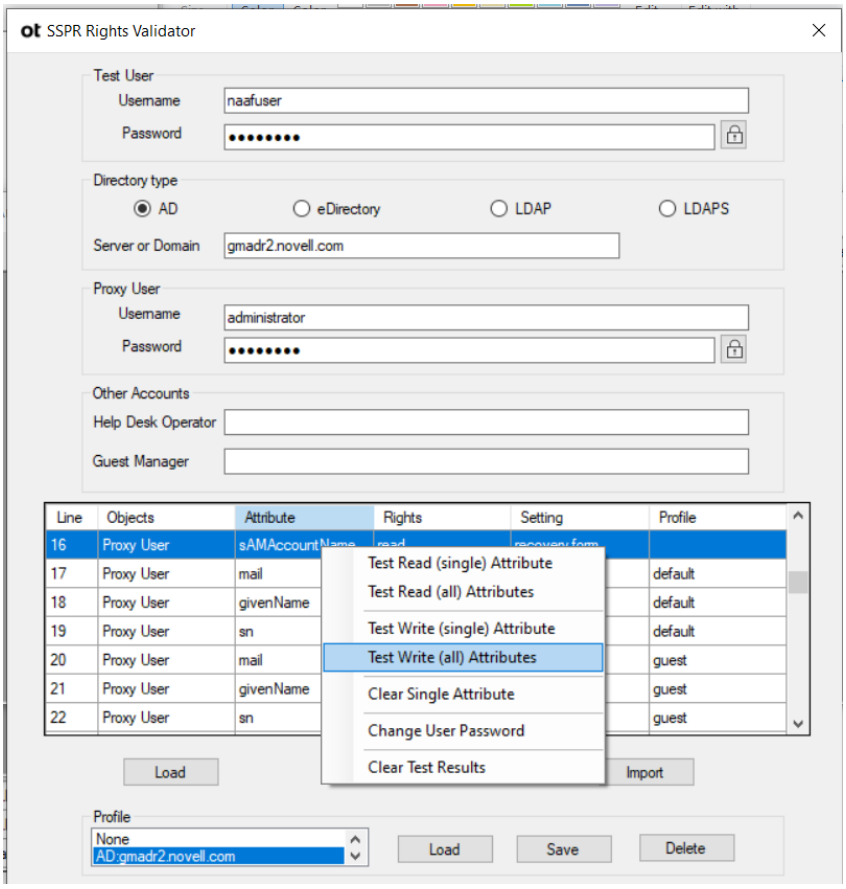
The report window displays the results of the operation.

******
Write attribute data.
******
Successfully wrote to attribute: mail

A subsequent read shows:
******
Read attribute data.
******
Attribute selected: mail
Attribute value: sspr\ldap@novell.com

Write all attributes:

To test the ability to write all populated attributes of the test user, right click on the data table and select Test Write (all) Attributes.



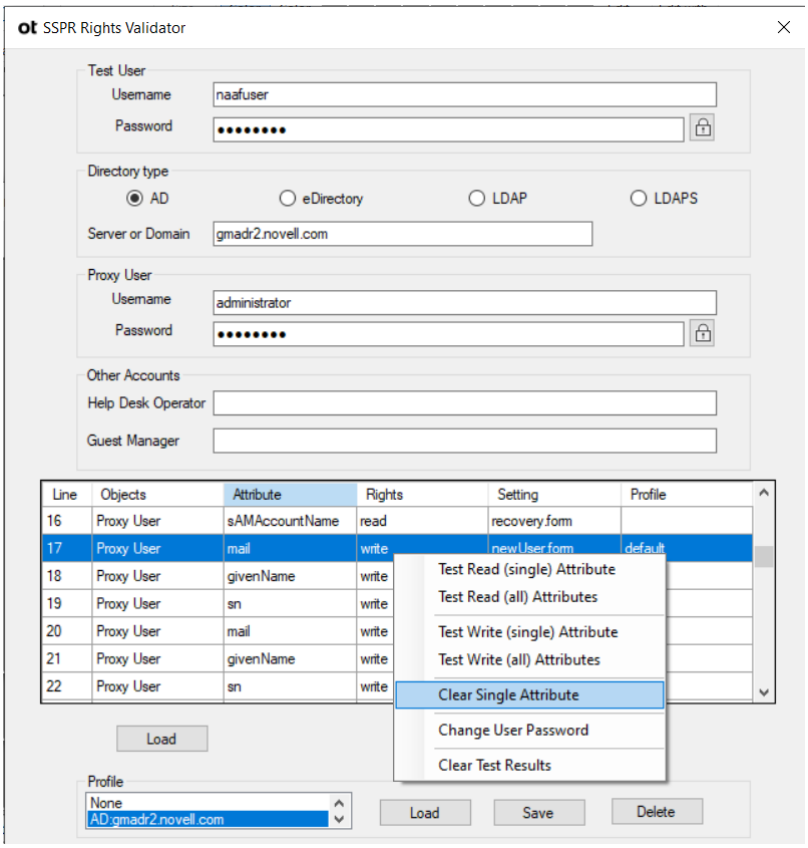
This option will only test the ability to write to attributes that already contain a value and are marked with the Write right in Column 3 of the data table. The following process occurs.

1. Check column 3 for write right
    a. If write access listed then continue
    b. If write access is not listed then skip attribute
2. Connect to server as Source user listed in Column 1
3. Read attribute value listed in Column 2 from test user
    a. If attribute contains value then continue
    b. If attribute doesn't contain a value then skip attribute
4. Delete attribute value
5. Write original value read in step 3 back to attribute of test user
6. Return to step 1 and continue with next attribute from data table

If an attribute is skipped, then it will be colorized as Yellow
If an error is encountered, then the item will be colorized as Red
If successful read/del/write then the item will be colorized as Green

Clear single attribute:

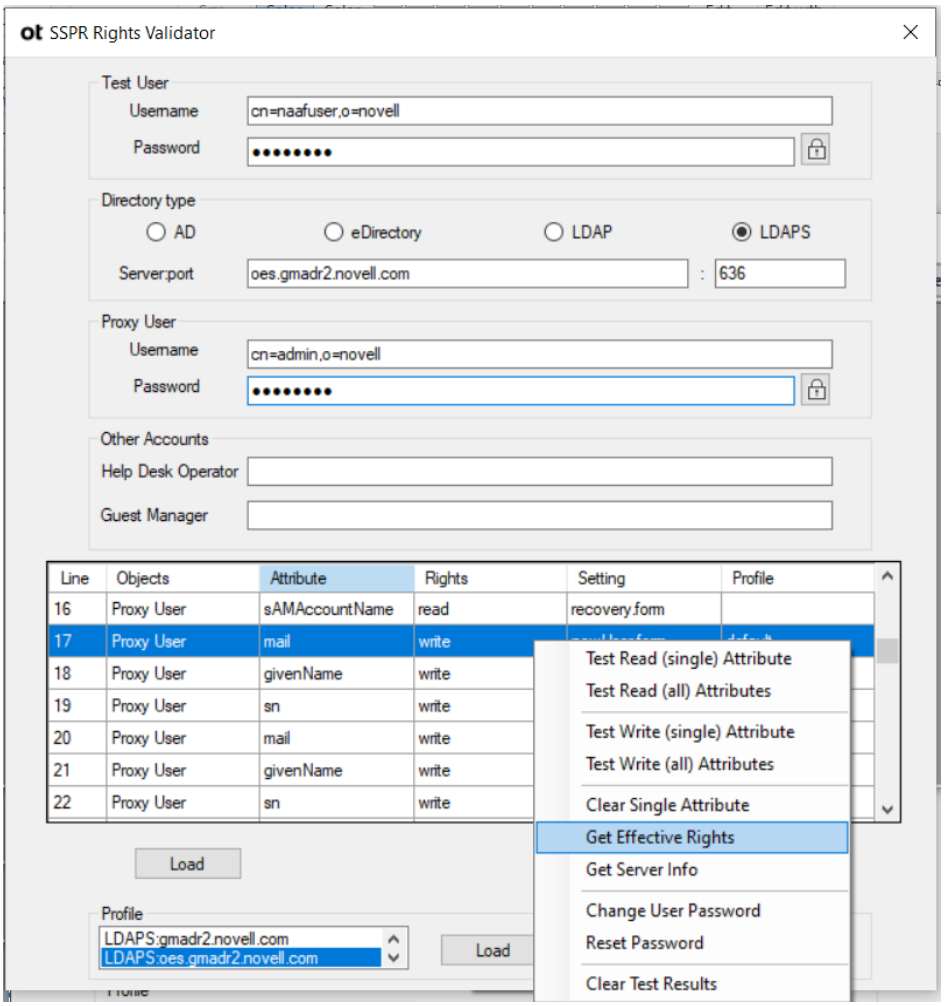
To test the ability to delete an attributes value on the test user, select an item from the data table and then right click and select Clear Single Attribute.



If successful, the table entry colorization will be removed. If there is an error, then the table will remain unchanged, and the report window will display the error message.

Get Effective Rights:

This option is only valid for eDirectory servers. This option is not supported by Microsoft Active Directory servers.



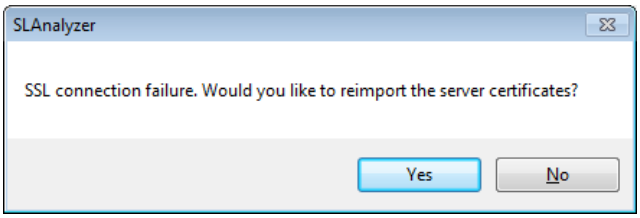
After successfully completing the Get Effective Rights call the report window will display the results of the test.

Successfully bound to server as User: cn=ssprproxyuser,o=novell
Get Effective Rights for: givenName

CompareAttributes: true
ReadAttributes: true
Write/Add/DeleteAttributes: false
Add/DeleteSelf: false
Supervisor: false

SSL Connection Failure

The Novell LDAP library uses the mono connection libraries to connect to the LDAP server. Mono has its own certificate database for secure connections. If an SSL/TLS encryption failure is encountered, then the user will be prompted to import the server certificates.



If the user clicks “Yes” then SLAnalyzer will run the mono certmgr utility and import the server certificates for the SSL/TLS connection. If the user clicks “No” then no action will be taken, and the process is aborted.

The SLAnalyzer report window will display the certificate import information.

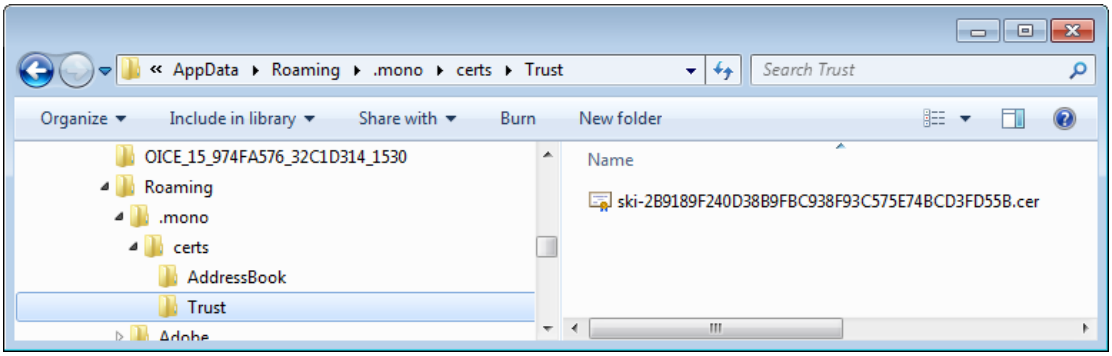
```
########################
Import certificate information
########################
Mono Certificate Manager - version 4.6.2.0
Manage X.509 certificates and CRL from stores.
Copyright 2002, 2003 Motus Technologies. Copyright 2004-2008 Novell. BSD licensed.

Self-signed X.509 Certificate v3
  Issued from: OU=Organizational CA, O=OESTREE
  Issued to:   OU=Organizational CA, O=OESTREE
  Valid from:  9/29/2014 3:01:59 PM
  Valid until: 9/28/2024 3:01:59 PM
Import this certificate into the Trust store ?

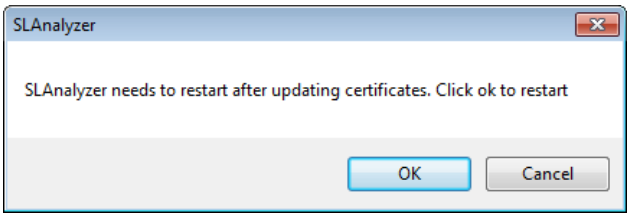
X.509 Certificate v3
  Issued from: OU=Organizational CA, O=OESTREE
  Issued to:   O=OESTREE, CN=linux-61w4.site
  Valid from:  2/14/2017 3:28:19 PM
  Valid until: 2/14/2019 3:28:19 PM
Import this certificate into the AddressBook store ?

2 certificates added to the stores.
```

The mono certificate databases are in the users roaming profile folder.

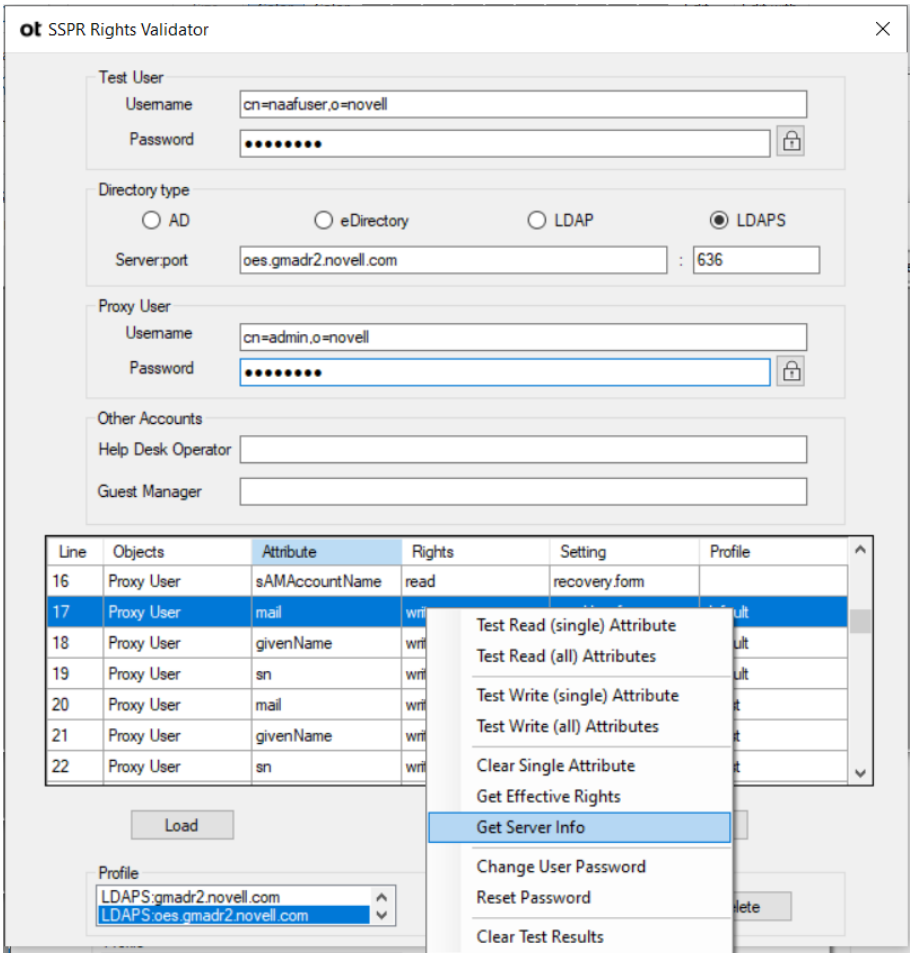


After importing new certificates SLAnalyzer needs to be restarted. The user is prompted to restart. If the user chooses cancel, then the current option will still fail until the application is restarted.



Get Server Info:

Queries the LDAP server for rootDSE information about the server.



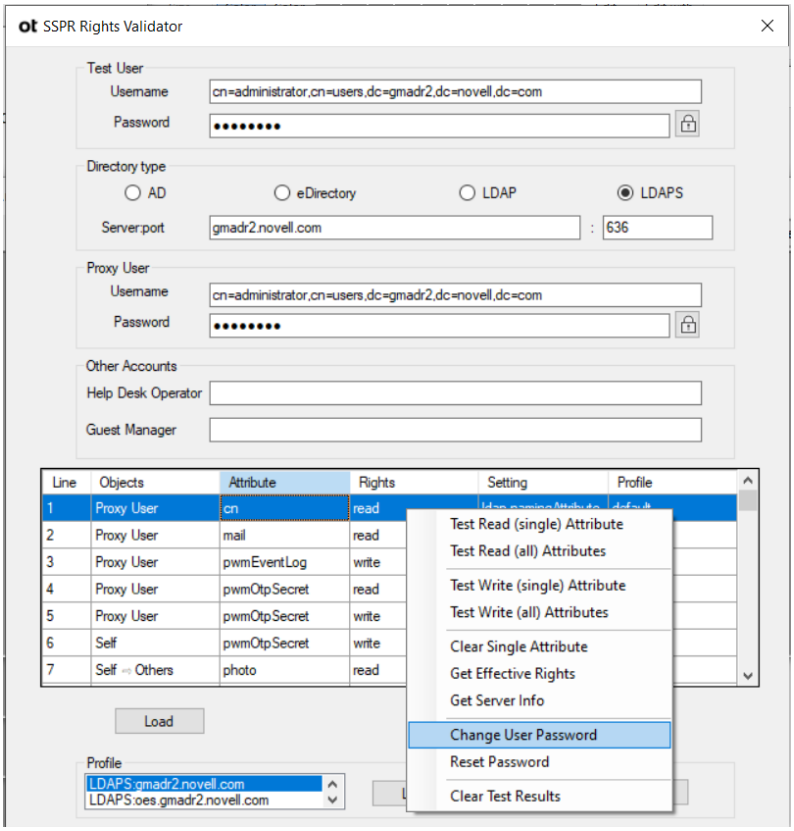
The LDAP server will return information about supported features and controls.

See sample reports within the appendix.

- Active Directory
- eDirectory

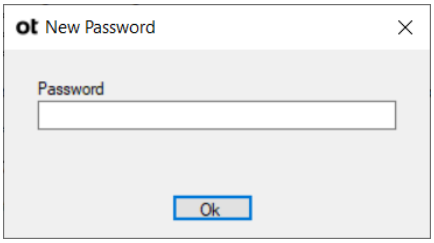
Change User Password:

This option allows the testing of a user to change the password or another user.



In the data table select a line for the source user (listed in Column 1) that you would like to test the ability to change the test user's password. Note that this option is only valid for the objects Proxy User, Help Desk Operator, and Guest Manager.

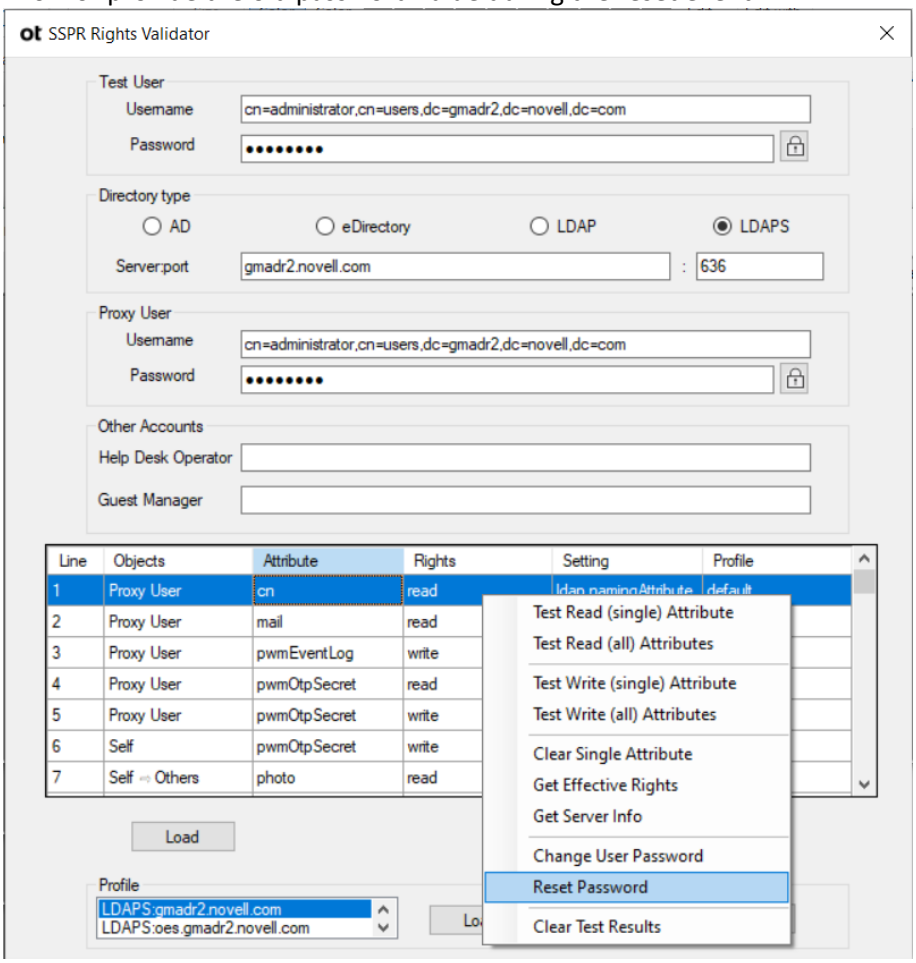
The user is prompted for a new password value.



Entering no value or closing without any value will cause the change password to abort.

Reset Password:

Reset password is different than change password because it requires specific rights since it does not know or provide the old password value during the reset event.



AD Validator (using Microsoft client)

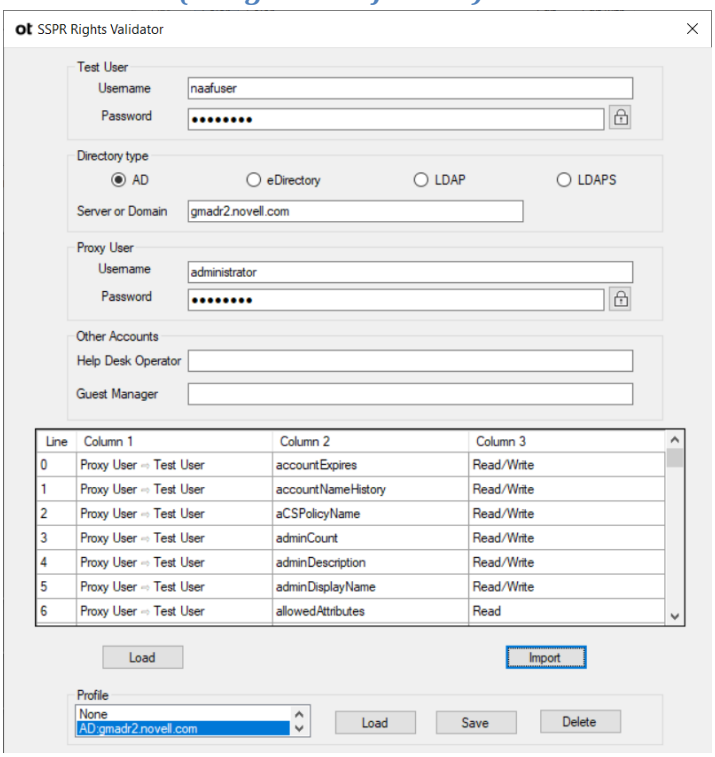


Figure 157 - SSPR AD Rights Validator

- Enter any AD user as the test user to validate against.
- Select AD as the directory type.
- Specify the DNS or IP address of the domain server.
- Enter the SSPR proxy user to check rights to the defined test user.
- Optionally, you can enter a Help Desk Operator and/or a Guest Manager.

Click the load button to load an LDAPPermissionRecommendations.csv file.
Click the import button to import attribute information from the domain server.

The user object names are located via the global catalog for the specified Domain. Syntax for user object should be just the user's login name. For example, "administrator". This is defined as a user attribute called "sAMAccountName".

Warning: This tool will write to the test users' attributes. Make sure the test user being used here can be recreated if necessary.

eDirectory Validator ***(Using Novell/OES client)***

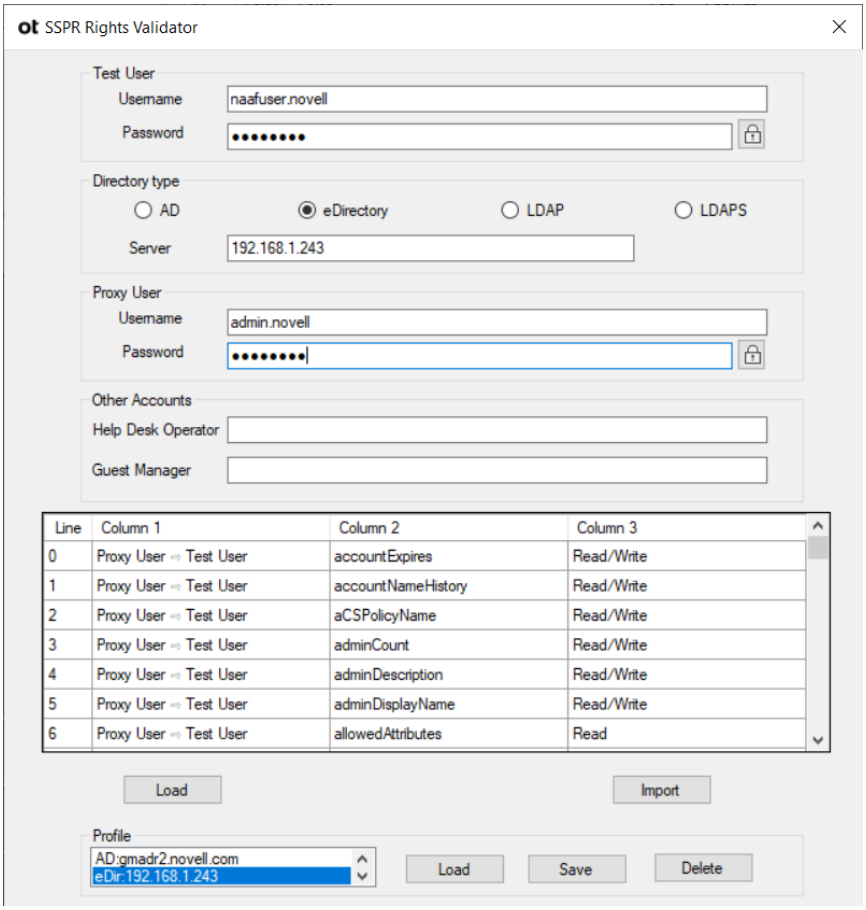


Figure 158 - SSPR eDirectory Rights Validator

- Enter any eDirector user as the test user to validate against.
- Select eDirectory as the directory type.
- Specify the DNS or IP address of the eDirectory server.
- Enter the SSPR proxy user to check rights to the defined test user.
- Optionally, you can enter a Help Desk Operator and/or a Guest Manager.

Click the load button to load an LDAPPermissionRecommendations.csv file.
Click the import button to import attribute information from the domain server.

Syntax for user object should be in the NDS full distinguished name format.
For example: username.context.context.

Warning: This procedure will logout any currently logged in connection. Please make sure you save your data in other applications that might be accessing resouces located on any Novell client connected server.

Warning: This tool will write to the test users' attributes. Make sure the test user being used here can be recreated if necessary.

LDAP/LDAPS validator

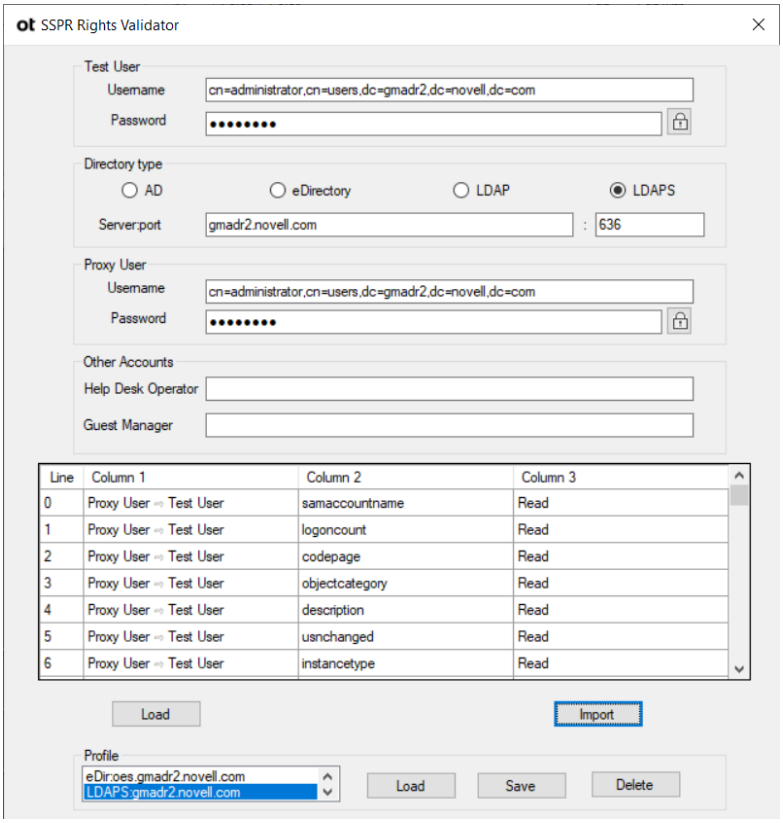


Figure 159 - SSPR LDAP Rights Validator

- Enter any LDAP user as the test user to validate against. Use fully qualified name in LDAP syntax.
- Select LDAP as the directory type.
- Specify the DNS or IP address of the LDAP server
- Specify the TCP port. Typical values (LDAP 389/LDAPS 636)
- Enter the SSPR proxy user to check rights to the defined test user. Use the fully qualified name in LDAP syntax.
- Optionally, you can enter a Help Desk Operator and/or a Guest Manager.

Click the load button to load an LDAPPermissionRecommendations.csv file.
Click the import button to import attribute information from the LDAP server.

The user object names must be specified with the full LDAP naming syntax. (DistinguishedName/DN)
For example:
(AD server) cn=username,cn=users,dc=gmadr2,dc=novell,dc=com
(eDirectory server) cn=username,o=novell

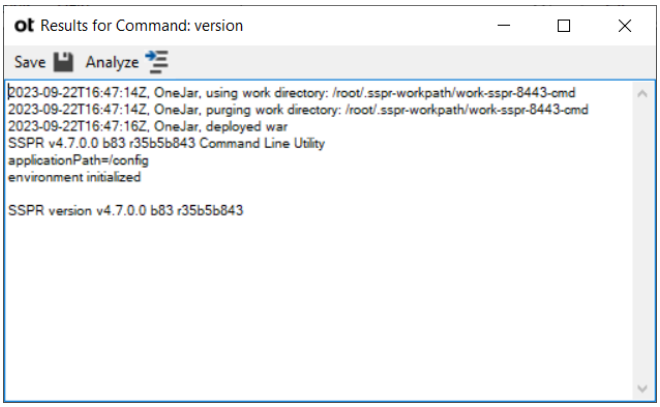
Warning: This tool will write to the test users' attributes. Make sure the test user being used here can be recreated if necessary.

Command

The options under command require SSH access to the server. When selecting one of these options the user will be prompted for their SSH credentils. These options are only valid for SSPR servers deployed as WAR or as an Appliance. After making an SSH connection the the command.sh script will be executed to perform the desired option.

Get App Version

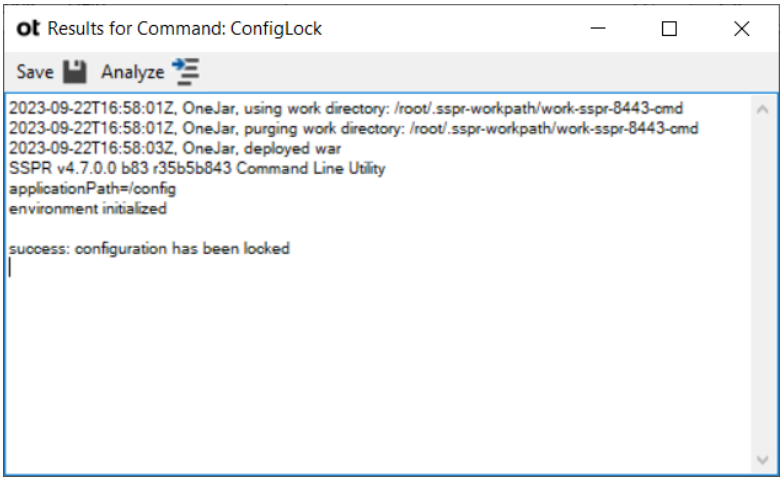
This option will return the version of SSPR running on the selected host.



Clear Local Responses

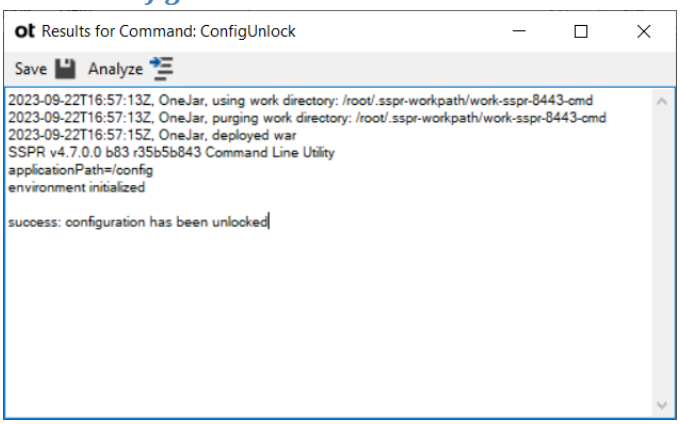
This option will clear all users responses from the database. This will result in users needed to recreate any saved responses. Make sure there is a backup of the server before using this option since all user data will be erased.

Lock Configuration



Please see the administration guide in the online SSPR documentation.
[Configuring Locked and Unlocked Modes - Self Service Password Reset 4.7 Administration Guide (netiq.com)]

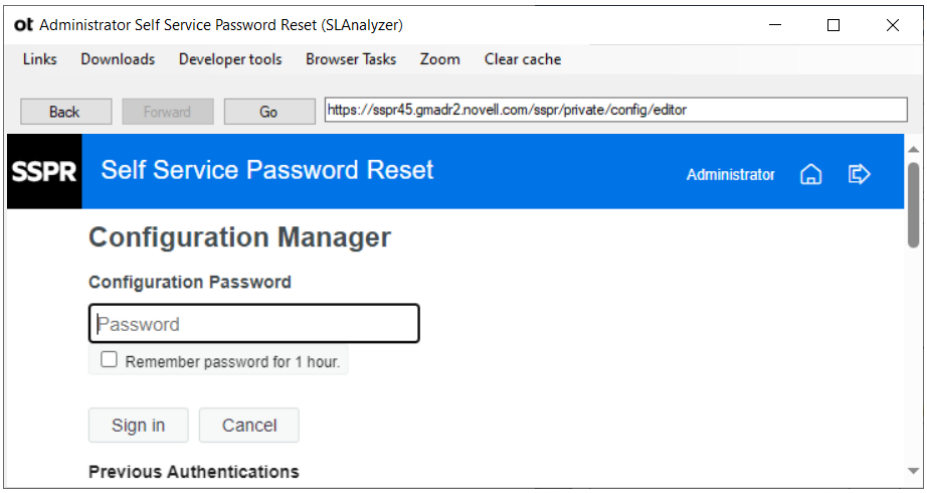
Unlock Configuration



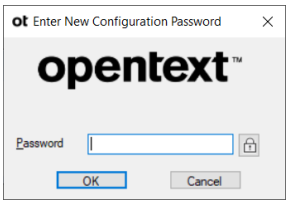
Please see the administration guide in the online SSPR documentation.
[Configuring Locked and Unlocked Modes - Self Service Password Reset 4.7 Administration Guide (netiq.com)]

Set Configuration Password

When attempting to access administrative functions in SSPR, the user is prompted for the configuration password. This option allows a user to reset the configuration password without having to manually modify the configuration file.



When executed the user will be prompted for the new password.



Delete Configuration

This option should be used only in cases where a server needs to be reset to the state of a new server. It will not contain any configuration and when navigating to the server with a browser session the new configuration wizard will be displayed. Make sure a backup of the server configuration file has been taken prior to executing this function. The old configuration is not retained.

After this option completes then please reference the SSPR installation guide in the online documentation for steps using the configuration guide.

Using the Configuration Guide - Self Service Password Reset 4.7 Installation Guide (netiq.com)

Advanced Authentication

The Advanced Authentication menu has several options.

1. REST Client
2. Risk Services
3. Remote Admin
4. Add CA Root Certificate
5. Find PostGres User
6. Gather Server Stats
7. Monitor server performance
8. Replace OSP Certificates
9. Reset Local Admin Pwd
10. OSP / OAuth2
11. Get OpenID Config
12. Get SAML metadata
13. Check AAuth connectivity

REST Client

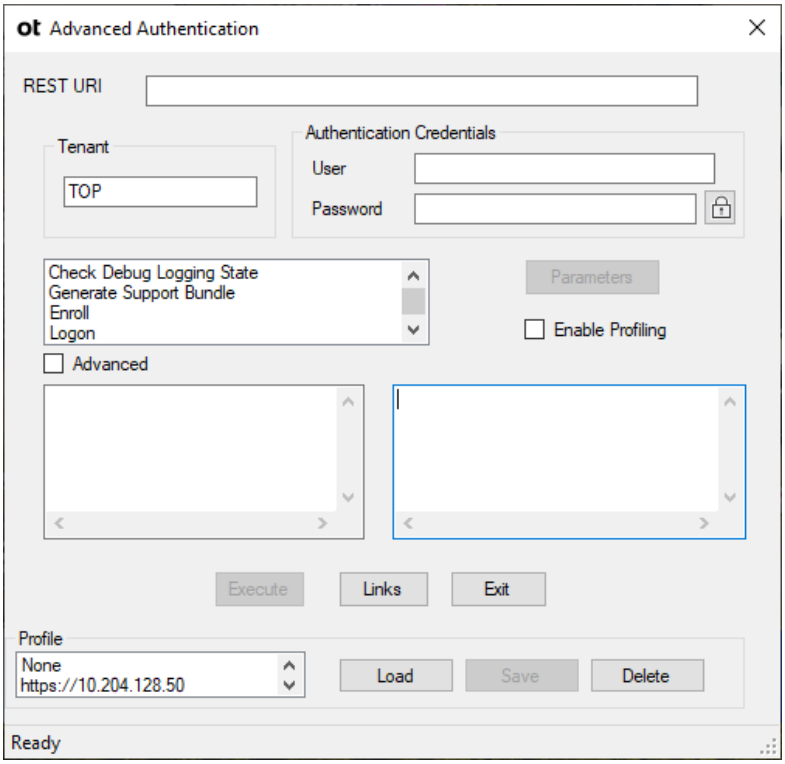


Figure 160 - Advanced Authentication

Note: This feature requires an endpoint session between the workstation and the AAF server. Prior to using this feature, you must enable one of the diagnostic endpoints or create a new endpoint. Click the links button and then click Endpoints, or see section Advanced/Register New Endpoint, Advanced/Read Endpoint Info, Advanced/Update Endpoint Info.

AAF REST Client Window components

The main window for the AAF REST client is composed of several components.

- REST URI
- Tenant
- Authentication Credentials
    - User
    - Password
- REST Calls Selection box
- Parameters button
- Enable Profiling checkbox
- Advanced checkbox
- Request window
- Reply window
- Execute button
- Links button
- Exit button

- Status message
- Profile data

When executing one or more of the items in the REST call window SLAnalyzer will display the Packet data window. This window provides detailed information on the request and reply information.

REST URI

The REST URI is the full URL of the AAF appliance.
For example
https://aaf.mydomain.com

Note that if the AAF Windows client is installed on the workstation then configuration data is read from the config.properties file located at C:\ProgramData\NetIQ\Windows Client.

Tenant

This field defaults to TOP. For customers using a multi-tenant configuration then the desired tenent should be entered to manage that specific tenant. This would include SaaS configurations accessing AAF in the cloud.

Authentication Credentials

The username and password provided in the authentication credentials are encrypted and included in the http header for authentication.

User

Any valid LDAP user located in the AAF repository. You can specify the repository first and then name.
For example: OESTREE\aafuser
If the repository is not specified, then the default repository will be used to authenticate the user.

Password

Password of the LDAP user

REST Call Selection box

Listed in the selection box are the possible REST calls that can be made to the AAF appliance. Each call has its own possible parameters and other requirements. Please refer to the documentation below for each possible REST call.

Initially the REST Call Selection box lists several automated processes. These items will invoke the necessary REST calls to perform the described activity.
For example, the logon process calls:

1. Create Endpoint Session – To create an endpoint session with the appliance
2. Get Authentication Chains – To acquire a list of login methods from the appliance
3. Logon – To initiate the logon process with the user selected chain
4. Logon Do – To complete the logon process with the user selected chain
5. If Logon Do indicated that there are more methods to authenticate to complete the login then issue Logon Next, then repeat steps 3-4 for next method in chain list.

The automated processes are:

- Check Debug Logging State
- Generate Support Bundle
- Enroll
- Logon
- Delete User(s)
- Get Server Status

- Lookup User
- List of Users
- Test Device Manager Plug-in
- Build enrolled methods database
- Manage OTP Tokens
- Show Shared Template Info
- Register Method for User
- Show Override Auto Enrollment
- Manage Radius Clients

Clicking the advanced button allows the selection of all possible REST calls. These calls are not automated so the user must ensure that requirements are made for the REST call before invoking. For example, to execute Read Logon Session, there must first be a Logon Session by executing Logon, Logon Do, Logon Next, etc.
SLAnalyzer will attempt to prompt the user for completion of required information for the selected REST call but please refer to the REST description for details.

- Assign User Template
- Create Endpoint Session
- Create Event
- Create OTP Token
- Create User Template with enroll data
- Create User Template without enroll data
- Delete All Records of OSLogon Data
- Delete Event
- Delete Login Session
- Delete OTP Token
- Delete Password Record Only
- Delete User
- Delete User Template
- Destroy Endpoint
- Destroy Endpoint Session
- Destroy Enroll
- Destroy Logon Process
- Do Enroll
- Do Logon
- Do Method call
- Enroll
- Enroll new TOTP
- Enroll OTP Token
- Generate Cookie Value
- Generate Ticket Value
- Get Authentication Chains
- Get Endpoint Session Info
- Get Event by Event ID
- Get Full Server Status

- Get OTP Token
- Get OTP Tokens with Pagination
- Get Server Status
- Get User Template
- List of Events
- List of Users
- Load Chain Image
- Logon
- Logon by Basic Auth
- Logon Domains Lookup
- Logon Next
- Lookup User
- Modify User Data
- Read All Custom Messages for Category
- Read All Records of OSLogon Data
- Read Available Chains
- Read Categories
- Read Custom Messages for Category and Key
- Read Effective Policies of User
- Read Effective Policies of Endpoint
- Read Endpoint Info
- Read Info about Component of Endpoint Policy
- Read Info about Component of User Policy
- Read Login Session Information
- Register Logon Domains for the Current Tenant
- Register New Endpoint
- Remove Already Enrolled TOTP Template
- Revoke OTP Token
- Search for Endpoint
- Update Endpoint Info
- Update Event
- Update User Template
- Verify Cookie Value

Parameters button

The parameters button will become enabled when the selected REST call has additional parameters that can be passed or used in the request to the server. If there are no optional parameters then this button will be disabled.

Enable Profiling checkbox

By enabling profiling, the server will return performance related information for the REST call being issued to the server. For more information see this link in the AAF documentation: https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/t4byj6vrd1gh.html

Advanced checkbox

By default, the automated Enroll method is listed. This method automates the enrollment process so that the REST calls are made in the correct order. Basically, providing the same functionality as the user web interface. By checking the “Advanced” checkbox, the user can individually test each of the AAF REST calls. Note that some calls require information from other calls before they are functional. For example, you cannot perform a Logon until after you have performed a Get Authentication Chains call.

SLAnalyzer attempts to notify the user of the options needed before the call will be attempted to the AAF appliance.

Request window

The request window will show the syntax of the request being sent to the server.

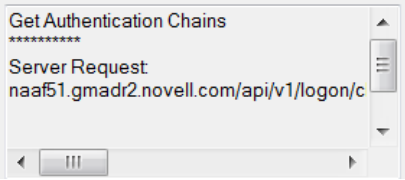


Figure 161 - AAF REST Request window

Reply window

The reply window will show the response received from the appliance.

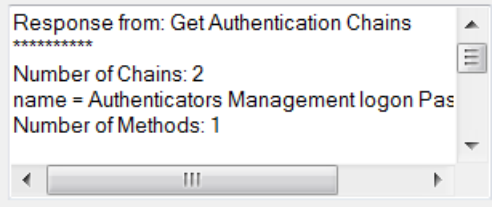


Figure 162 - AAF REST Reply window

Execute button

The execute button will attempt to send the selected REST Call to the specified server. If the connection is encrypted, then a window will popup providing the certificate details.

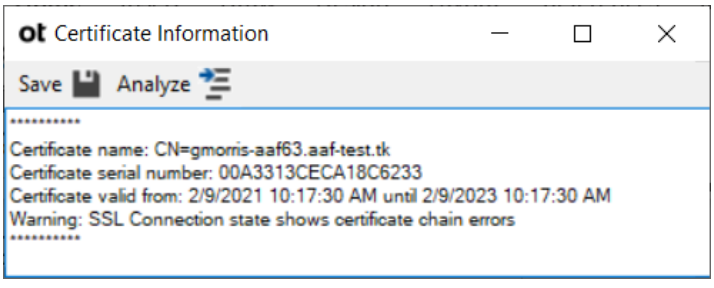


Figure 163 - Certificate details

Links button

The Links button displays a window with a listing of common quick links to the AAF appliance.

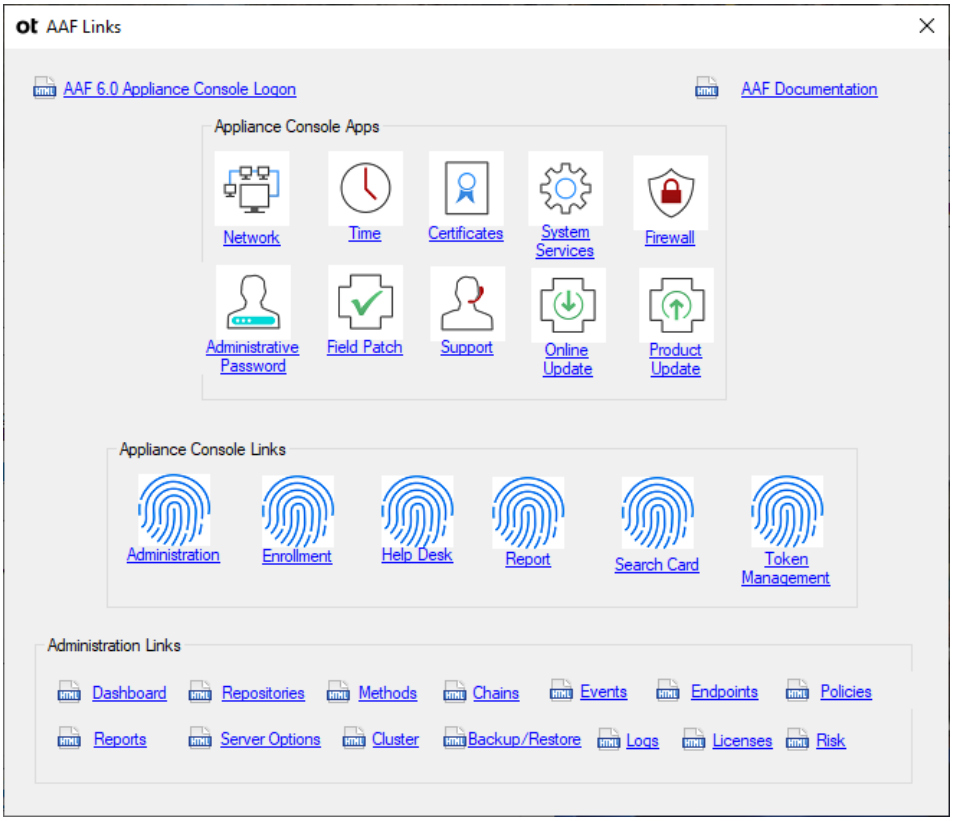


Figure 164 - AAF appliance Quick links

Clicking on one of the displayed links will open the built-in browser window to the selected link.

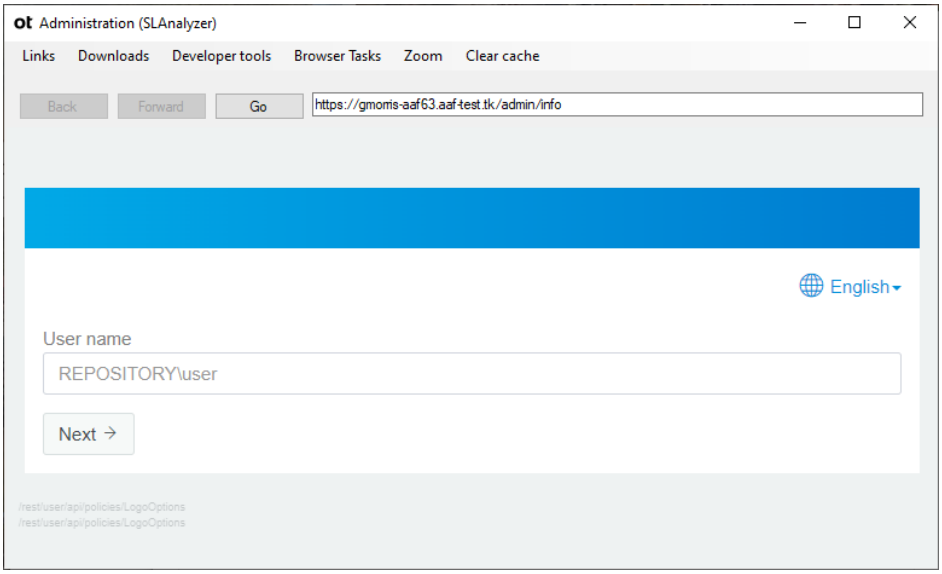


Figure 165 - Browser window

Exit button

The exit button will close the REST Client window and will return to the main SLAnalyzer window.

Status Message

At the bottom of the REST Client window is a status message box. The status will reflect the current activity that is occurring when the REST client is busy or performing some task.

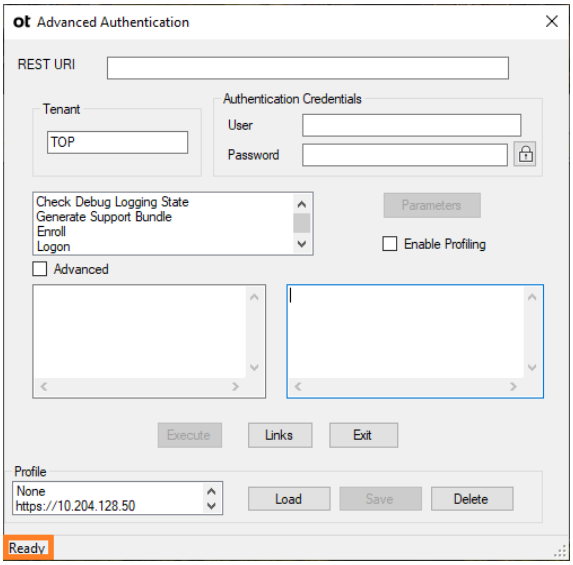


Figure 166 - AAF 5.x Rest Client status message

Profile data

Allows the storing and retrieving of configuration information of the SSPR Rights Validator window. For general information regarding the use of the profile options refer to the profile data section of the SSPR REST client section of this document. Data stored with this option will be saved to: HKEY_CURRENT_USER\Software\MicroFocus\SLAnalyzer\AAFRest.

Packet Data Window

This window displays the details about the request and reply packets sent between SLAnalyzer and the AAF appliance.

The data is presented in the following manner:

Packet
- Name – name of the REST call
- Request – REST call request structure
  - URL – REST URL
  - Data – JSON formatted data structure sent as the body of the REST call
- Reply
  - Status – Status messages and error details
    - HTTPStatus – HTTP protocol status messages
    - WebError – Microsoft Web Exception code messages
    - AAFError – AAF return values
  - Data – JSON formatted data structure received in body of response to the REST call

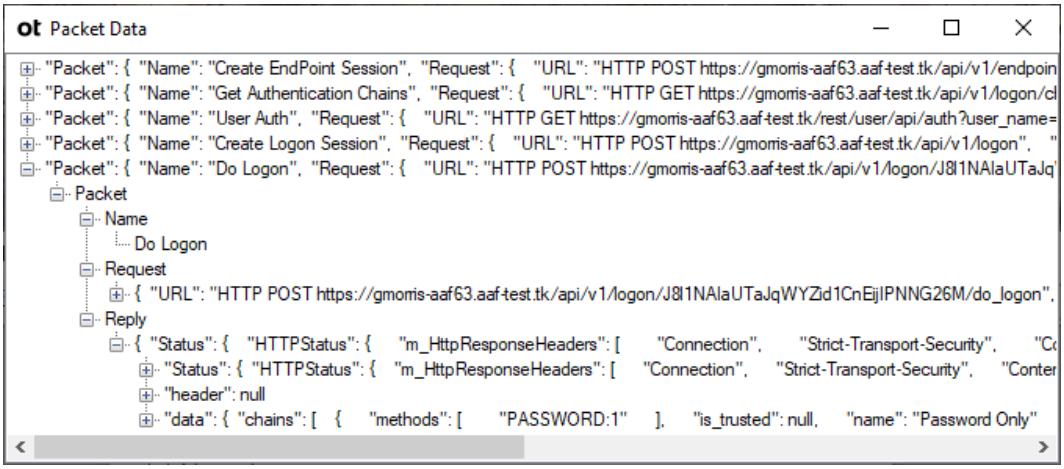
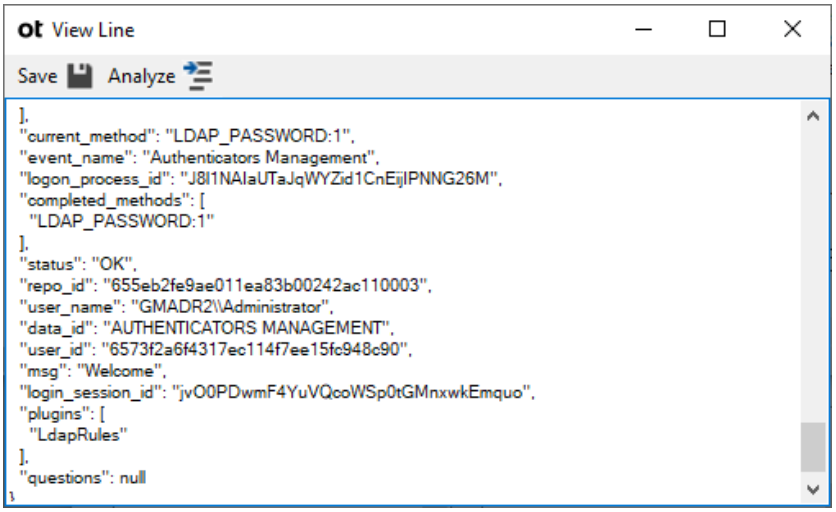


Figure 167 - AAF Packet Data window

Analyzing the data within the packet data window can be done by:

1. Expand and view items
2. Right click and select copy and then paste into a text message/editor
3. Right click and select the option “View Line”.

View Line:



Copy/Paste:



You can clear the items in the packet data window by closing the window. On the next REST call the packet data window will be displayed again with the updated information.

Automated Processes:

SLAnalyzer includes a set of automated processes to perform specific AAF tasks. Specific REST calls need to be made to the AAF server to complete higher level tasks. The automated tasks perform the underlying calls to support the desired function. For example, to perform a login, the following REST calls must be made.

1. Create Endpoint Session
2. Get Authentication Chains
3. Create Logon Session
4. Do Logon

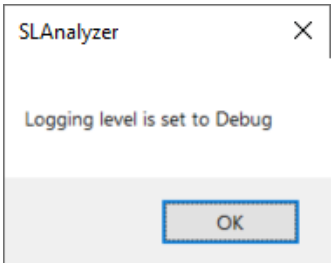
SLAnalyzer will automate the login process and will prompt the user for any required information. Like the selection of endpoint session to use, login chain, or authentication (IE password).

The following automated processes are currently defined:

- Check Debug Logging State
- Generate Support Bundle
- Enroll
- Logon
- Delete User(s)
- Get Server Status
- Lookup User
- List of Users
- Test Device Manager Plug-In
- Build enrolled methods database
- Manage OTP Tokens
- Show Shared Template Info
- Register Method for User
- Show Override Auto Enrollment
- Manage Radius Clients

Check Debug Logging State

This process will make a REST call to the server and return the state of debug logging.



Generate Support Bundle:

This process creates a support bundle.

1. Enter REST URI to the AAF appliance
2. Enter an administrative user for the Authentication credentials. Use local\admin or a member of the Full Admins group defined in the global roles of the local repository.
3. Click the option Generate Support Bundle (Advanced checkbox is unechecked)
4. Click the Execute button

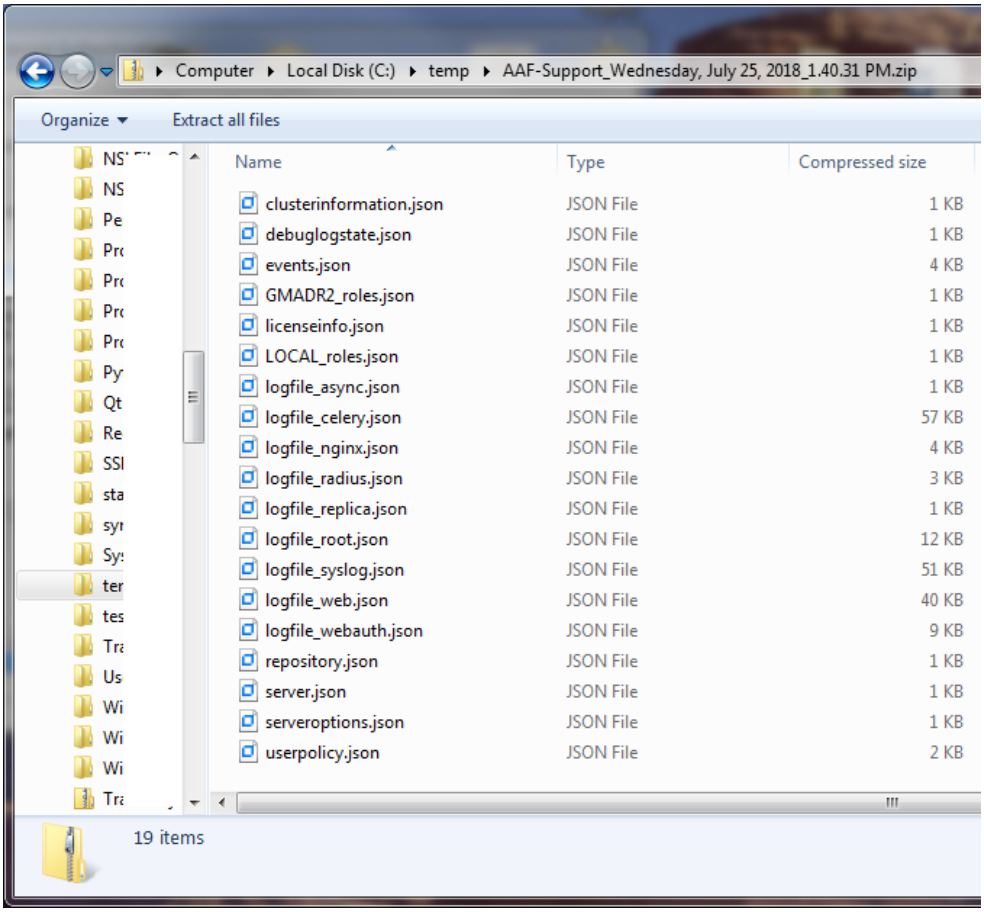
SLAnalyzer will now connect to the AA server via the user API. This is the same process when logging into the admin portal page.

Entering an invalid username will result in the default chains being displayed.

After entering a valid password click the ok button. SLAnalyzer will then proceed in generating the support bundle.

Once complete a message is displayed indicating the status and location of the support bundle.

So what is included in the AAF support bundle?



Clusterinformation.json – contains the information about cluster configuration

Debuglogstate.json – contains the status of debug logging

Events.json – contains information about events configured on the AAF appliance

REPOSITORNAME_roles.json – (IE. GMADR2_roles.json) – contains information about the roles assignments (groups) for the specified repository

Licenseinfo.json – contains information about the licenses installed on the AAF appliance

Logfile_xxxxx.json – contains the debug logs for each of the log types of the AAF appliance.

- Logfile_async.json
- Logfile_celery.json
- Logfile_nginx.json
- Logfile_radius.json
- Logfile_replica.json
- Logfile_root.json
- Logfile_syslog.json
- Logfile_web.json
- Logfile_webauth.json

Repository.json – contains information about the repositories configured on the AAF appliance

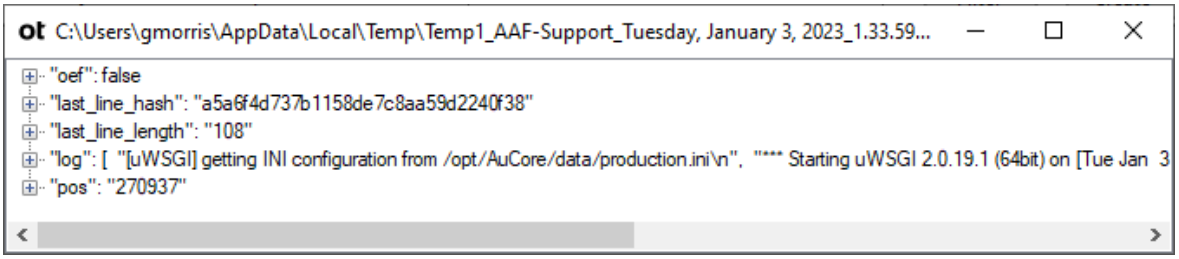
Server.json – contains information about server version and features

Serveroptions.json – server options information

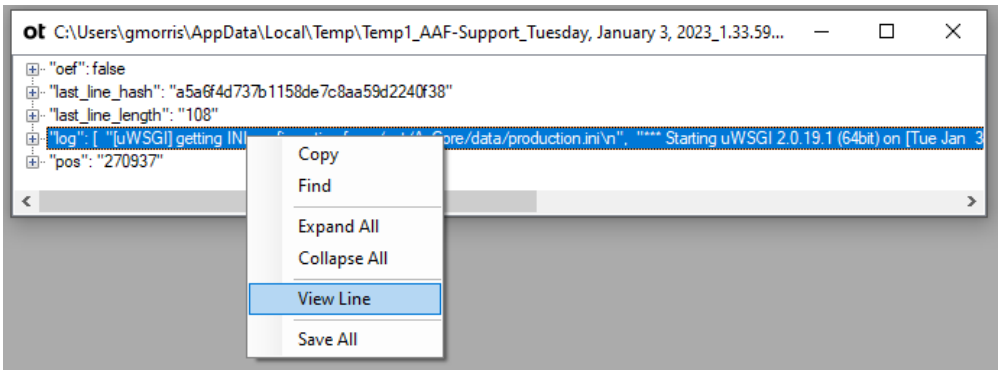
Userpolicy.json – contains information about server policy data effective for logged in user

Viewing the logs and other data.

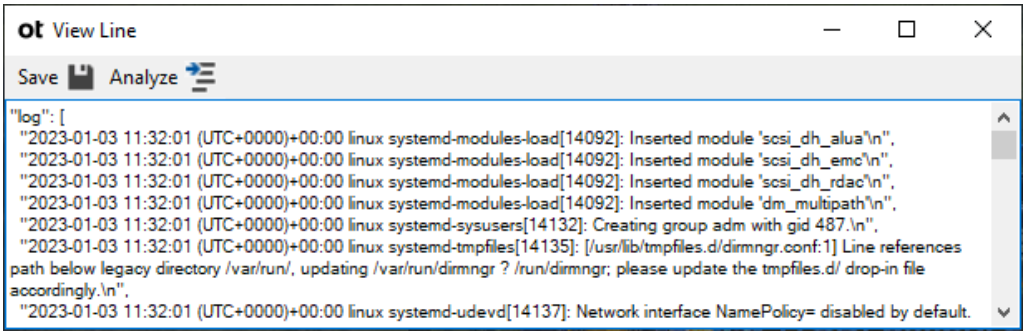
After creating a support bundle you can right click and open with SLAnalyzer. SLAnalyzer supports opening compressed files. Or if you view in Windows explorer, you can also just open the file directly with SLAnalyzer.



When opening a json file SLAnalyzer displays the information in a tree view. You can right click and select “Expand All” to see the data. You can also highlight a line and then right click and select “View Line”.

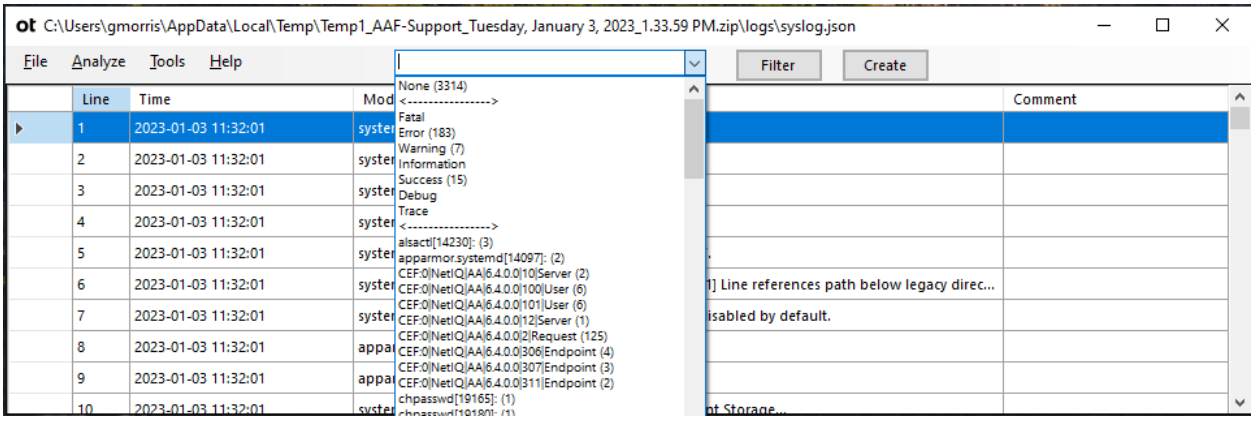


SLAnalyzer will then display the whole line and subsequent child items for easier view.



If you are looking for errors or would like the ability to filter and search the information, then click the Analyze button.

The data is then displayed in table form. The lines are colorized for errors, warnings, etc. The quick filters also allow you to quickly select different message types.



Enroll

Selecting Enroll when the “Advanced” checkbox is not checked will invoke the automated enrollment method. By clicking the execute button the required AAF REST calls will be made to invoke the enrollment process.

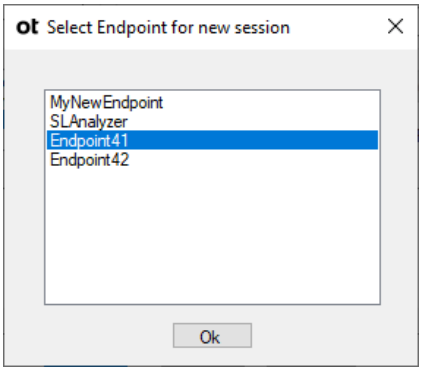
The REST request window displays the information for all the AAF REST calls made to the appliance.

For example:

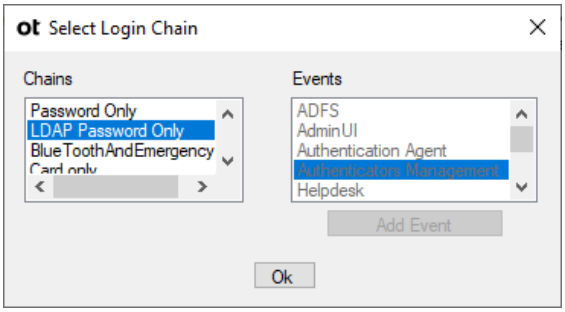
Get Authentication Chains
****
Server Request:
naaf51.gmadr2.novell.com/api/v1/logon/chains?application=Authenticators%20Management&endpoint_session_id=abC4bN4qNL4UoEqeHvOto9Th9A6doh7i&is_trusted=true
****
Logon
****
Server Request:
naaf51.gmadr2.novell.com/api/v1/logon
{"method_id":"LDAP_PASSWORD:1","user_name":"naafuser","application":"Authenticators Management","endpoint_session_id":"abC4bN4qNL4UoEqeHvOto9Th9A6doh7i"}
****
Do Logon
****
Server Request:
naaf51.gmadr2.novell.com/api/v1/logon/Snpge8OXKyzPemOGHJ70WR16dN12wSZK/do_logon
{"response":{"answer":"novell"},"endpoint_session_id":"abC4bN4qNL4UoEqeHvOto9Th9A6doh7i"}
****
Get Logon Information
****
Server Request:
naaf51.gmadr2.novell.com/api/v1/logon/sessions/v6jLCh1WnDJcu2FUPuocEm2QW7QKqJhc?endpoint_session_id=abC4bN4qNL4UoEqeHvOto9Th9A6doh7i
****

The reply window would display the information received for each of these requests that were made. If all the calls are successful, then the Methods window should be displayed. Otherwise, the reply window will provide information as to why the automated process failed.

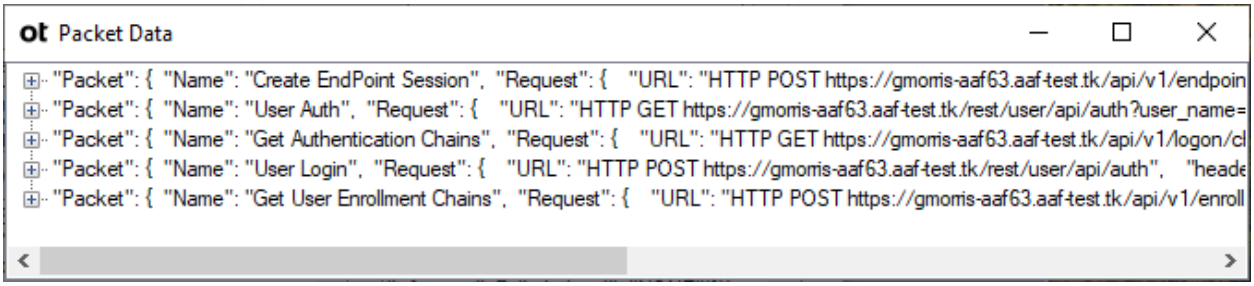
The first step in invoking the Enroll process is to establish an endpoint session with the appliance. SLAnalyzer will prompt the user to select the desired endpoint session.



SLAnalyzer will perform the necessary REST calls to build a list of the current Logon Chains. By Default, the Event Authenticators Management is selected and the Chains defined for this event are listed in the Chains selection box. Select a chain from the Chains selection box to logon to the appliance.



The packet data window will display the REST call information used in the automated Enroll process.



After login SLAnalyzer will build a list of the methods defined on the appliance. The methods window will then be displayed for enrollment.

Enrollment window

The enrollment window displays the possible logon chains as defined at the appliance.

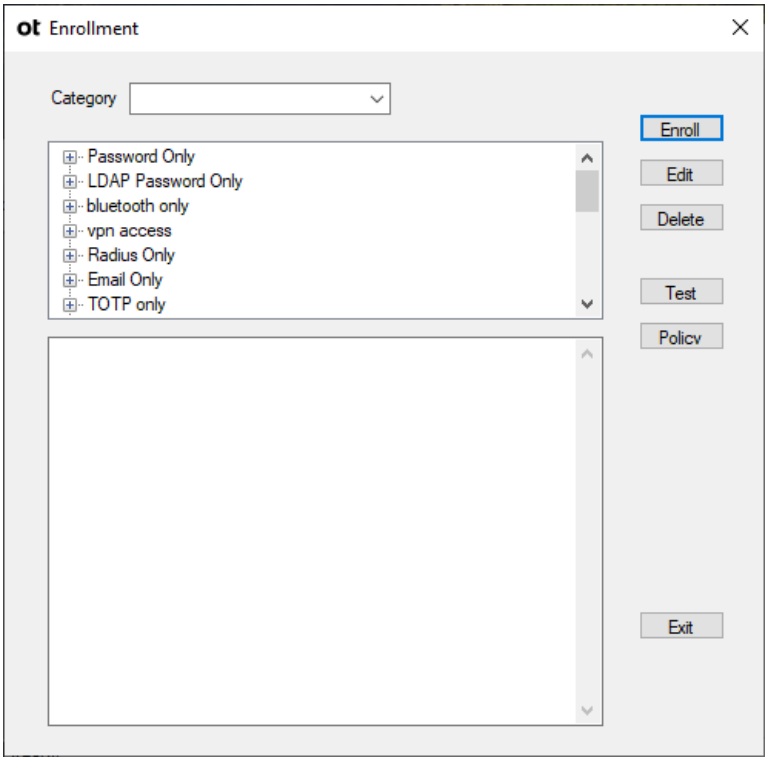


Figure 168 - Enrollment window

Included on the enrollment window are the following components:

- Chains/methods box
- Status box
- Enroll button
- Edit button
- Delete button
- Test button
- Exit button

Chains/Methods box

Expand any of the listed Logon chains listed in the Chains/Methods box to see the methods assigned to the chain. Clicking on one of the methods will display the information about this method in the status box. Also note that the buttons will be enabled or disabled depending on the status of the method selected.

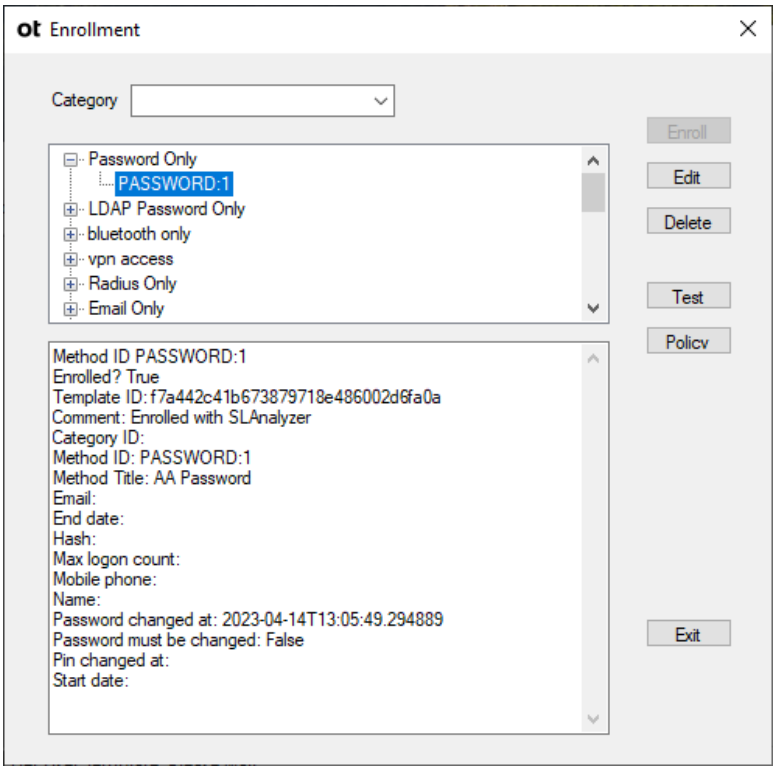


Figure 169 - Enrollment window with selected item

Methods in AAF 5.1.4

SLAnalyzer currently supports most of the methods defined in the AAF 5.1.4 or higher appliance. New methods are being added all the time. But due to lack of hardware or other testing resources some methods have not yet been tested. Untested methods might work but proper operation is unknown.

- Password (tested)
- LDAP Password (tested)
- Bluetooth (tested)
- Smart Card (tested)
- Email OTP (tested)
- Emergency Password (tested)
- Face (tested)
- Fingerprint (tested)
- HOTP (tested)
- PKI (tested)
- RADIUS (not tested)
- SMS OTP (tested)
- Security Questions (tested)
- Smartphone (tested)

- Swisscom (not tested)
- TOTP (tested)
- U2F (not tested)
- VOICE (tested)

Status box

The status box is the box located below the Chains/Methods list box. It displays information about the currently selected item in the Chains/Methods list box.

Enroll button

If the selected item in the method list is not currently enrolled, then the Enroll button will be enabled.

Clicking this button will start the enrollment process. The process invoked for the enrollment is different for each method. If required, the user will be prompted to enter some information to complete the enrollment process.

(PASSWORD:1) Password enrollment

The Password:1 method is the locally stored password on the AAF Appliance.

User prompted for their password.

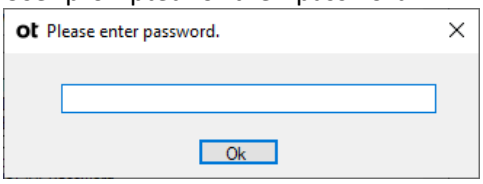


Figure 170 - Password enrollment

(LDAP_PASSWORD:1) LDAP Password enrollment

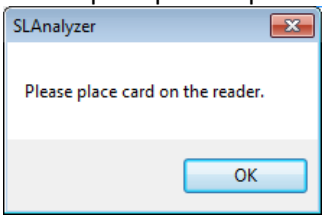
The LDAP_Password:1 method is the users' password in the repository.

This is always enrolled.

(CARD:1) Smart Card enrollment

Card:1 method is a contactless (proximity) card and reader.

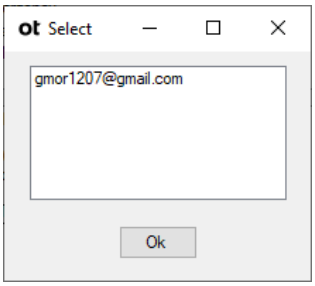
User is prompted to place their card on the reader.



(EMAIL_OTP:1) Email OTP enrollment

Email_OTP:1 method sends an email to the user with a one time password value.

SLAnalyzer will prompt the user for the email address to send the OTP too. If no email address is entered, then SLAnalyzer will send the request to the AAF server and it will read the email address assigned to the user in the directory. If no address is specified and no address can be found in the directory, then the enrollment process will fail.

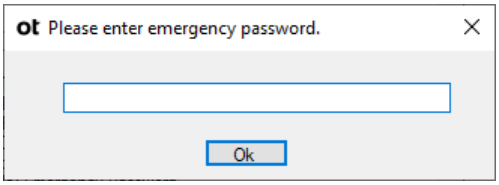


If the enrollment process fails, then the status window will display the message:
Status: Enrollment failure. For email OTP this is normally because the user object in the LDAP directory doesn't have a valid email address.

(EMERG_PASSWORD:1) Emergency Password enrollment

Emerg_Password:1 method is a local stored password for emergency access.

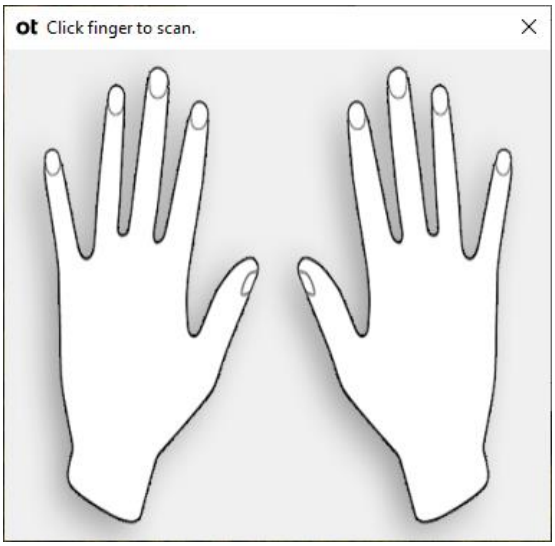
User is prompted to enter an emergency password.



(FINGER:1) Fingerprint enrollment

Finger:1 method is used with a biometric fingerprint scanner.

User is prompted to scan fingers.



(HOTP:1) HOTP enrollment

HOTP:1 method is a HMAC-based one-time password.

This is a good explaination of HOTP and TOTP.
https://blogs.forgerock.org/petermajor/2014/02/one-time-passwords-hotp-and-totp/

User prompted for a Secret.

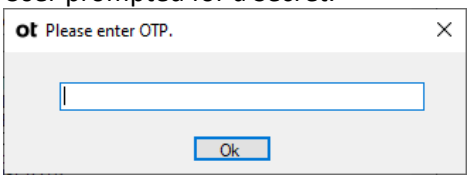


Figure 171 - HOTP enrollment

(PKI:1) PKI enrollment

PKI:1 method is used with smart cards and readers. These typically will have a gold or silver chip on the front of the card. Using a card management system (CMS) an administrative user will issue the card to a specific user. During this process a certificate is stored on the card. This certificate is then used during the enrollment and logon processes.

Although the device service mechanism can return the information from the card, the automated process of enrollment is not yet implemented in SLAnalyzer. The user will be prompted for the required parameters. For proper enrollment use the AAF user portal instead of SLAnalyzer. Note that you can use the Device Service test to access the card and validate the information. This could be recorded and then manually entered when prompted by SLAnalyzer, but this process has not be tested.

(RADIUS:1) RADIUS enrollment

Radius:1 method is used to authenticate the user based on authentication to a Radius server.

The AAF server has a built-in Radius server that can provide Radius services. Also, AAF supports external Radius server configurations. Please refer to the AAF online documentation on proper configuration of Radius servers. https://www.netiq.com/documentation/advanced-authentication-56/server-administrator-guide/data/radius_server.html

User is prompted for their Radius password.

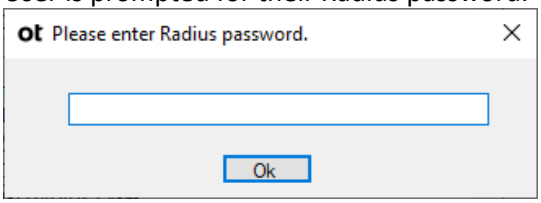
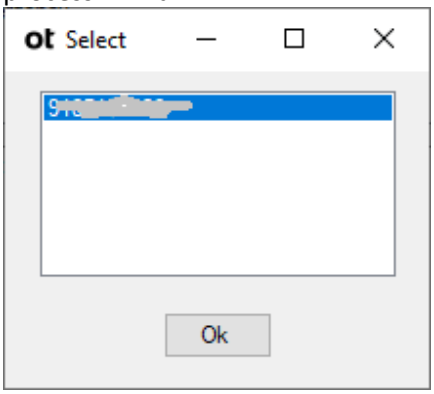


Figure 172 - Radius enrollment

(SMS_OTP:1) SMS OTP enrollment

SMS_OTP:1 method sends an SMS one time password to the user's mobile phone.

SLAnalyzer will prompt the user for the phone number to send the OTP too. If no number is entered, then SLAnalyzer will send the request to the AAF server and it will read the number assigned to the user in the directory. If no number is specified and no number if found in the directory, then the enrollment process will fail.



If the enrollment process fails, then the status window will display the message:
Status: Enrollment failure. For SMS OTP this failure normally indicates that the user object in the LDAP directory does not have a valid phone number.

(SECQUEST:1) Security Questions enrollment

Secquest:1 method is a

The user is prompted to provide an answer to each of the defined security questions.

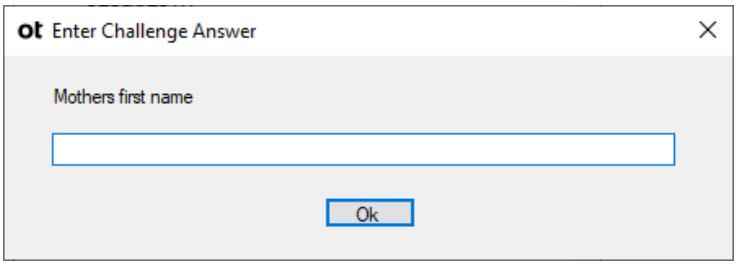


Figure 173 - Security Question enrollment

(SMARTPHONE:1) Smartphone enrollment

User is prompted to scan the QR code with the smartphone app.



Figure 174 - Smartphone enrollment

(SWISSCOM:1) Swisscom enrollment

This is always enrolled.

(TOTP:1) TOTP enrollment

User prompted for a Secret.

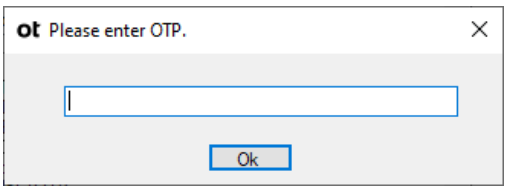


Figure 175 - TOTP enrollment

(U2F:1) U2F enrollment

This is always enrolled.

(VOICE:1) Voice enrollment

User is prompted for their pin.

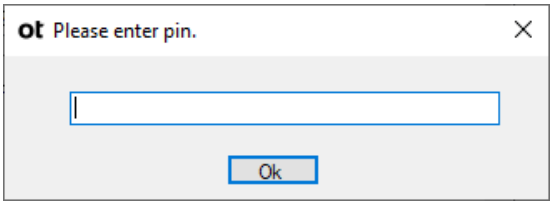


Figure 176 - Voice enrollment

Edit button

The edit button allows the user to edit the information stored for the currently enrolled logon method. The edit button is only enabled if the selected method in the method list has been enrolled. Otherwise, the button is disabled.

Clicking the button will prompt for the same information that the user defined with enrolling the method. See the enroll method list for details on each method.

- Password
- LDAP_PASSWORD
- TOTP
- HOTP
- SMS_OTP
- SMARTPHONE
- VOICE
- EMAIL OTP
- SECQUEST
- RADIUS

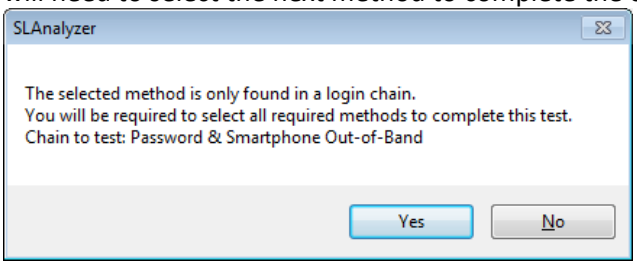
Delete button

The Delete button deletes the enrolled login method. This button is only enabled when the login method has already been enrolled by the user.

Test button

The test button is only available if the login method has been enrolled. The test button will attempt to perform a user login with the login method. The user will be prompted for the necessary information to complete the login process. For example, if the user clicks the test button for password, then the user will be prompted for their password. LDAP password will not prompt since it is defined on the REST window in the Authentication Credentials section.

Note: If the selected method is only found within a login chain, then the user will be notified that they will need to select the next method to complete the chain during the test.



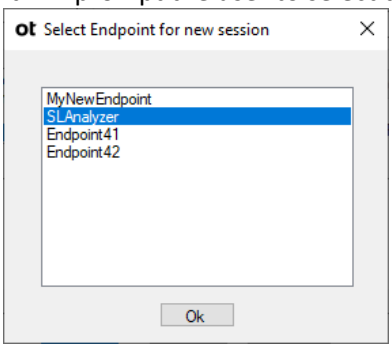
Exit/Done button

The exit button will exit the method list and return to the AAF REST client window.

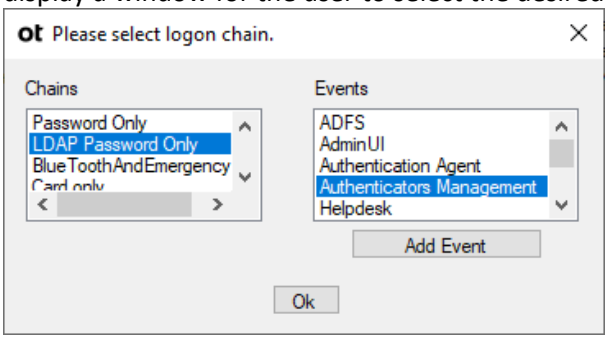
Logon

Executing Logon when the advanced checkbox is not checked invokes the automated Logon process.

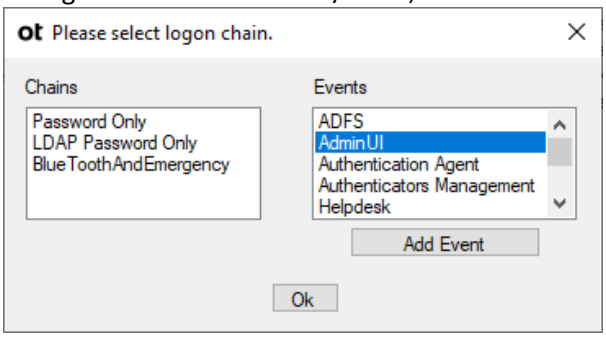
To perform a logon SLAnalyzer must first have an endpoint session. If an endpoint session is not present it will prompt the user to select the endpoint for the connection.



After an endpoint session has been established, SLAnalyzer will make the REST call “Get Authentication Chains” to build a list of logon chains defined on the appliance. After building the list SLAnalyzer will display a window for the user to select the desired logon chain.



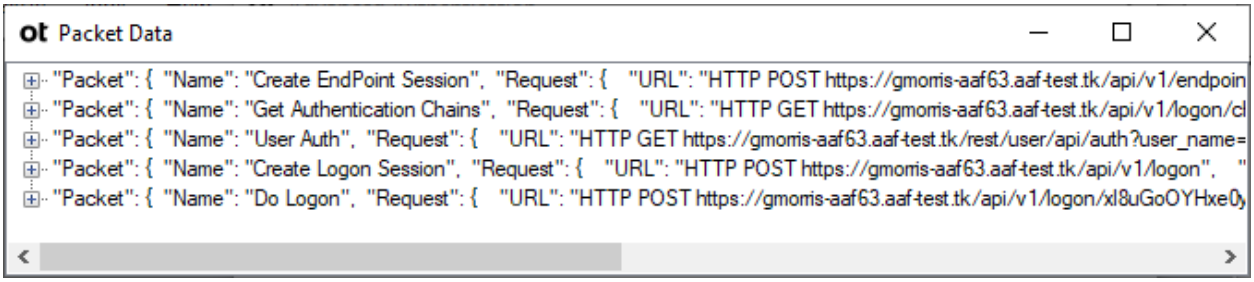
By default, SLAnalyzer will display the logon chains defined for the Authenticators Management event. To login with another event/chain, then select the event from the events list.



If a non-default event has been created, then you can click the Add Event button to add it to the list of Events.
After selecting the logon chain click the Ok button to perform the logon.
If the logon chain includes a single method, then the user will be prompted for the information required to perform that logon method authencation. If the chain contains multiple methods, then the user will be prompted for each method until the chain has been completed.

The following sections explain the data seen for a simple and chained logon

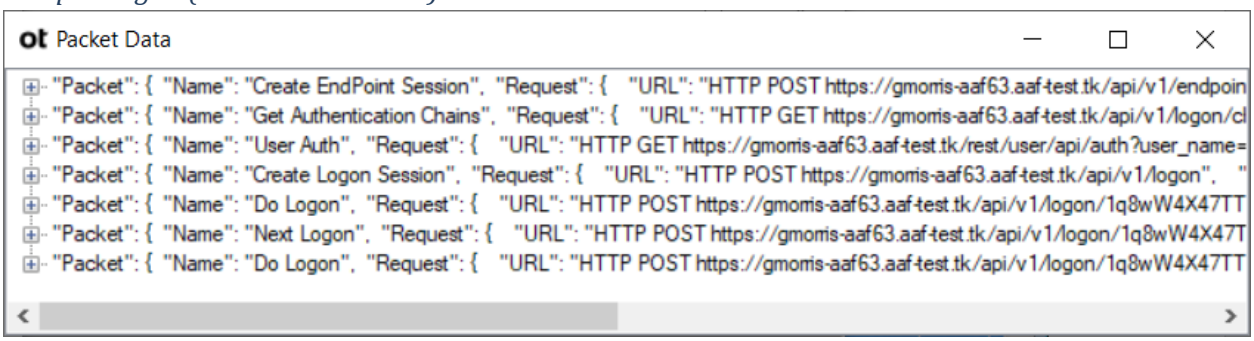
Simple logon (1 method)



In this example we selected the logon chain “LDAP Password Only”.

1. First we create the REST call Create Logon Session and include the logon method and event:
   "method_id": "LDAP_PASSWORD:1",
   "event": "Authenticators Management"
2. The reply from the server tells us to continue:
   "msg": "Process started"
3. The REST call Do Logon continues the logon request and provides the data to complete the logon process:
   {"response":{"answer":"Password"},"endpoint_session_id":"yWHkWcXLnX4fEc7UMz4OCRQhPn0P3ph7"}
   The server responds with:
   "completed_methods": ["LDAP_PASSWORD:1"]
   "msg": "Welcome!"

Complex logon (2 or more methods)



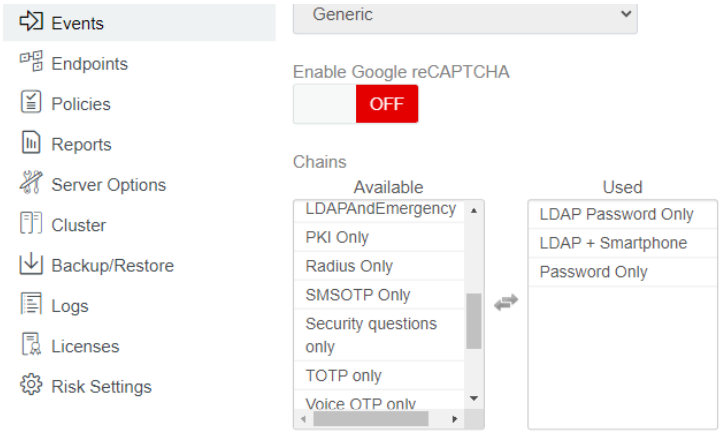
In this example we selected the logon chain “ldap and password”.

4. First we create the REST call Create Logon Session and include the logon method and event:
   "method_id": "LDAP_PASSWORD:1",
   "event": "NCA"
   The reply from the server tells us to continue:
   "msg": "Process started"
5. The REST call Do Logon continues the logon request and provides the data to complete the logon process:
   "response":{"answer":"Password"},"endpoint_session_id":"yWHkWcXLnX4fEc7UMz4OCRQhPn0P3ph7"
   The reply to the Do Logon tells us several things.
   "status": "NEXT"
   "completed_methods": ["LDAP_PASSWORD:1"]
   "msg": "Welcome!. Continue with next login method"
   "methods": ["LDAP_PASSWORD:1", "PASSWORD:1"], "is_trusted": null, "name": "ldap and password"
6. We now issue the Next Logon REST call. SLAnalyzer knows that LDAP_PASSWORD has been completed so it requests to login with the next method in the chain.
   "method_id": "PASSWORD:1"
   The appliance returns:
   MORE_DATA Process started
7. SLAnalyzer now issues the Do Logon request with the password value for the PASSWORD method
   "response":{"answer":"Password"},"endpoint_session_id":"yWHkWcXLnX4fEc7UMz4OCRQhPn0P3ph7"
   The server responds with:
   "completed_methods": ["LDAP_PASSWORD:1", "PASSWORD:1"]
   "msg": "Welcome!"

It is important to understand how the AA server processes logon chains. Logon chains are defined for an event. The chains are processed in order from the top entry to the botton entry. If during the logon process, a method is used for authentication that matches a method higher in the chain list, then logon will succeed without requiring all the methods in the selected logon chain.

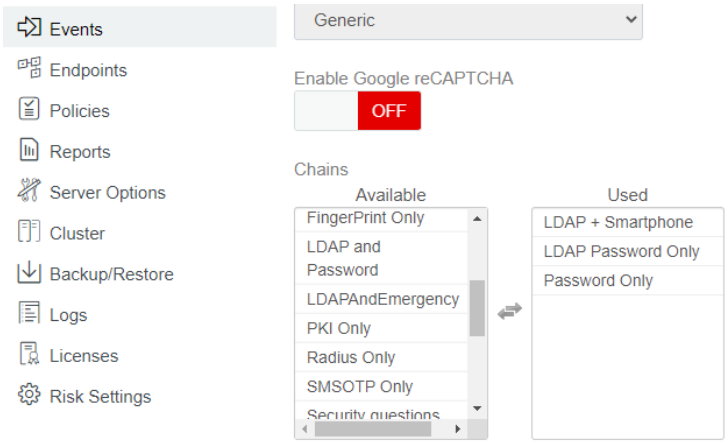
For example, if we had a chain with a single method of LDAP Password with the name LDAP only… And we had another chain with both LDAP password and Smartphone named LDAP + Smartphone…

In the event we see the Used chains list as…



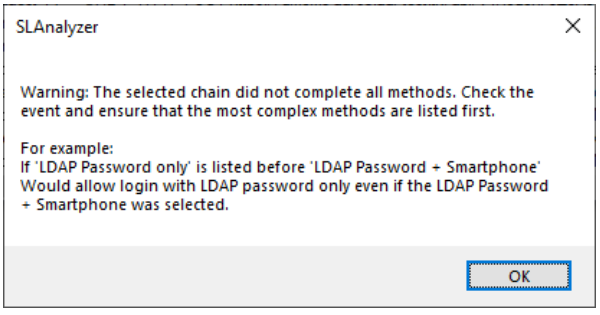
If a user selected to login with the chain LDAP + Smartphone… The user would only be prompted for their LDAP password. This is because the LDAP only chain higher in the list will match the LDAP Password requirement.

If we change the Used chain order to:



Now when the user selects LDAP + Smartphone, during login the server would first prompt for the LDAP password. It would then see that another method is required for this chain and would then send the push notification to the smartphone method.

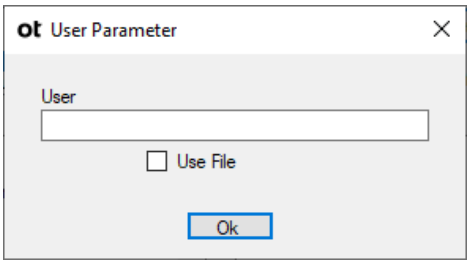
If SLAnalyzer detects this condition it will display a warning message informing the user to check the event.



Delete User(s)

This option allows for the deletion of users registered with the AA server.

To delete a single user just click the Execute button. SLAnalyzer will prompt to connect to an endpoint session if you have not logged in previously. It will then prompt for the Username.

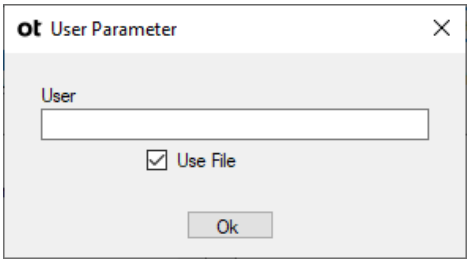


Enter a username or the user DN for deletion.

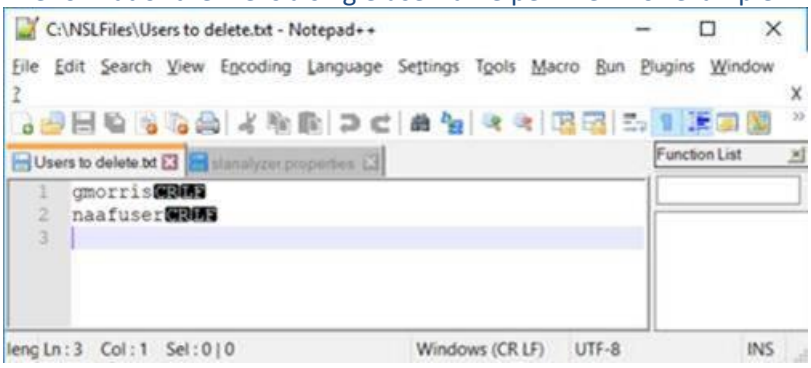
Bulk delete user

SLAnalyzer also provides the ability to delete multiple users at one time.

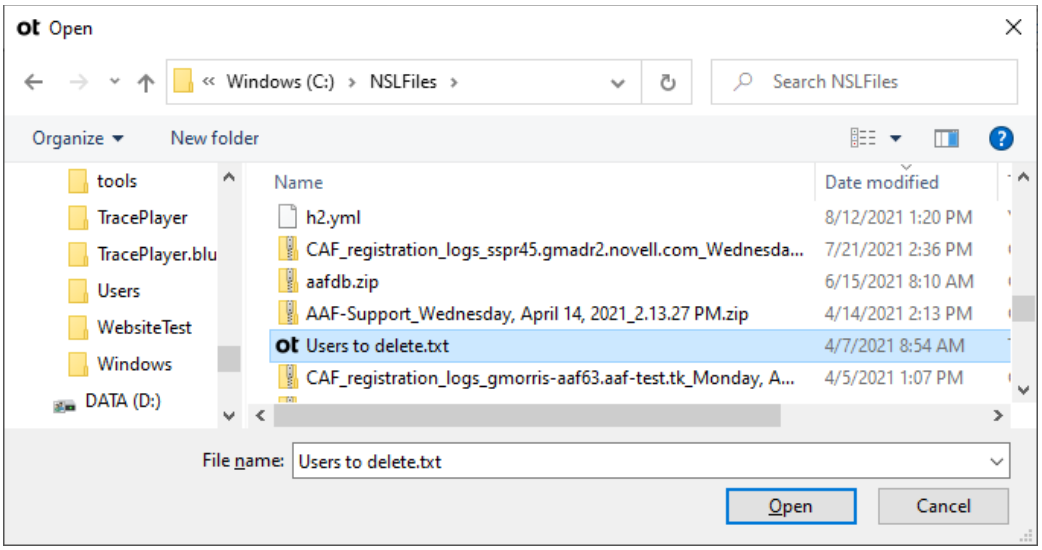
Click the parameters button to instruct SLAnalyzer to use a file.



The format of the file is a single username per line… For example.



After clicking the execute button you will be prompted to select the user file.



After selecting the file SLAnalyzer will then delete each user from the list.

Server Status

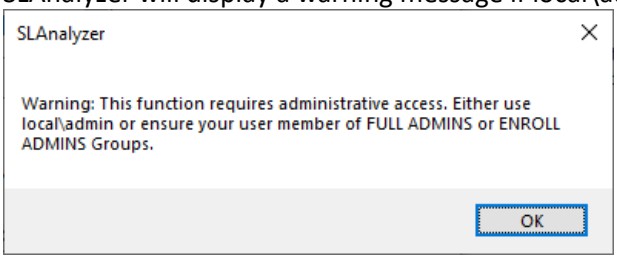
Returns server version and status.



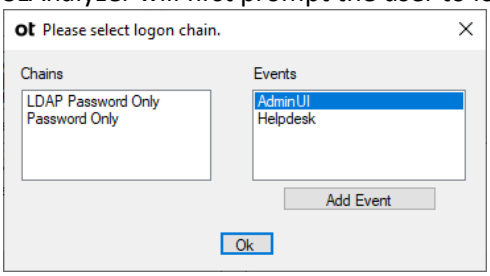
Lookup User

Lookup users requires that the logged in user be a member of FULL ADMINS or ENROLL ADMINS global roles.

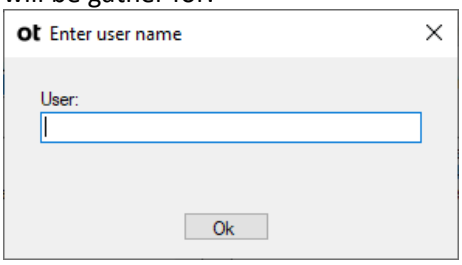
SLAnalyzer will display a warning message if local\admin is not the current user.



SLAnalyzer will first prompt the user to login to the AdminUI or HelpDesk application.



After successful login of the user then SLAnalyzer will prompt for the name of the user that information will be gather for.



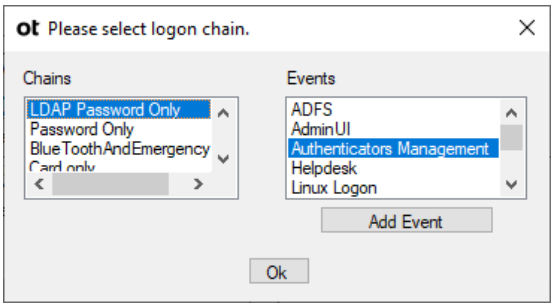
Server returns enrolled method data for the specified user.



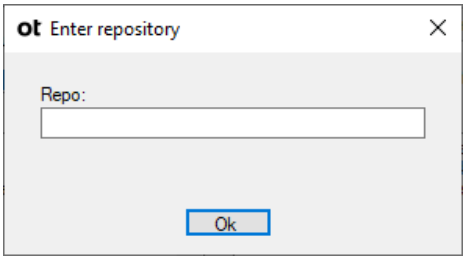
List of Users

Note: List of users is restricted to a maximum of 50K objects. To list more users than 50K click the parameters button and select the next page. For example, the first 50K users are page 0, the next 50K of users will be page 1, etc.

For authentication you need special rights for this REST call.
`Either use local\admin or ensure your user is a member of FULL ADMINS or ENROLL ADMINS Groups.`



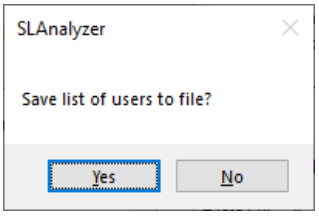
After a successful login, the user is prompted for the name of the repository.
Note to list the local accounts of the AAF server just enter the repo name of local.



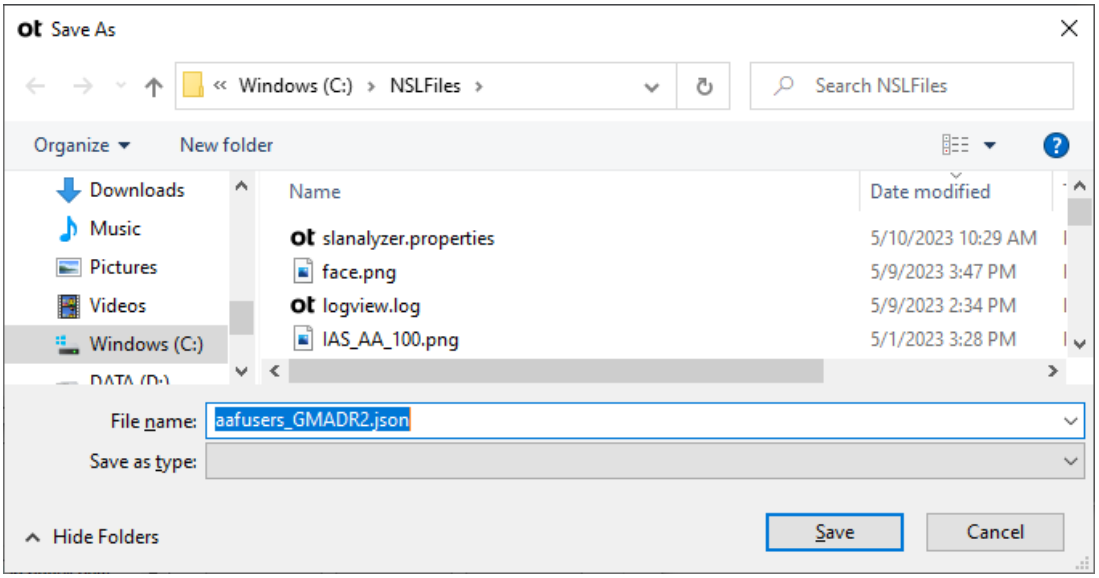
The server returns a list of users who have logged into AAF for the specified repository.



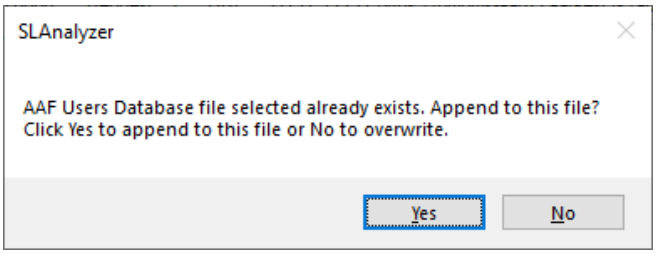
After the list of users has been obtained SLAnalyzer will prompt to save the user information to a file. This file can then be used in the build enrolled methods database option.



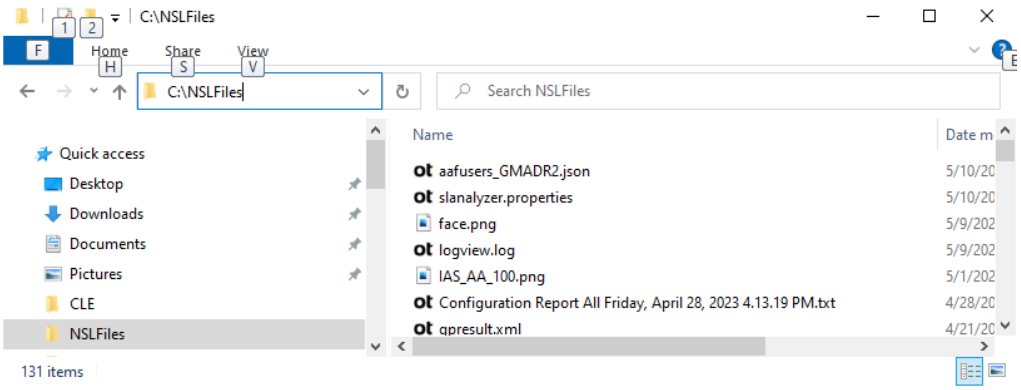
If the user selects “Yes” to save the data to a file, then SLAnalyzer will open a saveas window to allow the user to specify the filename and path of the file. By default SLAnalyzer attempts to create the file as aafusers_<Repository_name>.json. It also attempts to save the file to the local SLAnalyzer log path.



SLAnalyzer will check if the file already exists and will prompt the user if they want to append or overwrite the file.



After the list of users file is created you will find it in the SLAnalyzer log path. This path is defined in the SLAnalyzer Settings as the Default Report Folder. By default, SLAnalyzer will use c:\nslfiles.



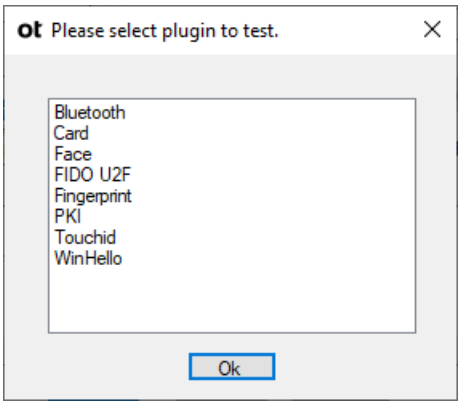
The users file is a json formatted file. You can open this with SLAnalyzer if you want to inspect the information returned by the AAF appliance.



Test Device Manager Plug-in

This option allows for testing of the AAF Windows device manager. Hardware devices like PKI, Fingerprint, etc. are interfaced with the device manager.

When selecting this option SLAnalyzer will prompt the user to select the type of device to test.

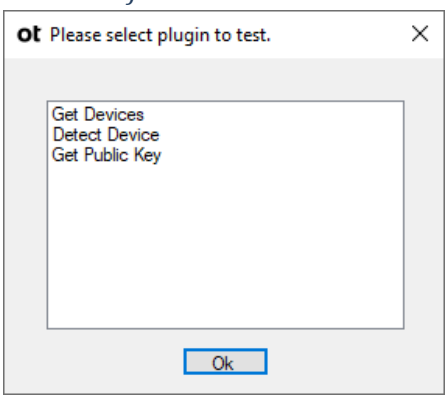


The following hardware devices are currently supported.

- Bluetooth
- Card
- Face
- FIDO U2F
- Fingerprint
- PKI
- Touchid
- WinHello

After selecting a device type to test a list of available functions for that specific device will be listed.

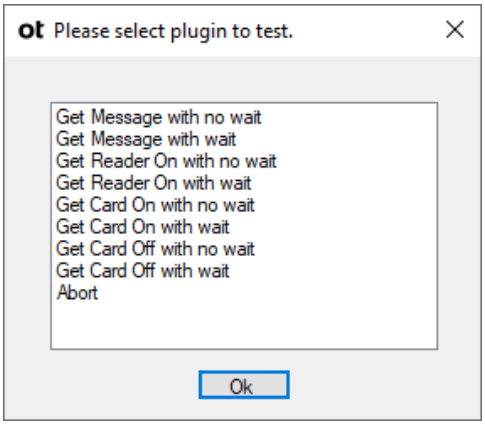
Bluetooth functions



- Get Devices – Return a list of all blue tooth devices
- Detect Device – Return the status of a blue tooth device
- Get Public Key – Gets the public key from the device service

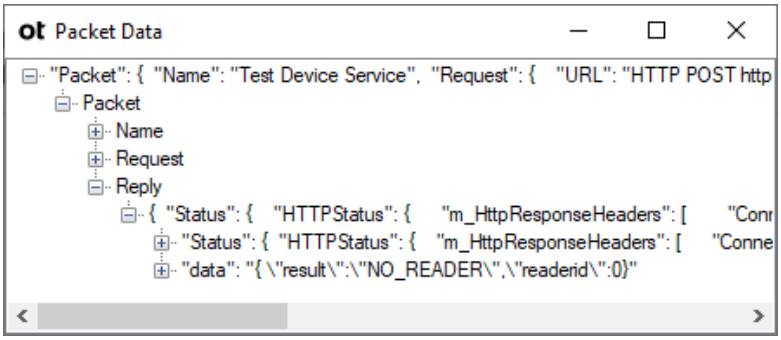
Card functions

Select the function for the plugin to test.



- Get Message with no wait – Will get the card reader status message and immediately return
- Get Message with wait – Will wait for a card to be placed or removed from reader
- Get Reader On with no wait – Will report reader On/Off and immediately return
- Get Reader On with wait – Will wait for Reader On state
- Get Card On with no wait – Will report card On/Off and immediately return
- Get Card On with wait – Will wait for Card On state
- Get Card Off with no wait – Will report card On/Off and immediately return
- Get Card Off with wait – Will wait for Card Off state
- Abort – Will abort current operation

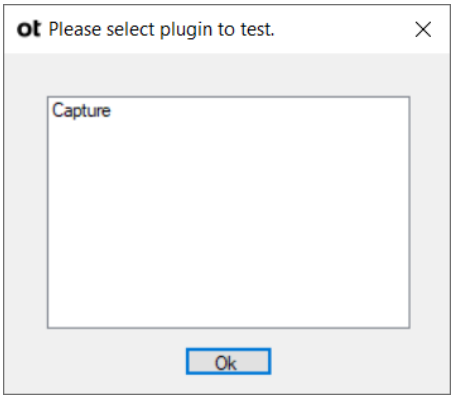
To see the results of the test look at the Packet Details screen



Note: if the user selects an option with the wait option then SLAnalyzer will appear to be unresponsive as it is scanning the device for a response. The Rest Client window status message will display the current status but the user will be unable to select the packet details window until the state has changed to satisfy the call or a timeout occurs.

Face functions

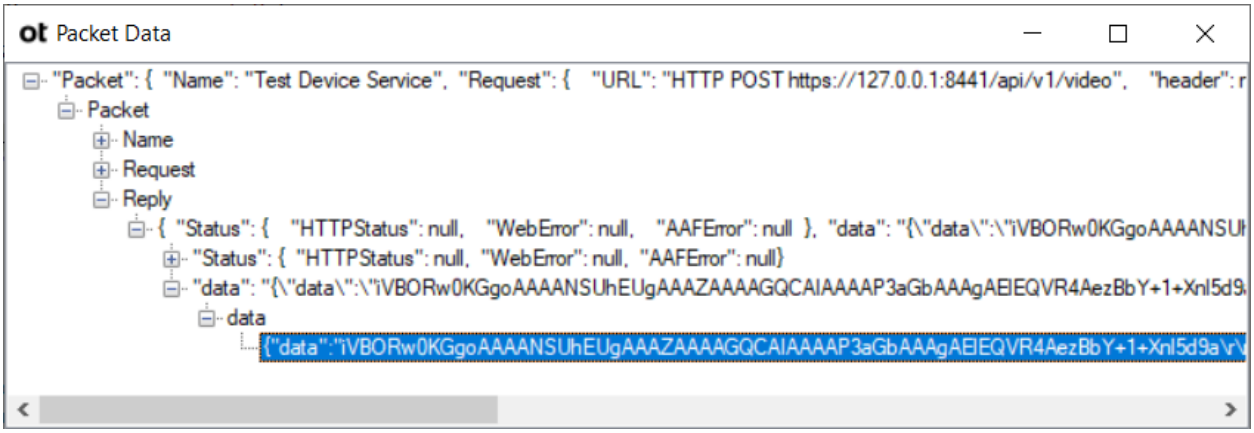
There is a single function to test



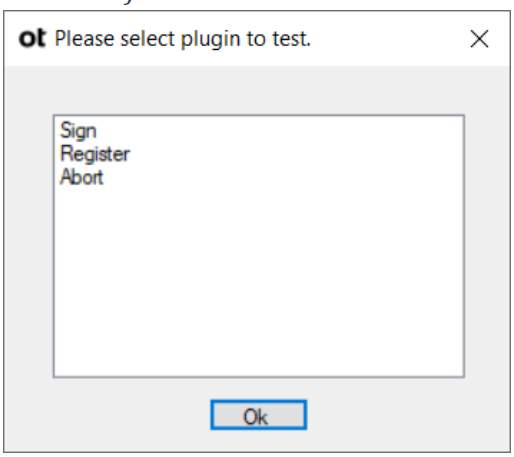
When selected the camera will be activated to capture a current image.



The packet data window will display the request and reply data from the local device service.

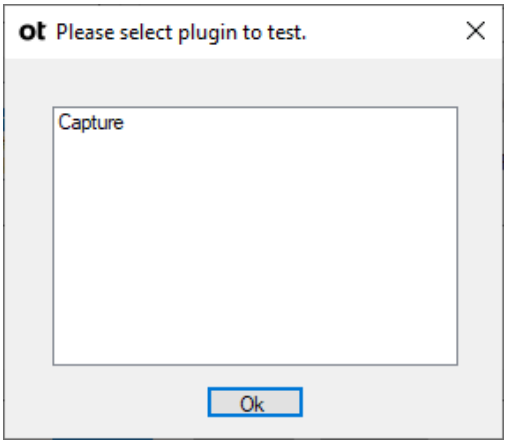


FIDO U2F functions



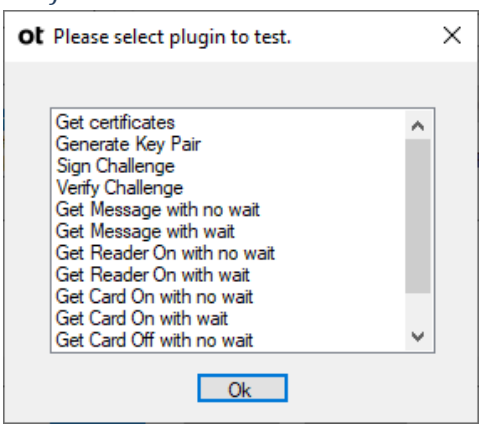
- Sign – Performs the U2F authentication
- Register – Performs the U2F register
- Abort – Aborts all pending operations

Fingerprint functions



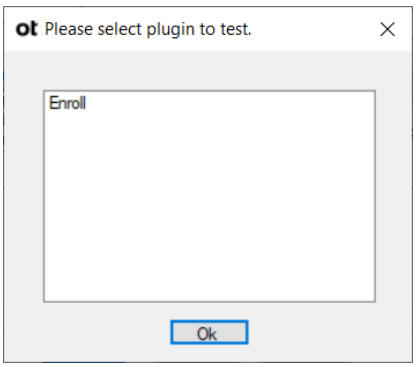
- Capture – performs a capture of a finger print

PKI functions

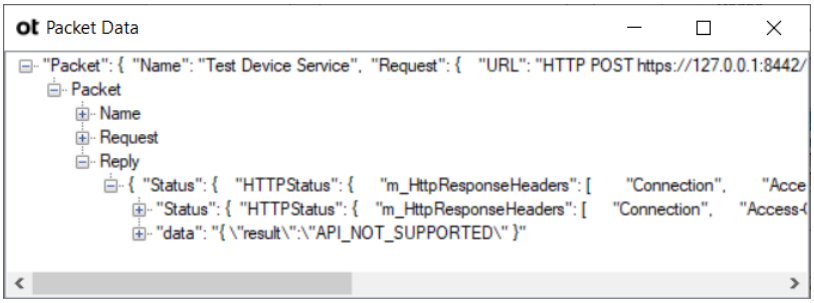


- Get certificates – Get all certificates from a token
- Generate Key Pair – Generates a new key pair for a token
- Sign Challenge – Sign a challenge string
- Verify Challenge – Verify a challenge string
- Get Message with no wait – Will get the card reader status message and immediately return
- Get Message with wait – Will wait for a card to be placed or removed from reader
- Get Reader On with no wait – Will report reader On/Off and immediately return
- Get Reader On with wait – Will wait for Reader On state
- Get Card On with no wait – Will report card On/Off and immediately return
- Get Card On with wait – Will wait for Card On state
- Get Card Off with no wait – Will report card On/Off and immediately return
- Get Card Off with wait – Will wait for Card Off state
- Abort – Will abort current operation

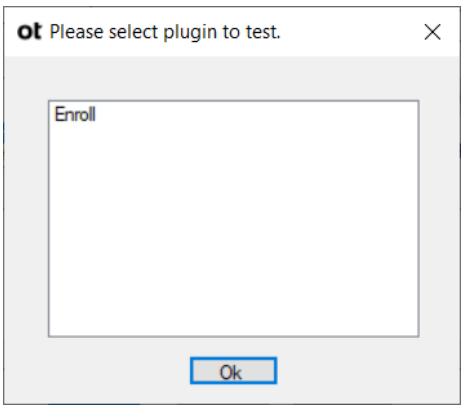
Touch ID



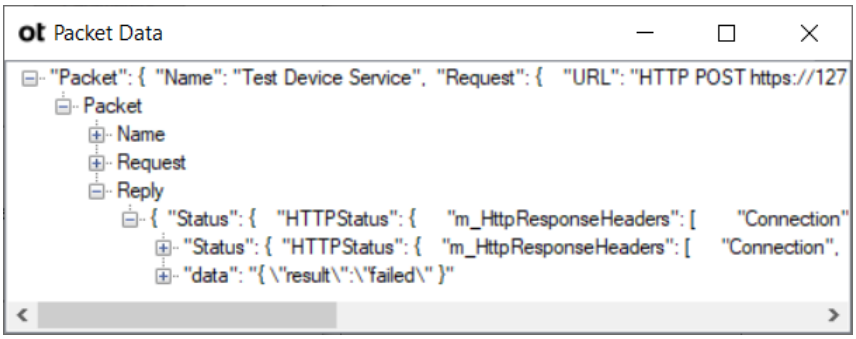
When selected this option the device service will attempt to communicate with the OS API's for TouchID. If the OS does not support Touch ID, then the following error will be seen in the Packet Data window.



Windows Hello



When selected this option the device service will attempt to communicate with the OS APIs for Windows Hello. If Windows Hello has not been configured, then the following error will be seen in the Packet Data window.



Build enrolled methods database

Build enrolled methods data base requires that the logged in user be local\admin or a member of FULL ADMINS or ENROLL ADMINS global roles.

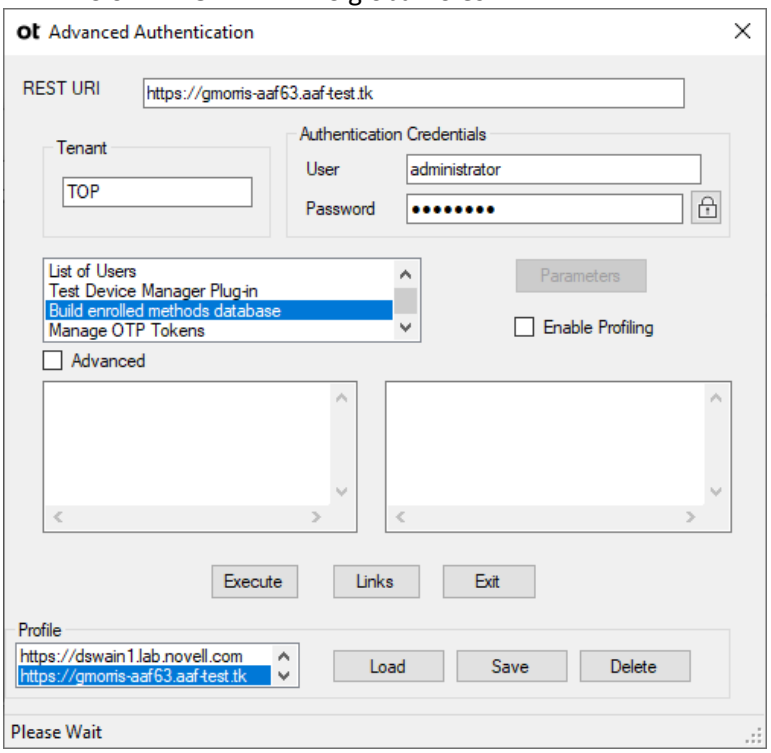
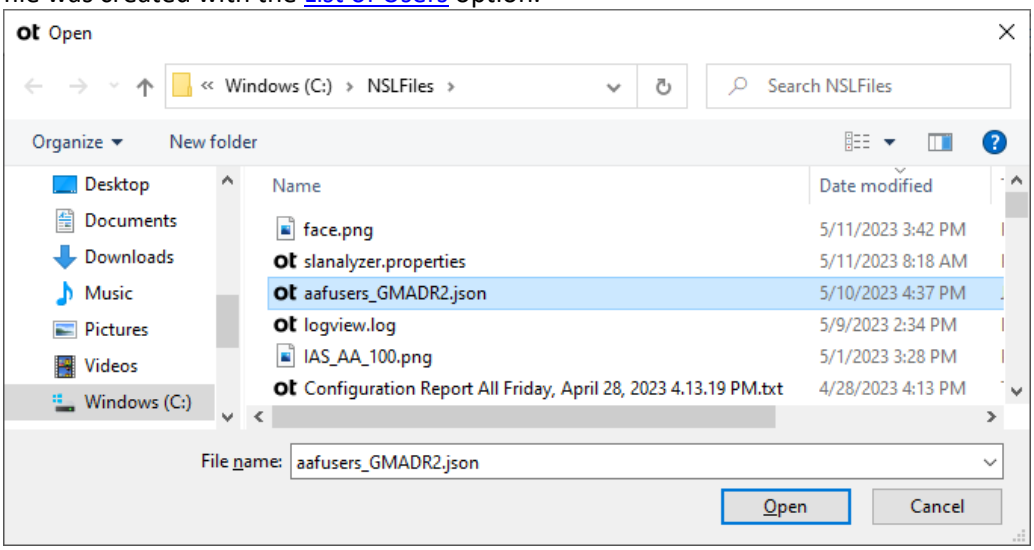


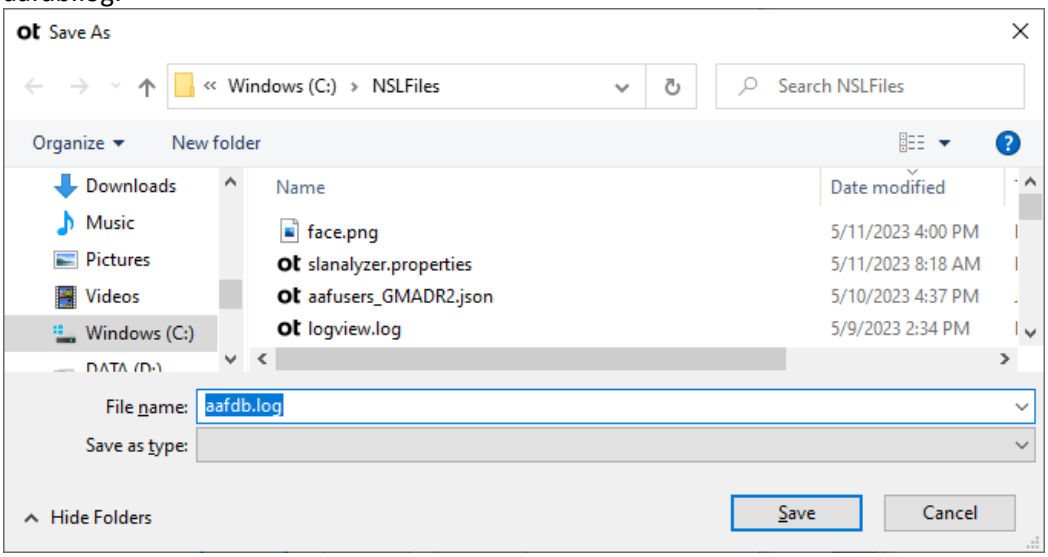
Figure 177 - Build enrolled methods database

You must first create the list of users to generate the report against. See the option List of Users.
Specify the local\admin account and then scroll down to the option “Build enrolled methods database”.

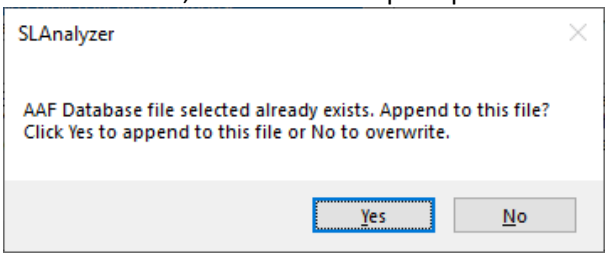
Click the Execute button to initiate the process. SLAnalyzer will prompt to open the aafusers list file. This file was created with the List of Users option.



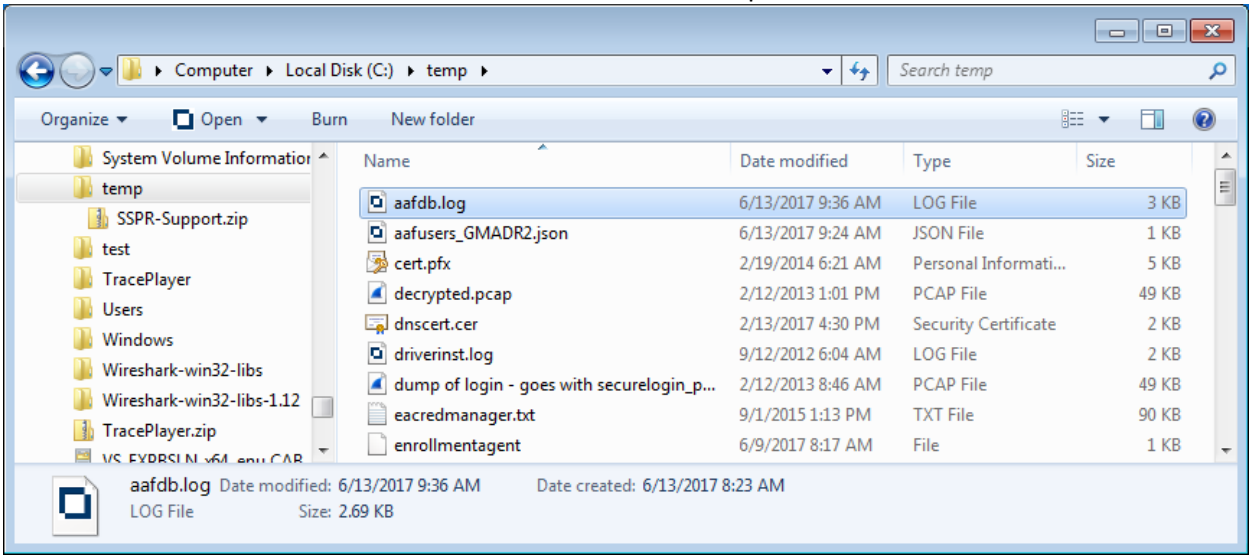
Next SLAnalyzer needs to know where to save the information. Navigate to the desired path and enter the database filename. By default, SLAnalyzer will save to the default log path with the filename of aafdb.log.



If the file exists, the user will be prompted to overwrite or append to the existing file.



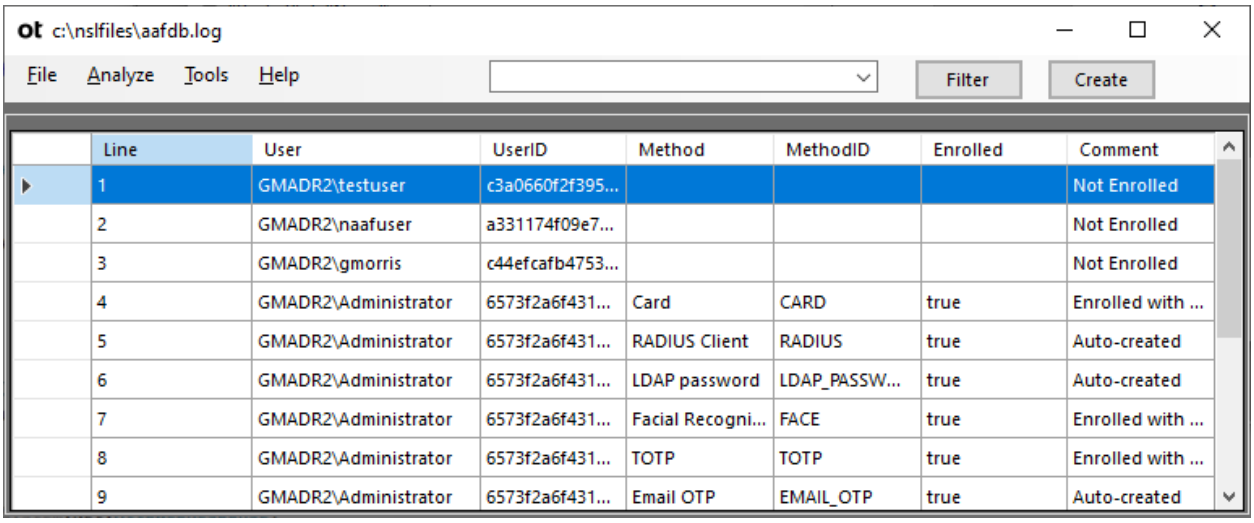
SLAnalyzer will now parse each of the users listed in the user list file and query the AAF appliance for enrollment data. The results are stored in the aafdatabase as specified above.



The aafdb database can be viewed under the File/Open menu.

(Sample content of c:\nslfiles\aafdb.db)

User:admin
UserID:36bdafe616c311e5846f000c29b9e140
Method:LDAP password
MethodID:LDAP_PASSWORD:1
Enrolled:True
Comment:

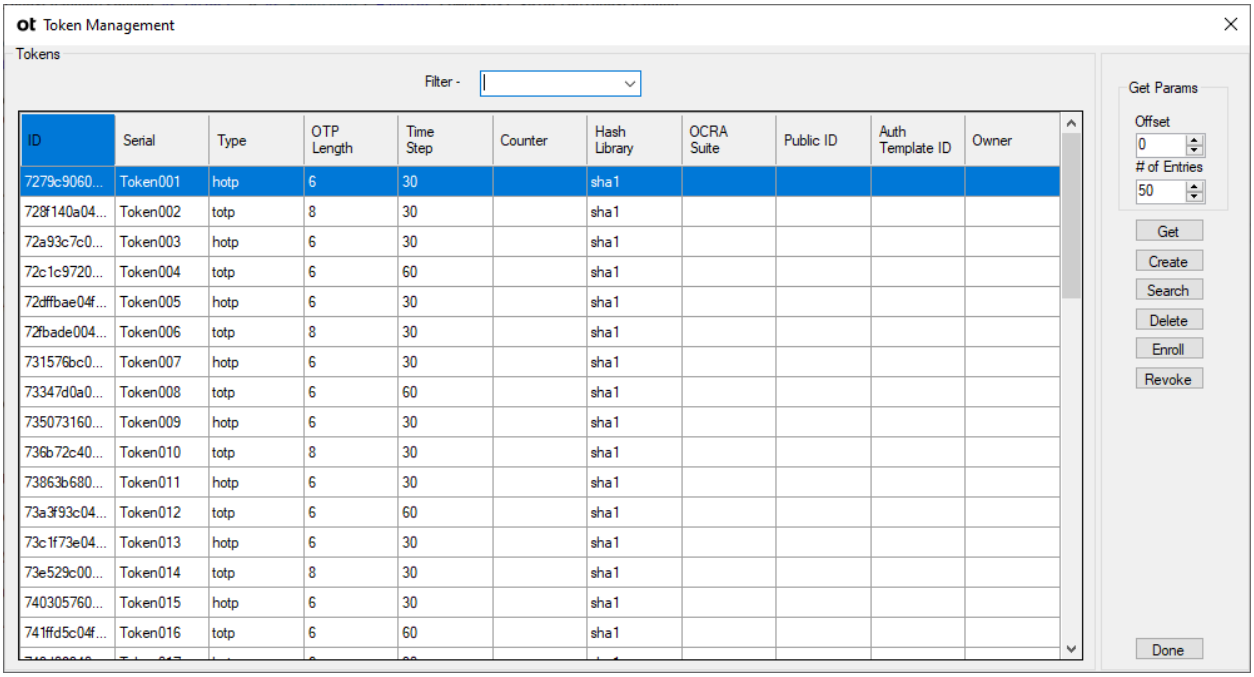


Line	User	UserID	Method	MethodID	Enrolled	Comment
1	GMADR2\testuser	c3a0660f2f395...				Not Enrolled
2	GMADR2\naafuser	a331174f09e7...				Not Enrolled
3	GMADR2\gmorris	c44efcafb4753...				Not Enrolled
4	GMADR2\Administrator	6573f2a6f431...	Card	CARD	true	Enrolled with ...
5	GMADR2\Administrator	6573f2a6f431...	RADIUS Client	RADIUS	true	Auto-created
6	GMADR2\Administrator	6573f2a6f431...	LDAP password	LDAP_PASSW...	true	Auto-created
7	GMADR2\Administrator	6573f2a6f431...	Facial Recogni...	FACE	true	Enrolled with ...
8	GMADR2\Administrator	6573f2a6f431...	TOTP	TOTP	true	Enrolled with ...
9	GMADR2\Administrator	6573f2a6f431...	Email OTP	EMAIL_OTP	true	Auto-created

User – repository \ username
UserID – AAF appliance ID for this user
Method – Method
MethodID – AAF appliance ID for this method
Enrolled – if the method is successfully enrolled. If partially enrolled but not completely enrolled then the method will show as false. Note that SLAnalyzer will only display those methods that have been either partially or completely enrolled. Other methods that are available but have not been used will not be reported.
Comment – reports any comments that are valid for the enrolled method.

Manage OTP Tokens

This option opens a new Token Manager window.



The Token Management window will display the first 50 tokens defined in the system.

Window components:

The Token management window contains the following components

- Filter box
- Token display table
- Get Params
  - Offset
  - # of Entries
- Get button
- Create button
- Search button
- Delete button
- Enroll
- Revoke

In addition to the listed components the user can right click on the list of tokens to access the context menu. This menu contains 1 option – Export List to File

Token display table

This table displays the tokens found in the system. By default, this table only lists the first 50 tokens. To display more items in the table, change the Get Params setting "# of Entries" to the desired number of tokens. After changing the Get Params setting for # of Entries, click the Get button to read the new set of tokens.

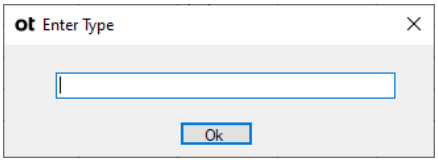
Filter box

The filter box allows the user to set a filter so that only a subset of tokens will be displayed.

Tokens can be filtered by:

- ID
- Serial
- Type
- OTP Length
- Time Step
- Counter
- Hash Lib
- OCR Suite
- Public ID
- Auth Template ID
- Owner

For example: to filter the list of tokens to only the hotp tokens, select Type in the filter box and then enter hotp when prompted.



After clicking Ok the list of tokens in the table will be filtered to only show those tokens that match the filter.

ID	Serial	Type	OTP Length	Time Step
7279c9060...	Token001	hotp	6	30
72a93c7c0...	Token003	hotp	6	30
72dffbae04f...	Token005	hotp	6	30
731576bc0...	Token007	hotp	6	30
735073160...	Token009	hotp	6	30
73863b680...	Token011	hotp	6	30
73c1f73e04...	Token013	hotp	6	30

To reset a filter, click in the filter box and select the option – None

Get Parms

Offset

By default, SLAnalyzer will read the token data from the server starting with the first token. In environments with thousands of tokens a user may want to only see a subset of tokens. Using the Offset setting tokens can be read from any starting token in the list. For example, the user could read the first 50 tokens. Then change the offset to 50 and then click the Get button to get the next 50 tokens.

# of Entries

This option will populate the token table with the number of Tokens specified. By default SLAnalyzer displays the first 50 tokens defined in the system.

Get button

The get button issues the appropriate REST call to get the list of tokens from the system. The Get Params options are used when issuing the get request to the server.

Create button

This option allows the creation of a single token entry or the use of the standard csv token file. Optionally the user can use the Token Manager page of the server to import from other token file types.

Search button

The search button allows the searching of the token database on the server for a specific token ID. The REST api for search token only allows for the searching by token id.

Delete button

The delete button allows for the deletion of one or more tokens from the server token database. For single token deletion select the token from the list in the table and then click the delete button. For multiple token deletions, first filter the list of tokens in the table to display the tokens to be deleted. Then right click in the table and select the option “Export List to File” from the context menu. Once the token list file has been created, click the delete button, when prompted select the option to delete multiple tokens from file. SLAnalyzer will then process the token list and delete each token from the token database.

Enroll button

The enroll button will enroll/assign a selected token to a specific user. Note that a single user can only have one token enrolled/assigned. After clicking the enroll button the user will be prompted to enter the name of the user to assign the selected token too.

Revoke button

This button will remove the enrollment/assignment for the selected token in the table.

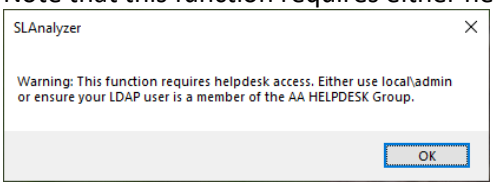
Done button

Click to close the token management window and return to the AAF Rest client window.

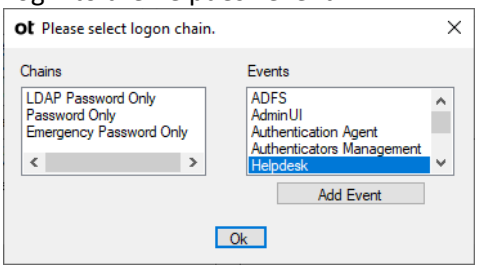
Show Shared Template Info

Advanced Authentication allows for the sharing of login information between users. This API allows the user to view the shared template information per user.

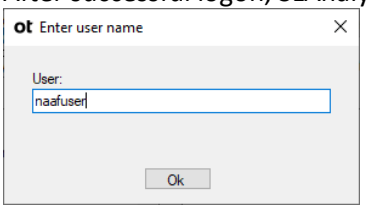
Note that this function requires either helpdesk or admin-based user access.



Login to the helpdesk event



After successful logon, SLAnalyzer will prompt for the user to display shared template information on.



The shared information is listed in the packet data window.



We can see in this example that the user naafuser is assigned the shared template for “Password” from the user GMADR2\gmorris.

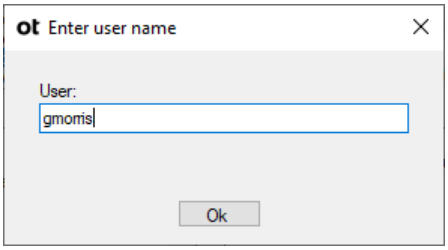
Register Method for User

This feature allows for the administrative enrollment of methods. A helpdesk or admin-based user can enroll one or more methods per user.

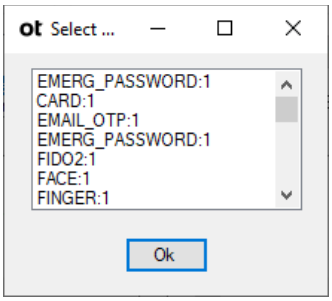
First login to the helpdesk event with a helpdesk or admin-based user.

After logon then execute “Register Method for User”

SLAnalyzer will then prompt for the user to perform the administrative enrollment for.



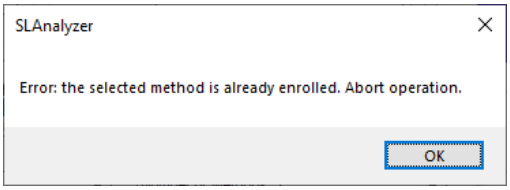
SLAnalyzer will query the AA server for the methods assigned to the administrative management event (enrollment portal).



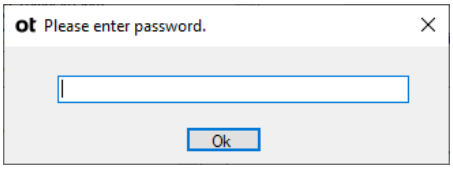
Note: Although all methods are listed it is not feasible to enroll methods where user physical devices are needed for the enrollment process. For example, an administrative user cannot enroll another users smartphone since they don’t have the physical device.

In this example the option Password:1 was selected.

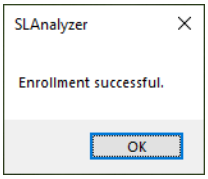
If the user already has the method enrolled, then SLAnalyzer will fail and report this error.



If the user does not have the method enrolled, then SLAnalyzer prompts for the Password:1 value.



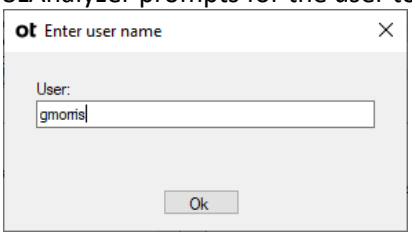
When successful SLAnalyzer will display a successful message.



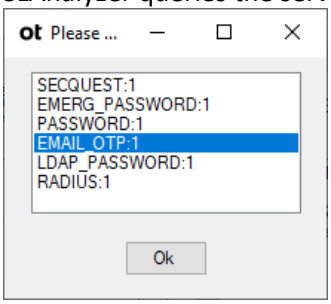
Show Override Auto Enrollment

Some methods in AA allow for an override value to be used in place of the one specified in the directory. For example, email address could be overridden with a different email address. This feature allows the administrative user to view the overridden values per user/method.

SLAnalyzer prompts for the user to display override information on.



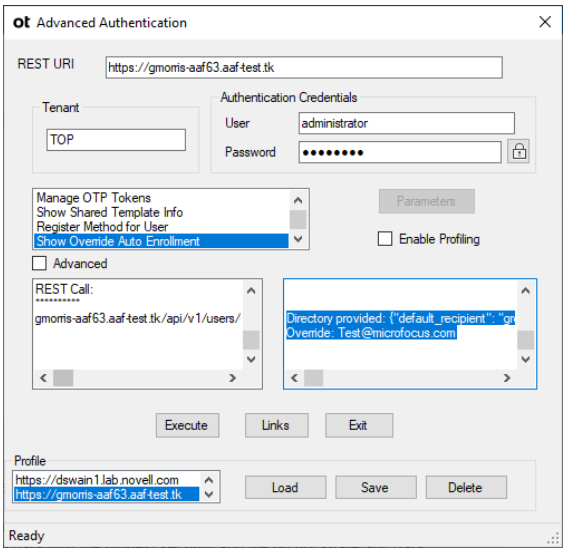
SLAnalyzer queries the server and builds a list of methods enrolled by the user specified.



Select a method and SLAnalyzer will display the override information.

Directory provided: {"default_recipient": "greg.morris@microfocus.com"}

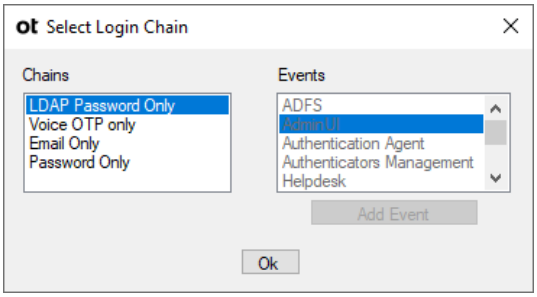
Override: Test@microfocus.com



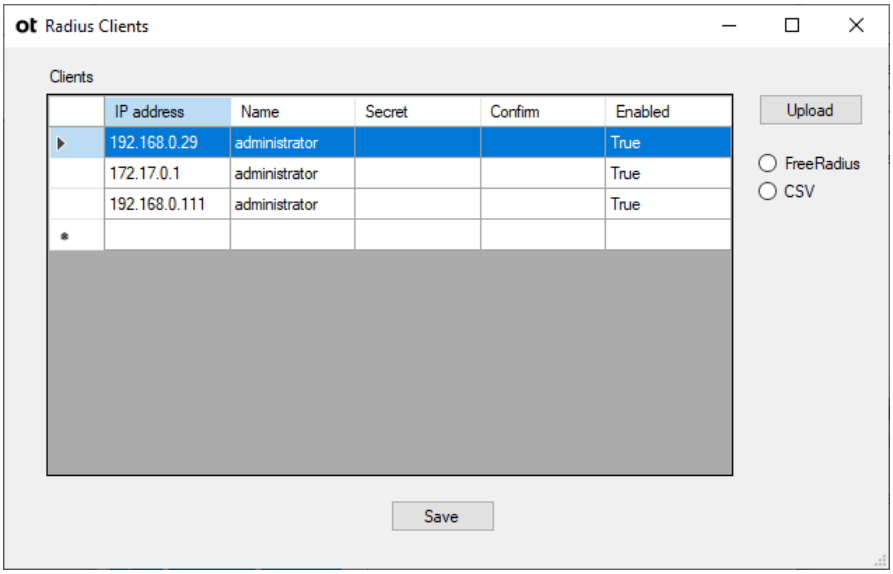
Manage Radius Clients

This option provides the ability to upload Radius client information from a file. Supported file formats include the FreeRadius clients.conf file or a comma separated value (csv) file.

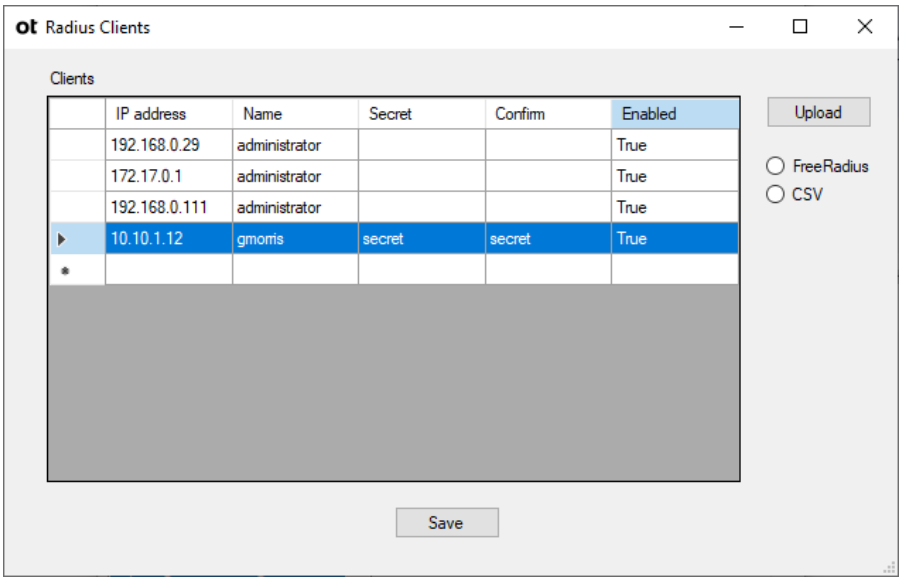
When executing this option the user is first prompted to login.



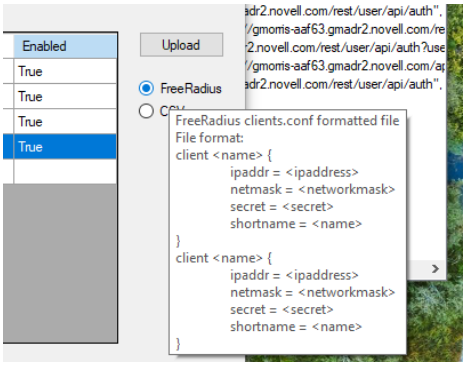
After login then the current Radius client table is displayed.



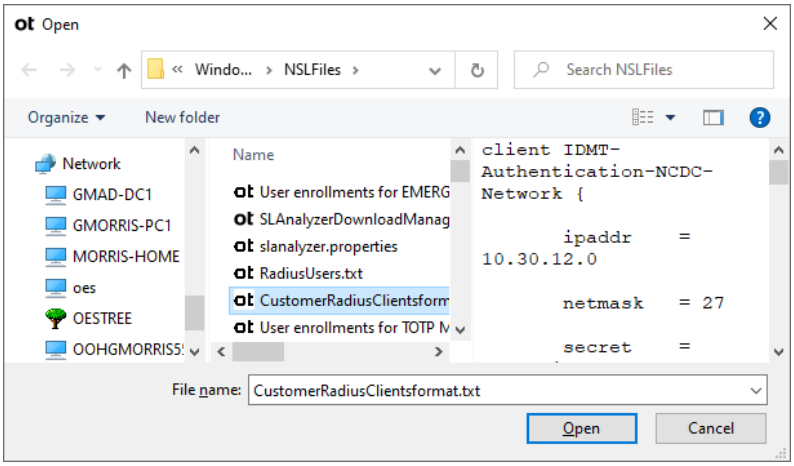
A new entry can be made in the table by selecting the fields at the end of the table. (marked with asterisk) Note that all fields are required for new entries. Existing entries do not require the Secret or confirm fields to be defined unless you want to change the value stored in the database..



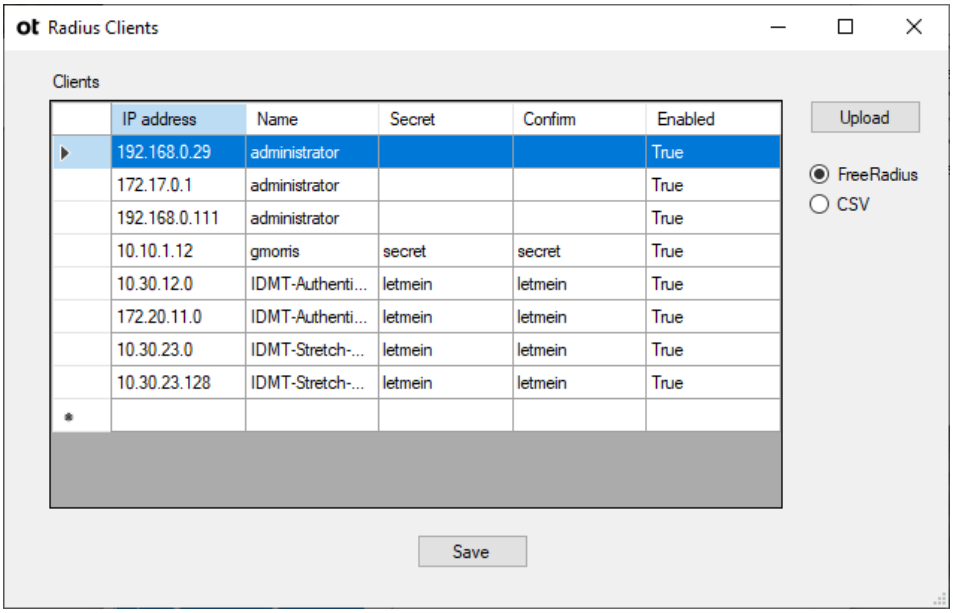
To upload from file, select either FreeRadius formatted file or CSV. Hovering the mouse over either item will display information about the file format.



Click the upload button to start the upload process.
A file dialog will be displayed to allow the user to choose the file to upload.



After the upload is completed, the table will be updated with the file information



Click the Save button to save the table to the server. To abort any changes click the X in the upper right corner of the window.

Advanced

If the user checks the checkbox labeled Advanced, then the REST command window will display all of the possible REST commands that can be sent to the appliance.

The purpose of the advanced feature is to allow for diagnostics and testing of specific functionality.

Note: All the REST calls except Register New Endpoint require an endpoint session to communicate with the AAF appliance. For this reason, when selecting any of the REST calls, SLAnalyzer will first prompt the user to select an endpoint to use for that session. Please see the REST call Create Endpoint Session for more information.

- Assign User Template
- Create Endpoint Session
- Create Event
- Create OTP Token
- Create User Template with enroll data
- Create User Template without enroll data
- Delete All Records of OSLogon Data
- Delete Event
- Delete Login Session
- Delete OTP Token
- Delete Password Record Only
- Delete User
- Delete User Template
- Destroy Endpoint
- Destroy Endpoint Session
- Destroy Enroll
- Destroy Logon Process
- Do Enroll
- Do Logon
- Do Method call
- Enroll
- Enroll new TOTP
- Enroll OTP Token
- Generate Cookie Value
- Generate Ticket Value
- Get Authentication Chains
- Get Endpoint Session Info
- Get Event by Event ID
- Get Full Server Status
- Get OTP Token
- Get OTP Tokens with Pagination
- Get Server Status
- Get User Template
- List of Events
- List of Users

- Load Chain Image
- Logon
- Logon by Basic Auth
- Logon Domains Lookup
- Logon Next
- Lookup User
- Modify User Data
- Read All Custom Messages for Category
- Read All Records of OSLogon Data
- Read Available Chains
- Read Categories
- Read Custom Messages for Category and Key
- Read Effective Policies of User
- Read Effective Policies of Endpoint
- Read Endpoint Info
- Read Info about Component of Endpoint Policy
- Read Info about Component of User Policy
- Read Login Session Information
- Register Logon Domains for the Current Tenant
- Register New Endpoint
- Remove Already Enrolled TOTP Template
- Revoke OTP Token
- Search for Endpoint
- Update Endpoint Info
- Update Event
- Update User Template
- Verify Cookie Value

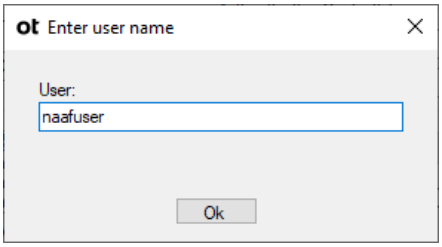
Assign User Template

This API will link a new method template to a user. Typically used during Enroll. Create the enrollment template and then link to the user.

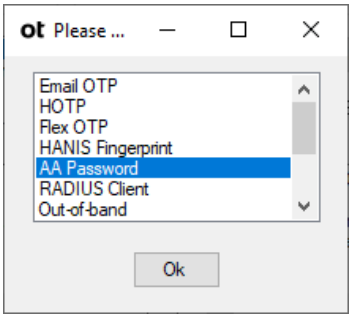
For a description of this feature see the helpdesk manual.
https://www.netiq.com/documentation/advanced-authentication-64/helpdesk-administrator-guide/data/sharing_authenticators_helpdesk.html

This API requires helpdesk/admin access.

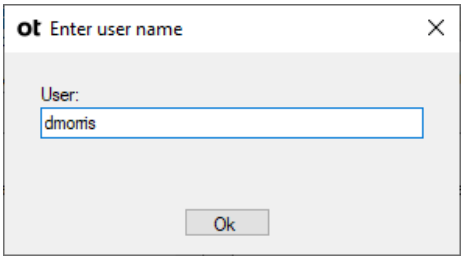
After executing this API, the user will be prompted for the name of the source user.



SLAnalyzer will now query the server for the methods enrolled by specified user.



After selecting a method to share then SLAnlyzer will prompt for the user to link too.



Once completed the packet data window will display the results.



To view the linked authenticator use the API Show Shared Template Info

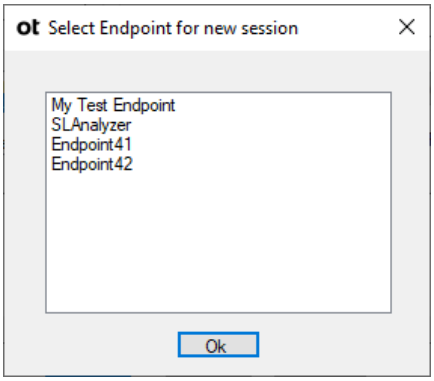
https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#user-templates-link-existing-template-to-user.-post

Create Endpoint Session

This REST call is the first REST call to be made to the appliance. Prior to communicating with an appliance, you must have an endpoint session established. This REST call creates an endpoint session.

When executing this REST call, SLAnalyzer will prompt the user to select the endpoint to use for the session. This REST call requires the endpoint session ID so SLAnalyzer will only allow the use of known and cached endpoints.

- Local Machine – Endpoint registered by the AAF Windows client
- Custom endpoints – Cached endpoints create with SLAnalyzer
- SLAnalyzer – Diagnostic endpoint
- Public endpoints – Endpoint41 and Endpoint42



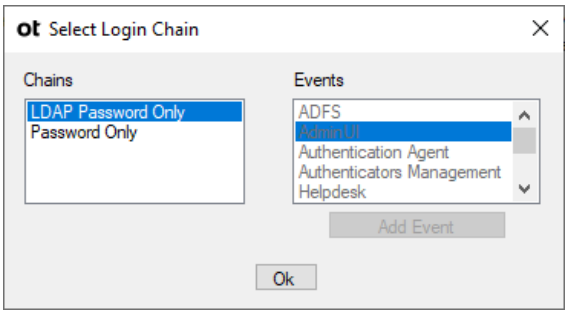
If successful, the appliance will return an endpoint session id.



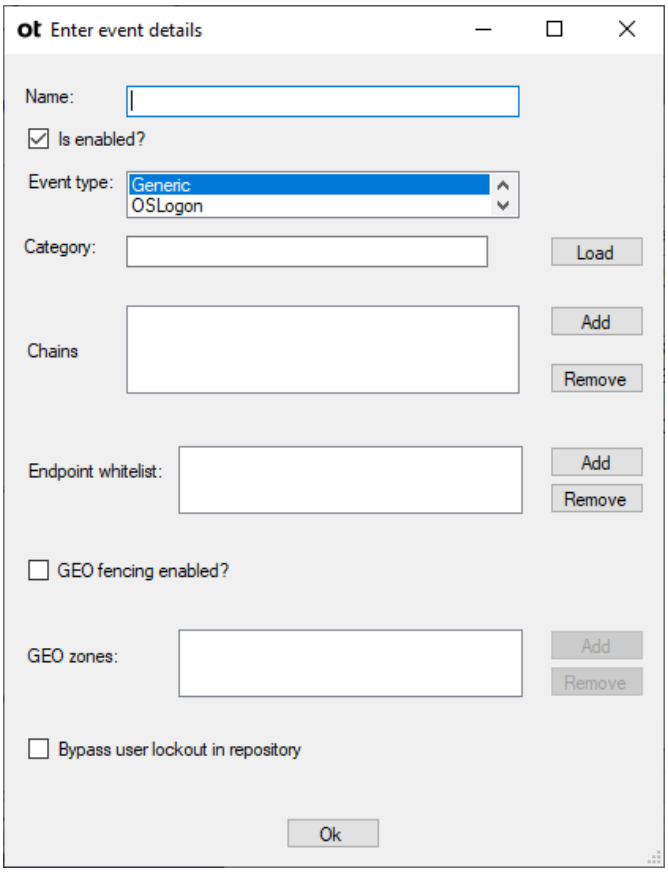
https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#endpoint-sessions-create-endpoint-session-post

Create Event

This REST call requires administrative access. When executing, SLAnalyzer will first prompt for administrative login with the AdminUI event.



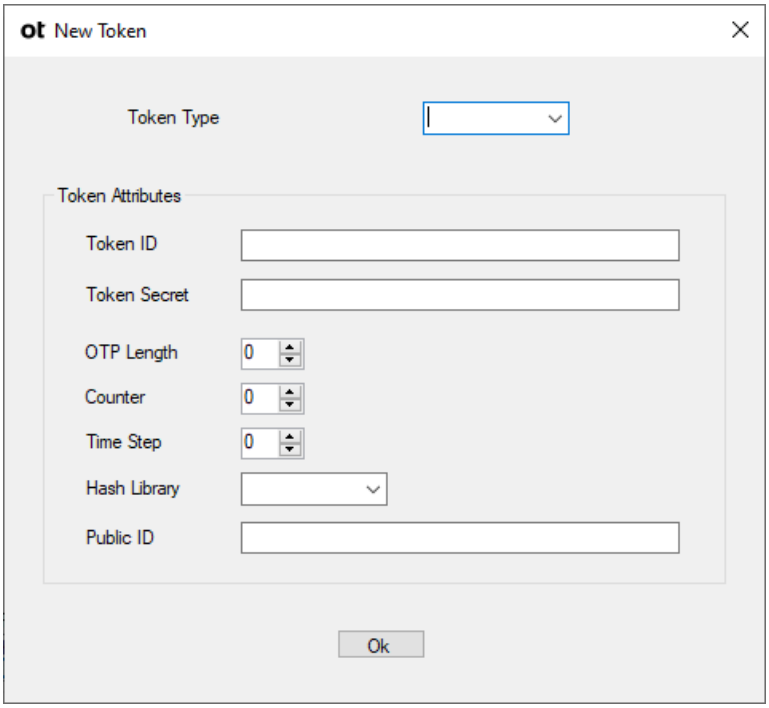
After successful login then the create event window is displayed.



Enter appropriate information for the new event and then click the OK button to create the new event.

Create OTP Token

This function will create a new token of type (hotp, pin, totp, or ocra)



Create User Template with enroll data

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#user-templates-create-template,-fill-it-from-enroll-session-and-link-to-user-post

Create User Template without enroll data

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#user-templates-create-template-without-data-and-link-to-the-user-post

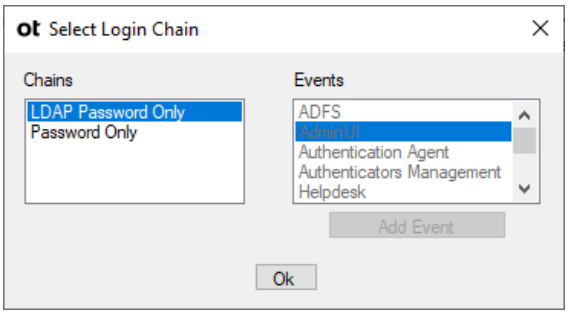
Delete All Records of OSLogon Data

This REST call will delete all of the cached OS Logon data for the currently logged in user.

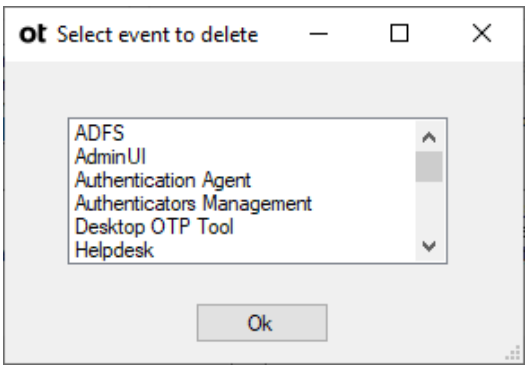
https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#user-data-delete-all-records-of-oslogon-data-delete

Delete Event

This REST call requires administrative access. When executing, SLAnalyzer will first prompt for administrative login with the AdminUI event.



After successful login then the list of current events is displayed. Select the event to delete and click the Ok button.



Delete Login Session

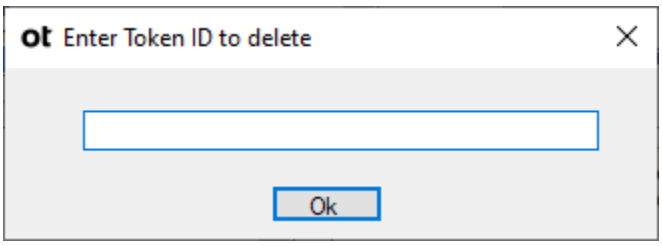
This REST call will delete the current login session (logoff).


```
  "Request": {
    "URL": "HTTP DELETE https://gmorris-aaf63.aaf-
test.tk/api/v1/logon/sessions/wTBnvGY9rTY2PhW9l1J274Bhr3zfEUQi?endpoint_session_id=4JJDyhvVeL7mBKaQYH18pRfHZfhHn
CPK",
    "header": [
      "Accept: application/json",
      "Content-Type: application/json"
    ],
    "data": null
  },
  "Reply": {
    "Status": {
      "HTTPStatus": {
        "m_Uri": "https://gmorris-aaf63.aaf-
test.tk/api/v1/logon/sessions/wTBnvGY9rTY2PhW9l1J274Bhr3zfEUQi?endpoint_session_id=4JJDyhvVeL7mBKaQYH18pRfHZfhHn
CPK",
        "m_StatusCode": 200,
        "m_ContentLength": 4,
        "m_Verb": "DELETE",
        "m_StatusDescription": "OK",
      "WebError": null,
      "AAFError": null
```


https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#login-sessions-delete-login-session-delete

Delete OTP Token

When selecting this API, SLAnalyzer will prompt the user for the Token ID to delete.



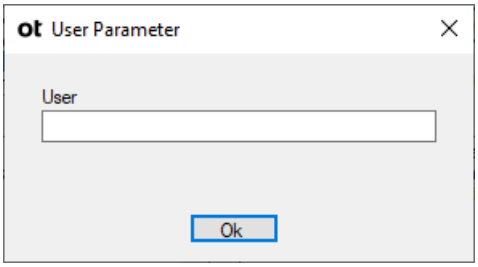
Delete Password Record Only

This REST call will delete only the password record cashed in the OS Logon data for the currently logged in user.

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#user-data-delete-password-record-only-delete

Delete User

Press the parameters button and specify the user to delete.



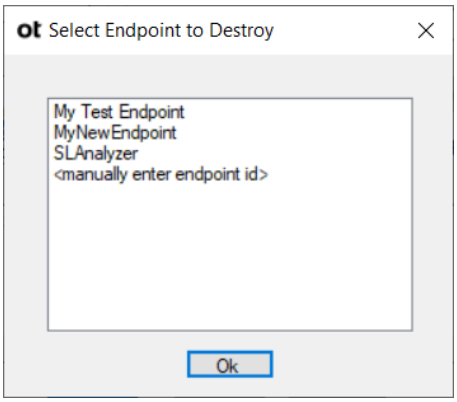
After specifying the user to delete, click the Execute button to send the request to the server.

Delete User Templatee

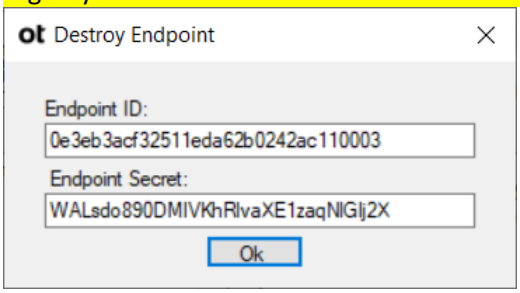
https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#user-templates-unlink-user-and-template-delete

Destroy Endpoint

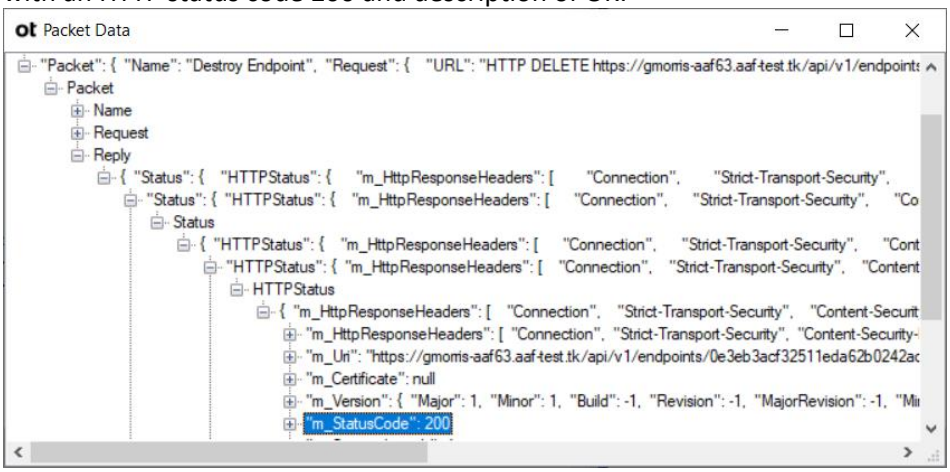
This REST call allows the deletion of an existing endpoint.



SLAnalyzer will display a list of cached endpoints to delete. After selecting the endpoint, the cached endpoint ID and secret will be displayed. Note that this REST call requires the Endpoint secret. This value is returned when registering a new endpoint. See the details of the REST call Register New Endpoint. SLAnalyzer will utilize the cached information from the Local Machine configuration file or from the local registry of the workstation. There is no other method of obtaining the secret with SLAnalyzer.



After confirming the ID and Secret SLAnalyzer sends the REST call to the server. The server responds with an HTTP status code 200 and description of OK.

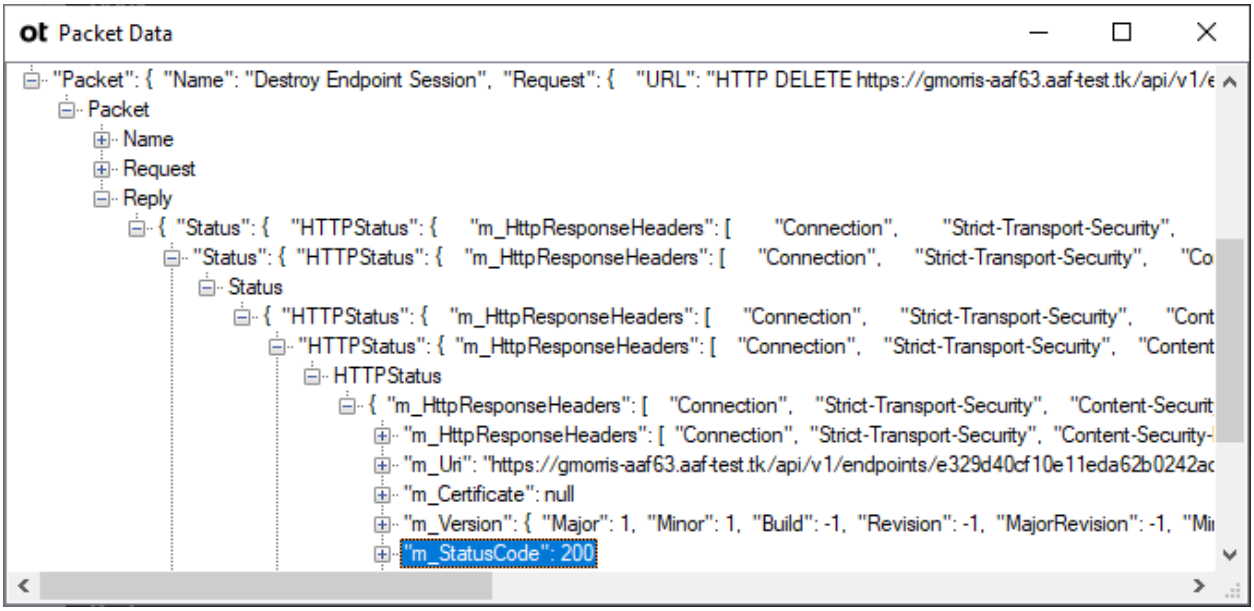


https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#endpoints-destroy-endpoint-delete

Destroy Endpoint Session

This REST call terminates the current endpoint session between SLAnalyzer and the AAF appliance.

If successful, the server will return an HTTP status of 200.



https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#endpoints-destroy-endpoint-delete

Destroy Enroll

This REST call should be used to cancel a failed enroll call.

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#enroll-destroy-pending-waiting-process-delete

Destroy Logon Process

This REST call will delete the current logon process. This call would be typically made by an application that issued the Logon REST api call but cannot complete the logon process due to some failure or user cancel. This will cleanup any server resources allocated to the current logon process.

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#logon-destroy-logon-process-delete

Do Enroll

This REST call will complete the enrollment of a specific method for the currently logged on user.

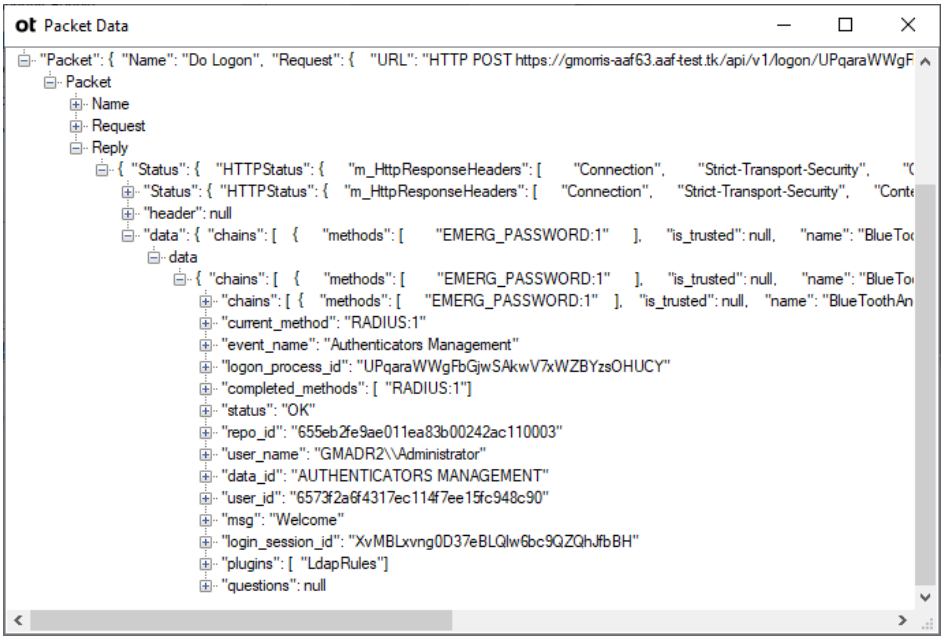

```
 "Request": {
   "URL": "HTTP POST https://gmorris-aaf63.aaf-test.tk/api/v1/enroll/oLu0JYt9rO0vKLTxzYDj9iSQR067XMoI/do_enroll",
   "header": [
     "Accept: application/json",
     "Content-Type: application/json"
   ],
   "data": "{\"response\":{\"password\":\"Password\"},\"login_session_id\":\"aNguheThvFbdMW0yoNIJRn6h30aDTdM0\"}"
 },
 "Reply": {
   "Status": {
     "HTTPStatus": {
       "m_Uri": "https://gmorris-aaf63.aaf-test.tk/api/v1/enroll/oLu0JYt9rO0vKLTxzYDj9iSQR067XMoI/do_enroll",
       "m_StatusCode": 200,
       "m_ContentLength": 68,
       "m_Verb": "POST",
       "m_StatusDescription": "OK",
     "WebError": null,
     "AAFError": null
   "data": {
     "reason": "",
     "method_id": "PASSWORD:1",
     "status": "OK",
     "msg": ""
```


https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#enroll-common-do-enroll-post

Do Logon

This REST call continues the Logon process initiated by the Logon REST call. It provides the necessary information needed to complete the logon method. For example, for the password method then this call will pass the users password.





https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#logon-common-do-logon-post

Selected Logon method for logon:

Depending on what method was selected, SLAnalyzer will possibly prompt the user for the necessary information to complete the logon process. For example, if Password was selected then SLAnalyzer will prompt the user for their password.

(TOUCHID:1) Apple Touch ID

Not currently supported by SLAnalyzer

(BANKID:1) BankID

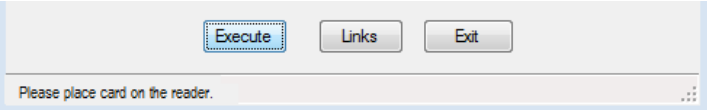
Not currently supported by SLAnalyzer

(BLUETOOTH:1) BlueTooth

This method is valid prior to AA version 6.4..
When selected, SLAnalyzer will prompt the user to select the Bluetooth device.

(CARD:1) Smart Card

The REST window status bar instructs user to insert their card into the reader.



(NEMID:1) Denmark National ID

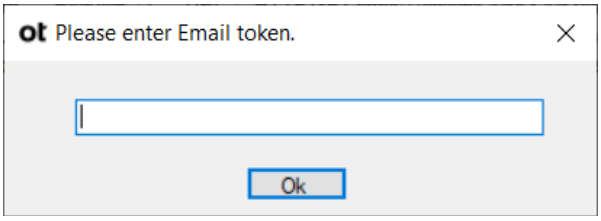
Not currently supported by SLAnalyzer

(DEVICE_AUTH:1) Device Authentication

Not currently supported by SLAnalyzer

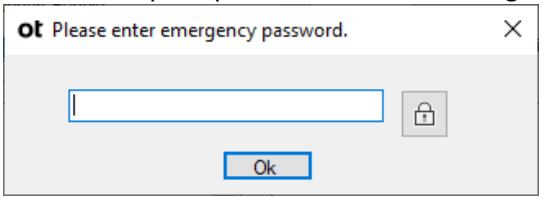
(EMAIL_OTP:1) Email OTP

SLAnalyzer will send the request to the AAF server, and it will read the email address assigned to the user in the directory or an enrolled override address. If no override address is specified and no address can be found in the directory, then the logon process will fail. Note that the override address is defined when the method is enrolled.



(EMERG_PASSWORD:1) Emergency Password

User will be prompted to enter their emergency password.



(FACE:1) Facial Recognition

Users' camera is activated, and a picture is taken. The user can select Reload to take another picture or click Accept to use the current image.

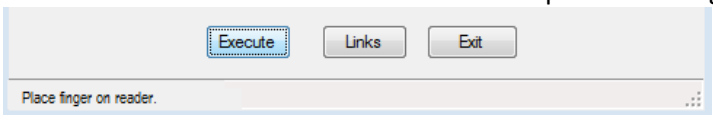


(FIDO2:1) FIDO2

Not currently supported by SLAnalyzer

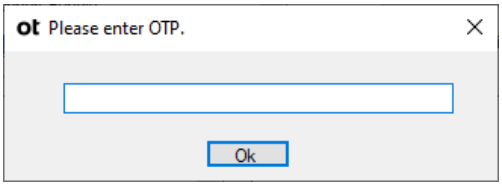
(FINGER:1) Finger Print

The REST window status bar instructs user to place their finger on the reader.



(FLEX_OTP:1) Flex OTP

This method will work with OTP, HOTP, or smartphone OTP. SLAnalyzer will prompt the user to enter the provided OTP value.



(HANIS_FACE:1) HANIS Face

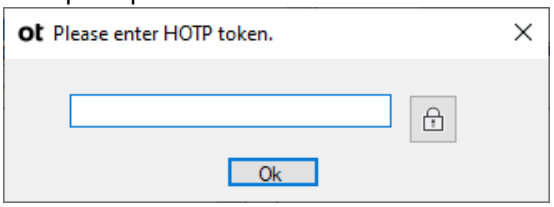
Not currently supported by SLAnalyzer

(HANIS:1) HANIS Fingerprint

Not currently supported by SLAnalyzer

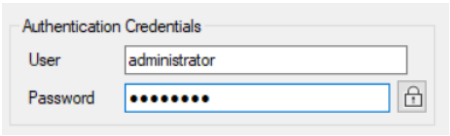
(HOTP:1) HOTP

User prompted for a token.



(LDAP_PASSWORD:1) LDAP Password

SLAnalyzer will use the password specified in the Authentication Credentials section of the REST window. Note that LDAP_PASSWORD is only valid for users in an LDAP repository. The method PASSWORD can be used for local accounts. LDAP_PASSWORD is defined in the LDAP repository. The method PASSWORD is defined in the AA database and is unique from any other password.



OATH OTP

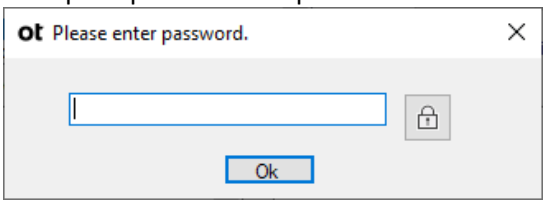
See HOTP or TOTP methods

(OOB:1) Out-of-band

Not currently supported by SLAnalyzer

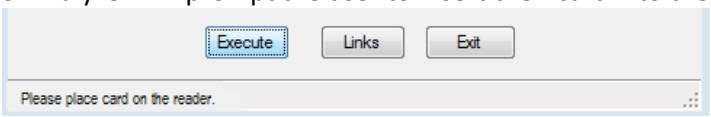
(PASSWORD:1) Password

User prompted for their password.



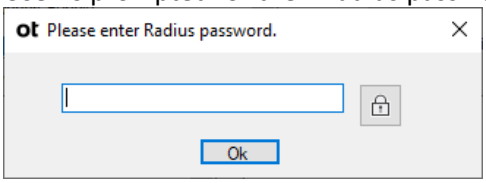
(PKI:1) PKI

SLAnalyzer will prompt the user to insert their card into the reader.



(RADIUS:1) RADIUS

User is prompted for their Radius password.

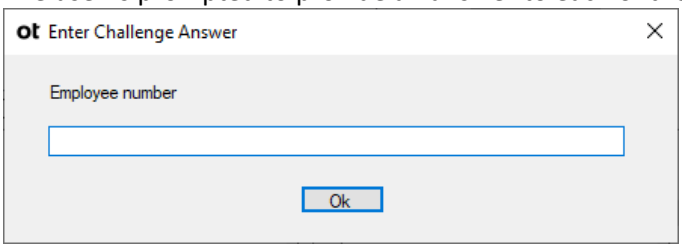


SAML Service Provider

Not currently supported by SLAnalyzer

(SECQUEST:1) Security Questions

The user is prompted to provide an answer to each of the defined security questions.

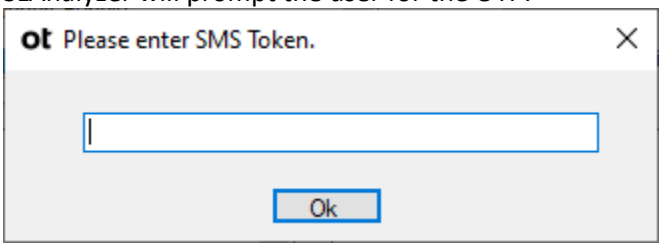


(SMARTPHONE:1) Smartphone

User is prompted on their mobile device with accept/deny.

(SMS_OTP:1) SMS OTP

The AAF server will send an SMS message to the users phone number specified when enrolled.
SLAnalyzer will prompt the user for the OTP.

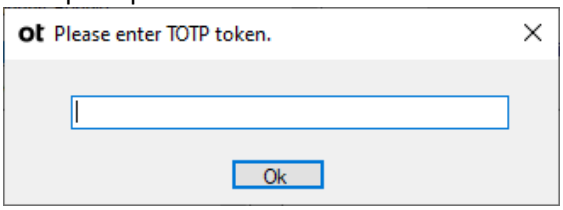


(SWISSCOM:1) Swisscom

This is always enrolled.
This method is not currently supported by SLAnalyzer.

(TOTP:1) TOTP

User prompted for an OTP.



(U2F:1) U2F

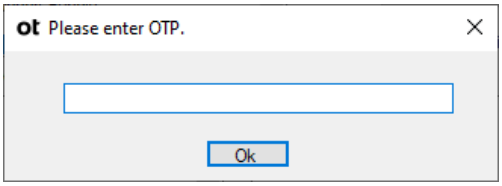
This is always enrolled.
This method is not currently supported by SLAnalyzer.

(VOICE:1) Voice

User phone number is called, and user is prompted for accept/deny.

(VOICE_OTP:1) Voice OTP

Users phone is called and message with OTP value is heard.



(WEBAUTH:1) Web Authentication

Not currently supported by SLAnalyzer

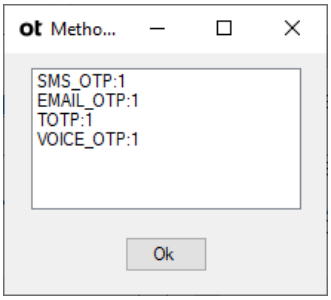
(WINHELLO:1) Windows Hello

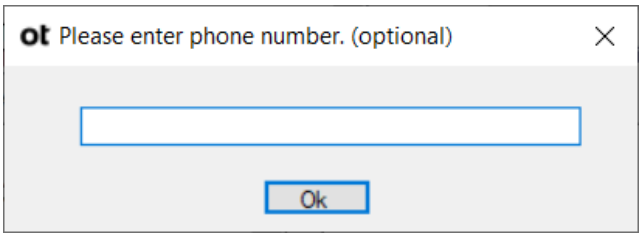
Not currently supported by SLAnalyzer

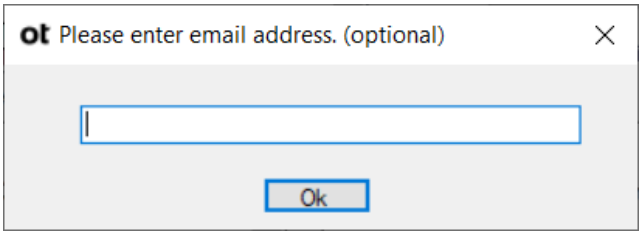
Do Method call

This REST call will generate an OTP for a specific method.
Requires an endpoint session, logon, do logon, and read logon session calls

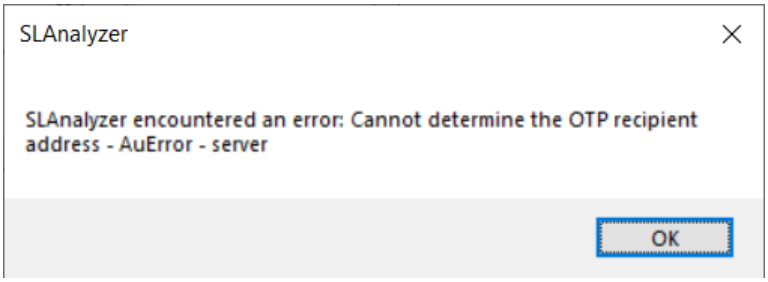
After executing the user will be prompted for the method to generate an OTP for. Note that the methods will need to be enrolled prior to execution.







If the currently logged in user does not have a phone number or email address defined in the LDAP repository, then the following error message will be displayed.



https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#methods-email_otp-1-method-call-post

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#methods-sms_otp-1-method-call-post

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#methods-voice_otp-1-method-call-post

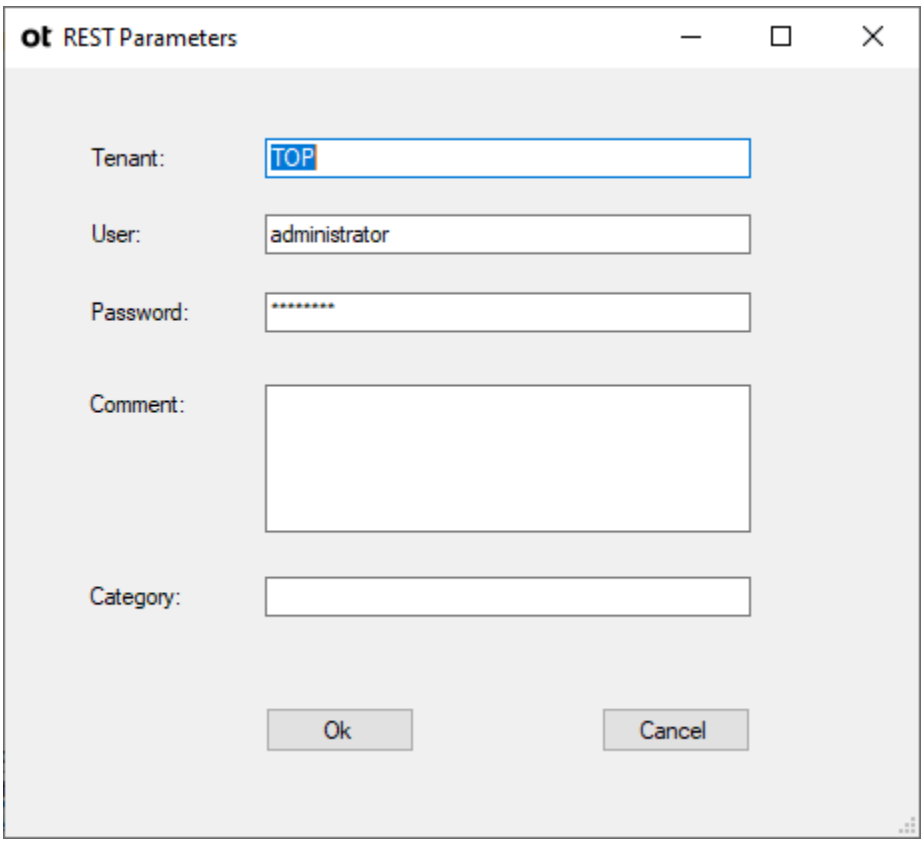
Enroll

This REST call will enroll a method for the currently logged on user. This call starts the enrollment process. To complete the enrollment of a method the Do Enroll call will need to be made.


```
"Packet": {
  "Name": "Enroll",
  "Request": {
    "URL": "HTTP POST https://gmorris-aaf63.aaf-test.tk/api/v1/enroll",
    "header": [
      "Accept: application/json",
      "Content-Type: application/json"
    ],
    "data": {
      "method_id": "PASSWORD:1",
      "login_session_id": "aNguheThvFbdMW0yoNIJRn6h30aDTdM0"
    }
  },
  "Reply": {
    "Status": {
      "HTTPStatus": {
        "m_Uri": "https://gmorris-aaf63.aaf-test.tk/api/v1/enroll",
        "m_StatusCode": 200,
        "m_ContentLength": 57,
        "m_Verb": "POST",
        "m_StatusDescription": "OK",
      "WebError": null,
      "AAFError": null
    "data": {
      "enroll_process_id": "oLu0JYt9rO0vKLTxzYDj9iSQR067XMoI"
```

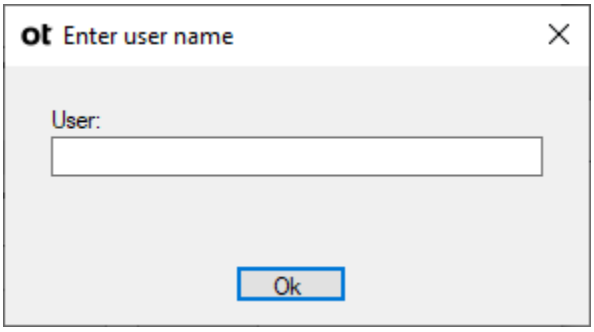

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#enroll-start-enroll-process-post

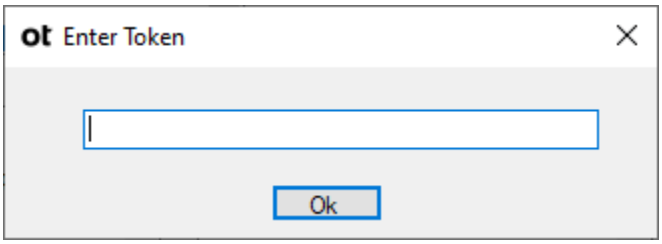
Enroll new TOTP



Enroll OTP Token

Used to assign an OTP token to a user.





Generate Cookie Value

Use login_session_id to generate cookie for this session. Will return json body with cookie_value and server_id. Server_id for single-node configuration is null.

Request

```
{
 "URL": "HTTP POST https://gmorris-aaf63.aaf-test.tk/api/v1/cookies",
 "header": [
  "Accept: application/json",
  "Content-Type: application/json"
 ],
 "data": {
  "login_session_id": "OelQ6GcJ4qNiGka3o17PauO1IT3kqrsR"
 }
}
```

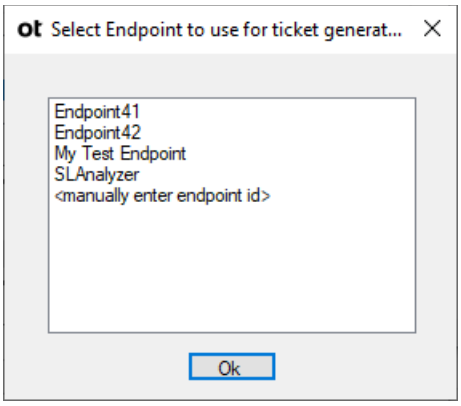
Reply

```
"data": {
 "server_id": null,
 "cookie_value": "eb7512c39c44892cb6a1e93ace61e387"
}
```

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#cookie-and-ticket-services-generate-cookie-value-post

Generate Ticket Value

Use login_session_id to generate ticket for this session. To encrypt session data, the server needs target endpoint secret to generate a ticket. Provide target_endpoint_id or target_endpoint_name. The API returns a json body with encrypted 'login_session_data'. Data is encrypted by AES with 32 bytes length key by CBC. Key is equal to target endpoint secret. Use it to decrypt data.





https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#cookie-and-ticket-services-generate-ticket-value-get

Get Authentication Chains

This REST call will get a list of authentication chains for the currently logged on user.

Requires and endpoint session, logon, do logon, and read logon session calls.

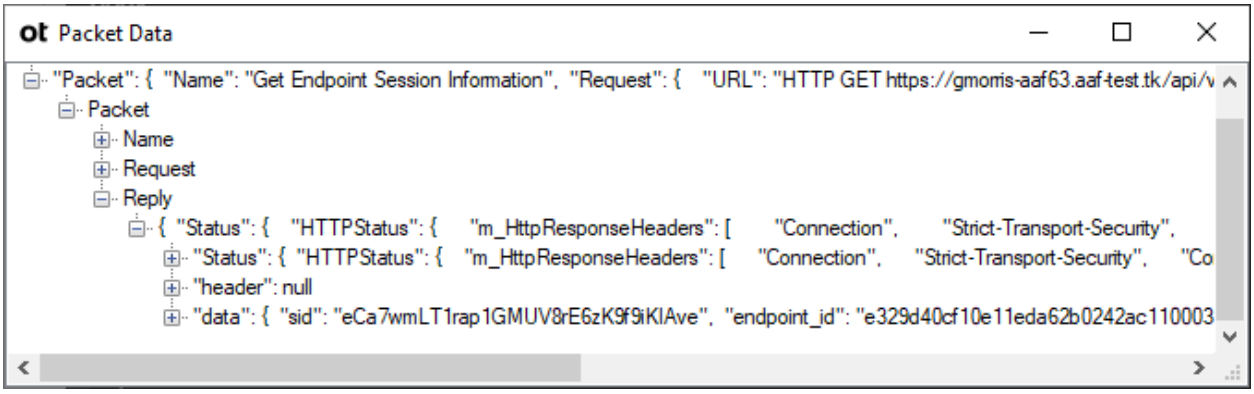

```
  "Request": {
    "URL": "HTTP GET https://gmorris-aaf63.aaf-test.tk/api/v1/logon/chains?event=Authenticators
Management&tenant_name=TOP&endpoint_session_id=4JJDyhvVeL7mBKaQYH18pRfHZfhHnCPK&is_trusted=true",
    "header": [
      "Accept: application/json",
      "Content-Type: application/json"
  "Reply": {
       "m_Uri": "https://gmorris-aaf63.aaf-test.tk/api/v1/logon/chains?event=Authenticators
Management&tenant_name=TOP&endpoint_session_id=4JJDyhvVeL7mBKaQYH18pRfHZfhHnCPK&is_trusted=true",
       "m_StatusCode": 200,
       "m_ContentLength": 2342,
       "m_Verb": "GET",
       "m_StatusDescription": "OK",
    "data": {
      "chains": [
       {
         "name": "Password Only",
         "position": 0,
         "id_hex": "28faca4696b211ea916a0242ac110003",
         "tenant_id": "def0def0def0def0def0def0def0def0",
         "id": null,
         "apply_for_ep_owner": false,
         "required_chain_id_hex": null,
         "methods": [
           "PASSWORD:1"
         ],
         "short_name": "",
         "image_name": "PASSWORD_1.png",
         "is_trusted": null,
         "is_enabled": true,
         "grace_period": null,
         "mfa_tags": [],
         "risk_level": "NONE"
       },
       {
         "name": "LDAP Password Only",
         "position": 1,
         "id_hex": "28fe1e6296b211ea916a0242ac110003",
         "tenant_id": "def0def0def0def0def0def0def0def0",
         "id": null,
         "apply_for_ep_owner": false,
         "required_chain_id_hex": null,
         "methods": [
           "LDAP_PASSWORD:1"
         ],
         "short_name": "",
         "image_name": "LDAP_PASSWORD_1.png",
         "is_trusted": null,
         "is_enabled": true,
         "grace_period": null,
         "mfa_tags": [],
         "risk_level": "NONE"
       },
       {
         "name": "passwordAndEmergency",
         "position": 2,
         "id_hex": "2a42c2d0db7211ecb3260242ac110004",
         "tenant_id": "def0def0def0def0def0def0def0def0",
         "id": null,
         "apply_for_ep_owner": false,
         "required_chain_id_hex": null,
         "methods": [
           "EMERG_PASSWORD:1",
```

```
    "PASSWORD:1"
   ],
   "short_name": "",
   "image_name": "default",
   "is_trusted": null,
   "is_enabled": true,
   "grace_period": null,
   "mfa_tags": [],
   "risk_level": "NONE"
  },
  {
   "name": "LDAPAndEmergency",
   "position": 3,
   "id_hex": "365bcfcedb7411ecb3260242ac110004",
   "tenant_id": "def0def0def0def0def0def0def0def0",
   "id": null,
   "apply_for_ep_owner": false,
   "required_chain_id_hex": null,
   "methods": [
    "LDAP_PASSWORD:1",
    "EMERG_PASSWORD:1"
   ],
   "short_name": "",
   "image_name": "default",
   "is_trusted": null,
   "is_enabled": true,
   "grace_period": null,
   "mfa_tags": [],
   "risk_level": "NONE"
  },
  {
   "name": "smartphone only",
   "position": 4,
   "id_hex": "6f32250a9ae411eab6be0242ac110003",
   "tenant_id": "def0def0def0def0def0def0def0def0",
   "id": null,
   "apply_for_ep_owner": false,
   "required_chain_id_hex": null,
   "methods": [
    "SMARTPHONE:1"
   ],
   "short_name": "",
   "image_name": "SMARTPHONE_1.png",
   "is_trusted": null,
   "is_enabled": true,
   "grace_period": null,
   "mfa_tags": [],
   "risk_level": "NONE"
  },
  {
   "name": "bluetooth only",
   "position": 5,
   "id_hex": "7e33c0e09ae411eab6be0242ac110003",
   "tenant_id": "def0def0def0def0def0def0def0def0",
   "id": null,
   "apply_for_ep_owner": false,
   "required_chain_id_hex": null,
   "methods": [
    "BLUETOOTH:1"
   ],
   "short_name": "",
   "image_name": "BLUETOOTH_1.png",
   "is_trusted": null,
   "is_enabled": true,
   "grace_period": null,
   "mfa_tags": [],
   "risk_level": "NONE"
```

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#logon-read-available-chains-get

Get Endpoint Session Info

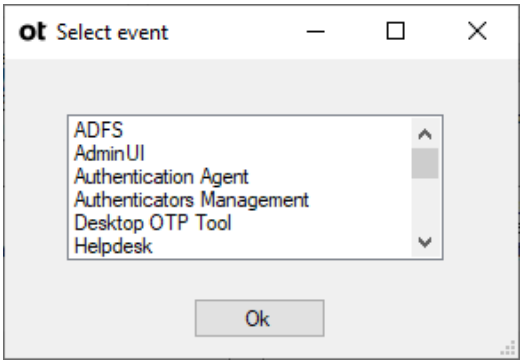
Get Endpoint Session Info reads the current endpoint session data.



https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#endpoint-sessions-read-information-about-endpoint-session-get

Get Event by Event ID

Reads the detail information about the selected Event.



Request:
{
"URL": "HTTP GET https://gmorris-aaf63.aaf-test.tk/api/v1/events/4025e590f8af11eda4140242ac110004?login_session_id=X8REMFPanYZaC5bQNGw5pONhNgbhEsJc",
"header": [
"Accept: application/json",
"Content-Type: application/json"
]
}

Reply
"data": {
"type": "Generic",
"endpoints": [],
"chains": [
{
"name": "LDAP Password Only",
"position": 0,
"id_hex": null,
"tenant_id": null,
"id": "28fe1e6296b211ea916a0242ac110003",
"apply_for_ep_owner": false,
"required_chain_id_hex": null,
"methods": [
"LDAP_PASSWORD:1"
],
"short_name": "",
"image_name": "LDAP_PASSWORD_1.png",
"is_trusted": null,
"is_enabled": true,
"grace_period": null,
"mfa_tags": null,
"risk_level": "NONE",
"app_name": null
},
{
"name": "Password Only",
"position": 0,
"id_hex": null,
"tenant_id": null,
"id": "28faca4696b211ea916a0242ac110003",
"apply_for_ep_owner": false,
"required_chain_id_hex": null,
"methods": [

```
      "PASSWORD:1"
    ],
    "short_name": "",
    "image_name": "PASSWORD_1.png",
    "is_trusted": null,
    "is_enabled": true,
    "grace_period": null,
    "mfa_tags": null,
    "risk_level": "NONE",
    "app_name": null
   },
   {
    "name": "LDAP + Smartphone",
    "position": 0,
    "id_hex": null,
    "tenant_id": null,
    "id": "a1a2526cef7311eda6d10242ac110003",
    "apply_for_ep_owner": false,
    "required_chain_id_hex": null,
    "methods": [
     "LDAP_PASSWORD:1",
     "SMARTPHONE:1"
    ],
    "short_name": "",
    "image_name": "default",
    "is_trusted": null,
    "is_enabled": true,
    "grace_period": null,
    "mfa_tags": null,
    "risk_level": "NONE",
    "app_name": null
   },
   {
    "name": "Voice OTP only",
    "position": 0,
    "id_hex": null,
    "tenant_id": null,
    "id": "14eec870646611eda4980242ac110003",
    "apply_for_ep_owner": false,
    "required_chain_id_hex": null,
    "methods": [
     "VOICE_OTP:1"
    ],
    "short_name": "",
    "image_name": "VOICE_OTP_1.png",
    "is_trusted": null,
    "is_enabled": true,
    "grace_period": null,
    "mfa_tags": null,
    "risk_level": "NONE",
    "app_name": null
   }
  ],
  "is_enabled": true,
  "json_data": {
   "oauth2_appid": null,
   "oauth2_appsecret": null,
   "oauth2_redir_uris": null,
   "nas_id": null,
   "clients": null,
   "groups_enabled": false,
   "groups_white_list": null,
   "saml2_metadata": null,
   "saml_send_email_as_nameid": false,
   "ignore_user_lockout": false
  },
```

```
 "is_standard": true,
 "is_geo_fencing_enabled": "false",
 "category_id": null,
 "geo_zones": [],
 "id": "28fa393c96b211ea916a0242ac110003",
 "name": "AdminUI",
 "forced": "false"
}
```


https://www.netiq.com/documentation/advanced-authentication-64/apidoc/data/apidoc.html#events-get-event-by-event-id-get

Get Full Server Status

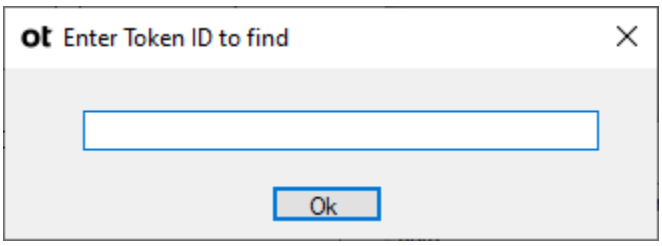
Reads the full status of the server…

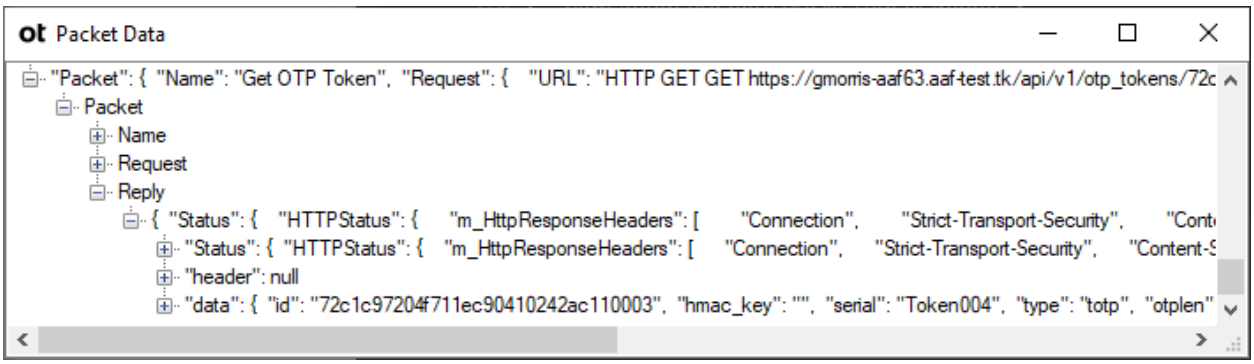
{"status": "OK", "multitenancy_mode": false, "version": "6.4.1.1-237", "hosted_saas_mode": false, "fips_mode": true}

https://www.netiq.com/documentation/advanced-authentication-64/apidoc/data/apidoc.html#server-status-read-exact-server-version,-check-license,-fips-mode-state-post

Get OTP Token

Gets the details about a token.



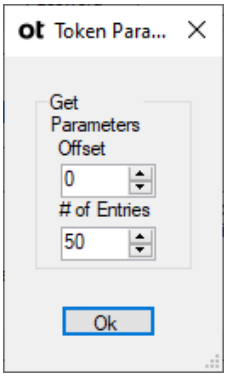


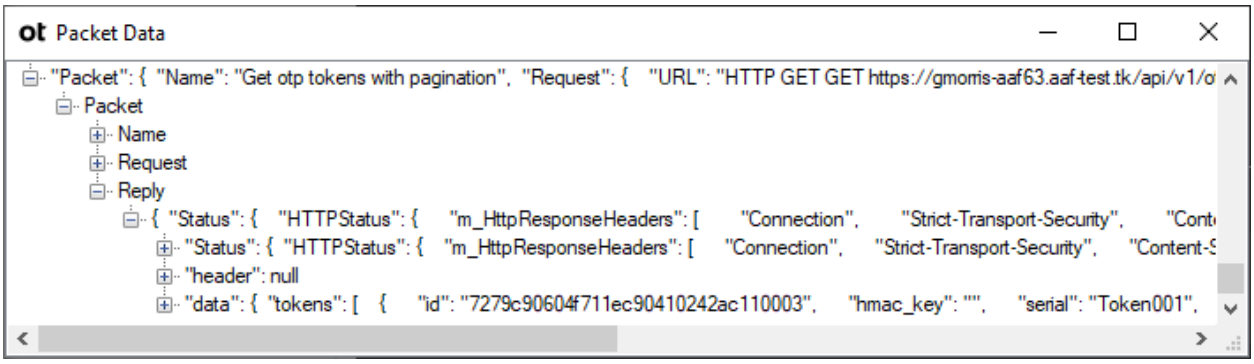
https://www.netiq.com/documentation/advanced-authentication-64/apidoc/data/apidoc.html#otp-tokens-get-otp-token-get

Get OTP Tokens with Pagenation

The API retrieves a block of tokens.

Click on the parameters button to specify the start of the search and the size of the block to return.





https://www.netiq.com/documentation/advanced-authentication-64/apidoc/data/apidoc.html#otp-tokens-get-otp-tokens-with-pagination-get

Get Server Status

This API returns the basic server status. This API is like the Get Full Server Status API.

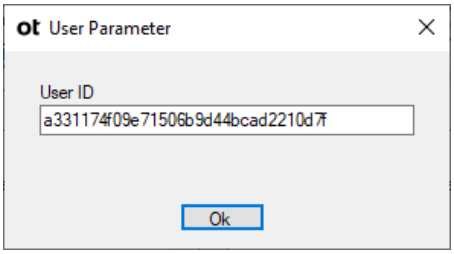
{"status": "OK", "multitenancy_mode": false, "version": "6.4.1.1", "hosted_saas_mode": false}

https://www.netiq.com/documentation/advanced-authentication-64/apidoc/data/apidoc.html#server-status-get-server-status-and-version-get

Get User Templatee

This API will return user registered methods (templates)

Click the parameters button and enter the user ID to return registration information.



Request:
{
"URL": "HTTP GET
https://aaf64gm.gmadr2.novell.com/api/v1/users/b1b28d320766981b65b625c2e8d01446/templates?login_session_id=twKserv9DojgwceQfZgH75IWGdpB3VbR",
"header": [
"Accept: application/json",
"Content-Type: application/json"
],
"data": null
}
Reply:
"data": {
"templates": [
{
"id": "ba3a2aa4e00405bcae0989f1bc012865",
"method_id": "PASSWORD:1",
"is_enrolled": "true",
"method_title": "Password",
"comment": "Enrolled with SLAnalyzer",
"category_id": "",
"data": {
"password_changed_at": "2023-06-12T13:21:05.386252",
"password_must_be_changed": false,
"pin_changed_at": null,
"mobile_phone": null,
"start_dt": null,
"end_dt": null,
"max_logon_count": null,
"name": null,
"hash": null,
"email": null
}
},
{
"id": "81b57dee3db7290deb35ea6f43c75337",
"method_id": "PASSWORD:1",
"is_enrolled": "true",
"method_title": "Password",
"comment": "Enrolled with SLAnalyzer",
"category_id": "3938f7ce092411ee9fcb0242ac110003",
"data": {
"password_changed_at": "2023-06-12T13:25:18.284076",
"password_must_be_changed": false,
"pin_changed_at": null,
"mobile_phone": null,
"start_dt": null,
"end_dt": null,

```
      "max_logon_count": null,
      "name": null,
      "hash": null,
      "email": null
    }
   },
   {
    "id": "c941157ecf196e62519173a7207d4acb",
    "method_id": "LDAP_PASSWORD:1",
    "is_enrolled": "true",
    "method_title": "LDAP password",
    "comment": "Auto-created",
    "category_id": "",
    "data": {
      "password_changed_at": null,
      "password_must_be_changed": false,
      "pin_changed_at": null,
      "mobile_phone": null,
      "start_dt": null,
      "end_dt": null,
      "max_logon_count": null,
      "name": null,
      "hash": null,
      "email": null
    }
   },
   {
    "id": "7ee95ba481be89a1a6643bfffaf88733",
    "method_id": "PASSWORD:1",
    "is_enrolled": "true",
    "method_title": "Password",
    "comment": "Enrolled with SLAnalyzer",
    "category_id": "360b59a2092411ee9fcb0242ac110003",
    "data": {
      "password_changed_at": "2023-06-12T13:24:51.270313",
      "password_must_be_changed": false,
      "pin_changed_at": null,
      "mobile_phone": null,
      "start_dt": null,
      "end_dt": null,
      "max_logon_count": null,
      "name": null,
      "hash": null,
      "email": null
    }
   }
  ]
}
```


https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#user-templates-list-of-user-s-linked-templates-get

List of Events

This API returns the current list of events. AdminUi access is required for this API.

REST Call:
****
gmorris-aaf63.aaf-test.tk/api/v1/events?login_session_id=GMTeRjMWZRJQf1JFKGck4K01mSHrr5NA
****
Response from: List of Events
****
HTTP Status code: OK
Event: ADFS
Event: AdminUI
Event: Authentication Agent
Event: Authenticators Management
Event: Desktop OTP Tool
Event: Helpdesk
Event: Helpdesk user
Event: Linux logon
Event: Mac OS logon
Event: Mainframe Logon
Event: My SAML
Event: MyOauthEvent
Event: NAM
Event: NCA
Event: OOB UI logon
Event: Radius Server
Event: Reflection
Event: Report logon
Event: SSPR45
Event: Search Card
Event: Smartphone Enrollment
Event: Tokens Management
Event: Windows logon

https://www.netiq.com/documentation/advanced-authentication-64/apidoc/data/apidoc.html#events-list-of-events-get

List of Users

LOCAL repo - all local users. LDAP repo - users listed in server database - those who tried to authenticate at least once.

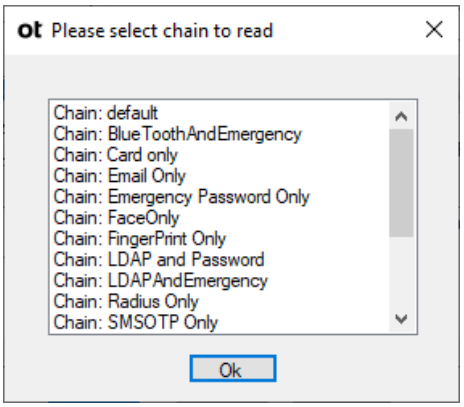
See the automated function for List of Users

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#users-list-of-users-get

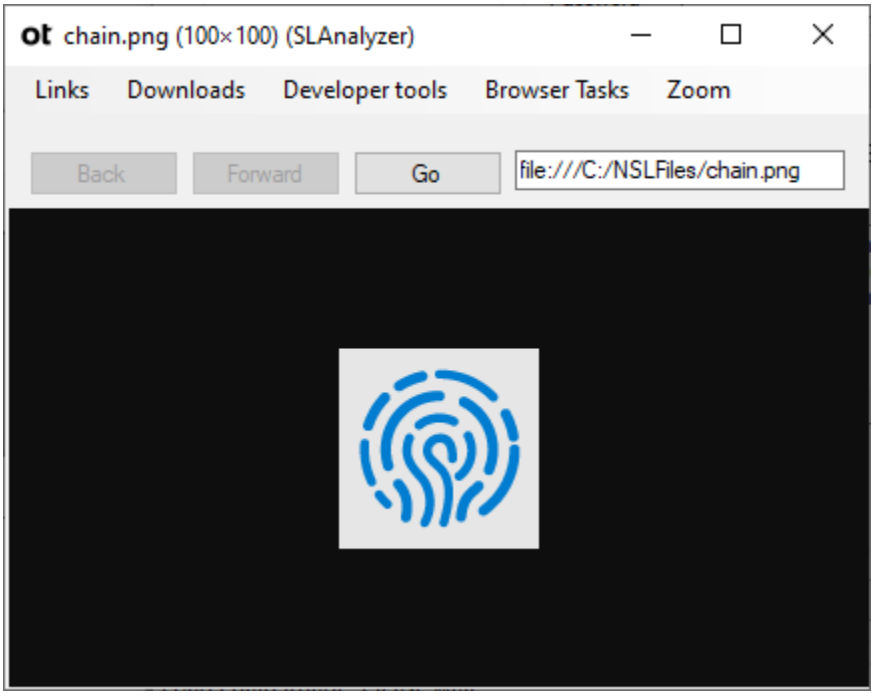
Load Chain Image

This API returns the image associated with a logon chain.

Select the desired chain:



After clicking the Ok button SLAnalyzer will display the image in a browser window.

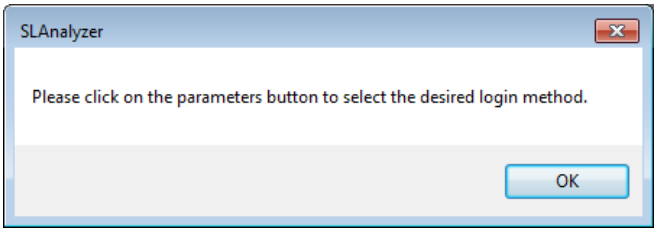


https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#chain-image-load-chain-image-get

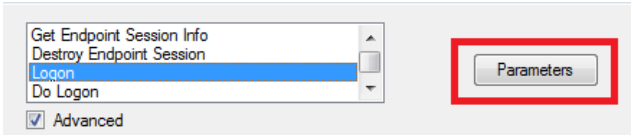
Logon

This REST call initiates the Logon process.

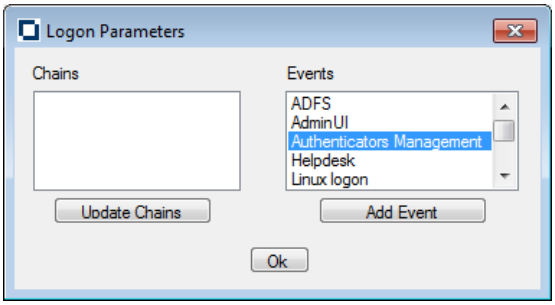
This REST call requires a logon chain. If you click the Execute button without specifying a logon chain SLAnalyzer will display this error:



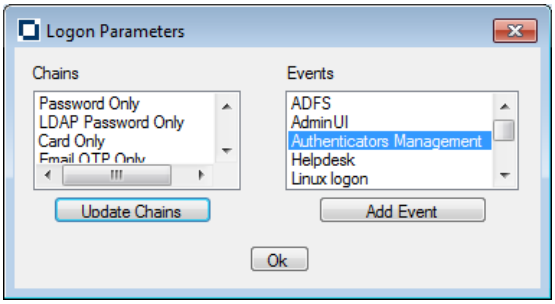
When selecting this REST call the Parameters button becomes available.



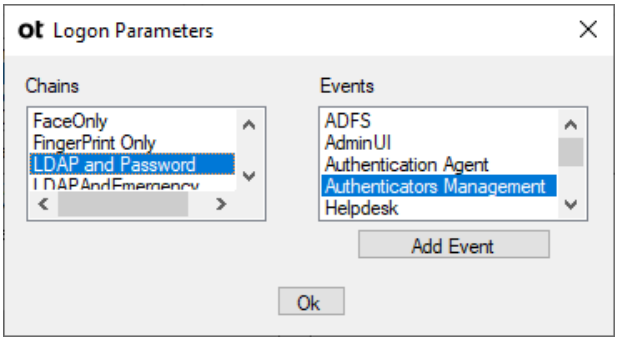
Click the Parameters button to choose the Logon chain to be used for this logon.



Choose the desired Event and then click the Update Chains button.
Note that SLAnalyzer will issue a Get Authentication Chains REST call to read the available chains for the selected Event.

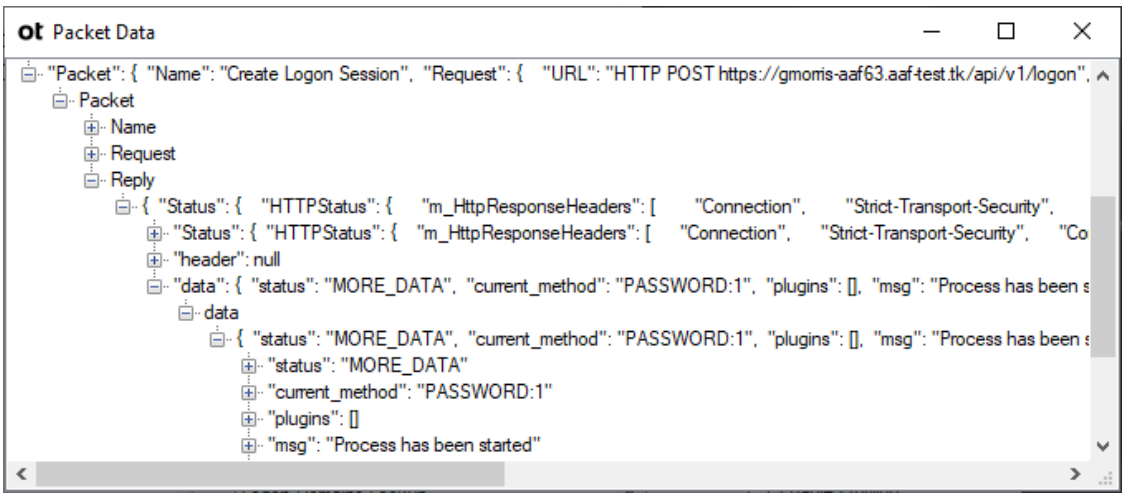


Select the desired Logon chain and then the Ok button to return to the main REST window.



After selecting the logon chain click the Execute button to submit the Logon REST call.

The server should respond with MORE_DATA and Process started.



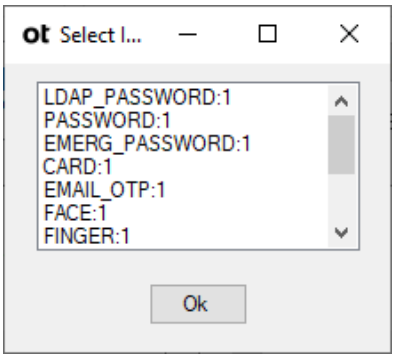
This is only the first part of the Logon process. To continue the logon, you must select the REST call Do Logon.

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#logon-create-logon-process-post

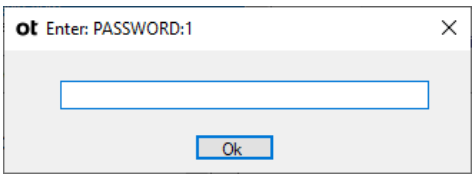
Logon by Basic Auth

This API allows for the login to the enrollment portal through basic authentication.

When selecting this API the user is first prompted for the logon method to use for basic auth. This method needs to be a text based method.. for example LDAP_PASSWORD, PASSWORD, HOTP, EMERGENCY_PASSWORD, etc… Methods that require user interaction will not work since the method data must be passed with the logon request.



After selecting the desired method then the user is prompted for the method data to pass. If the user selected LDAP_PASSWORD then the password from the Authentication Credentials section of the REST window will be used. All other methods will prompt for input.

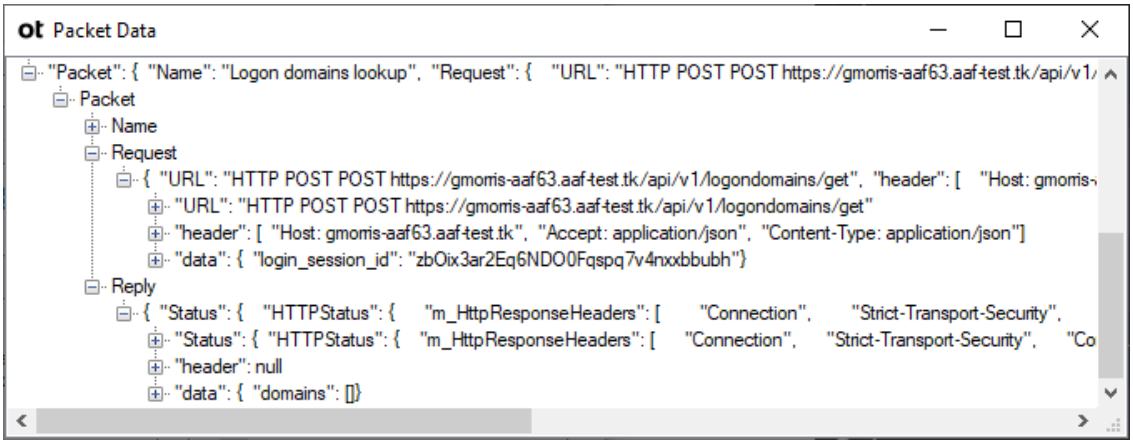


REST Call:
****
gmorris-aaf63.aaf-test.tk/account/basic
****
Response from: Logon by Basic Authentication
****
HTTP Status code: OK

https://www.netiq.com/documentation/advanced-authentication-64/apidoc/data/apidoc.html#logon-by-basic-auth-to-account

Logon Domains Lookup

Read any existing logon domains

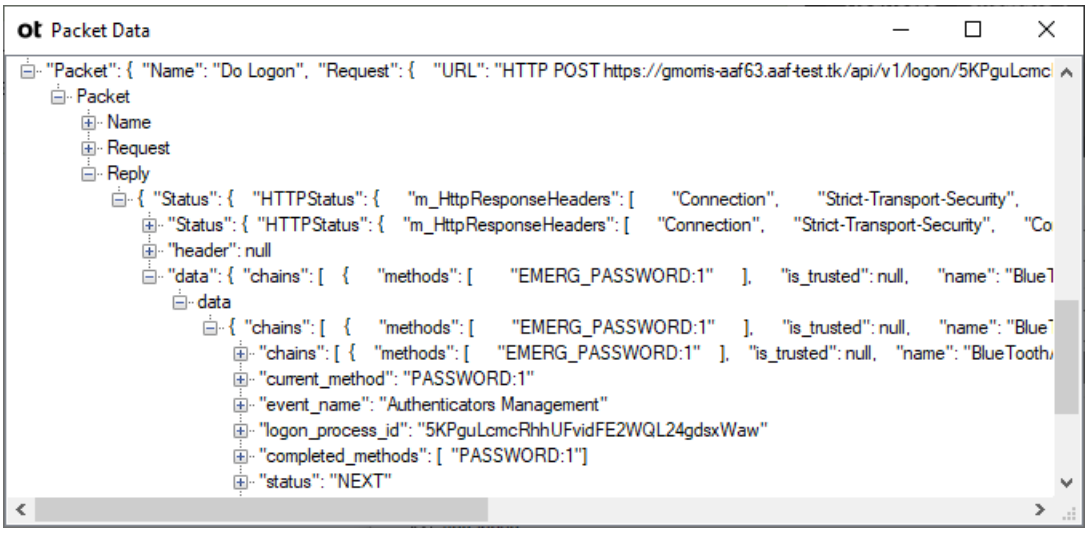


https://www.netiq.com/documentation/advanced-authentication-64/apidoc/data/apidoc.html#logon-domains-associated-with-this-tenant-logon-domains-lookup-post

Logon Next

The REST call will initate the next method in the login chain.

If the selected chain has more than one method defined, then the AA server will return a status of NEXT in response to the Do Logon REST call.



By issuing the Logon Next call we will proceed to the next method in the logon chain.

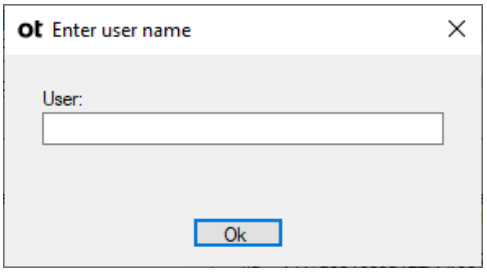


The next step would be to issue the Do Logon request again to process the next method.

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#logon-continue-logon-for-multiple-step-logon-post

Lookup User

When executing this API, the user will be prompted for the username to lookup.

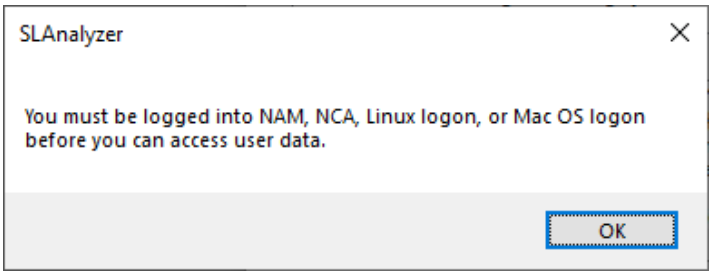


https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#users-user-lookup-by-given-user-name-get

Modify User Data

User data is stored on specific events. This will include NAM, NCA, Linux Logon, or Mac OS Logon. Before selecting this option login to one of the supported events.

If the user is not logged into one of the supported events, the following message is displayed.



When logged into one of the supported events, the data below will be written:

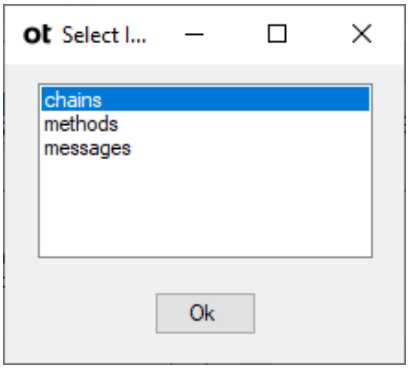
{"data":{"test1":"value 1","test2":"value 2","test3":"value 3"},"login_session_id":"M8aOSkpBfycXGxpUZ3hAcvnr5iqTjDdr"}

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#user-data-modify-data-patch

Read All Custom Messages for Category

This API will return the defined custom messages for chains, methods, or messages.

When executing this API, the user is presented with a list of categories.



https://www.netiq.com/documentation/advanced-authentication-64/apidoc/data/apidoc.html#custom-messages-read-all-custom-messages-for-category-get

Read All Records of OSLogon Data

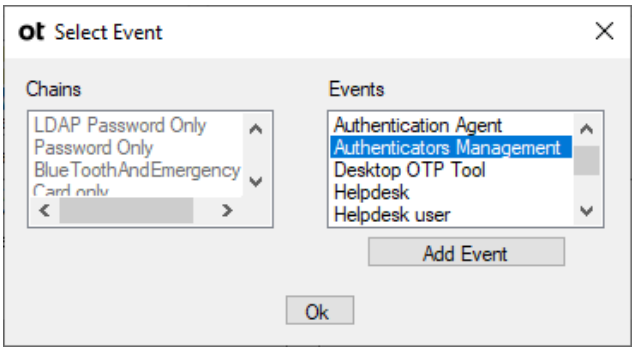
This REST call will read the OS Logon information for the currently logged on user. The user must be logged into a valid OS event.. For example Linux Logon, Mac OS Logon, etc.

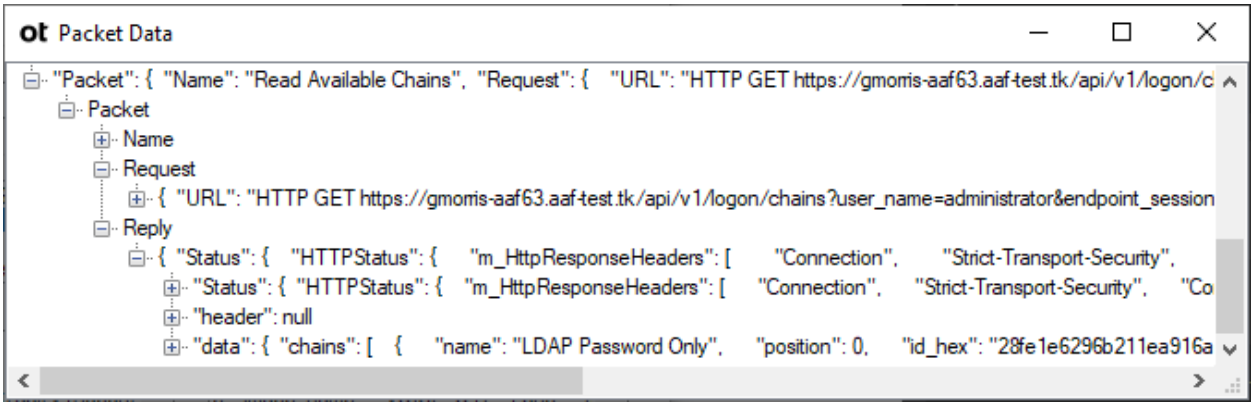

```
  "Request": {
    "URL": "HTTP GET https://gmorris-aaf63.aaf-
test.tk/api/v1/users/6573f2a6f4317ec114f7ee15fc948c90/data/OSLogon?login_session_id=lSmxBrS7bLM8Fb8WV9lU172Dzmjdd17
j",
    "header": [
      "Accept: application/json",
      "Content-Type: application/json"
    ],
    "data": null
  },
  "Reply": {
    "Status": {
      "HTTPStatus": {
        "m_Uri": "https://gmorris-aaf63.aaf-
test.tk/api/v1/users/6573f2a6f4317ec114f7ee15fc948c90/data/OSLogon?login_session_id=lSmxBrS7bLM8Fb8WV9lU172Dzmjdd17
j",
        "m_StatusCode": 200,
        "m_ContentLength": 34,
        "m_Verb": "GET",
        "m_StatusDescription": "OK",
      "WebError": null,
      "AAFError": null
      }
    "data": "{\"data\": {\"password\": \"Password\"}}"
```


https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#user-data-read-all-records-of-oslogon-data-get

Read Available Chains

This API returns all chains defined in the server. When selected the user will be prompted to select the event to display the defined chains for that event.



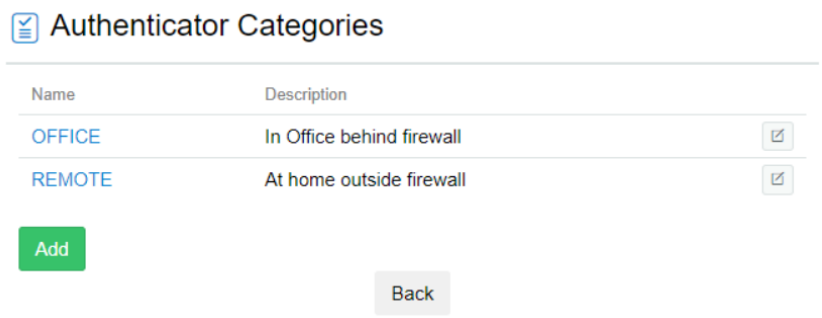


Read Categories

This API will return a list of the configured template categories.

For information about categories see…
https://www.netiq.com/documentation/advanced-authentication-64/server-administrator-guide/data/evnt_catgrs.html

Define categories in the admin portal under Policies->Event Categories



Returned categories as seen in the Packet data window.

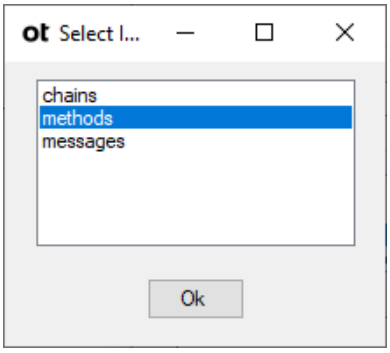


https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#template-categories-read-categories-get

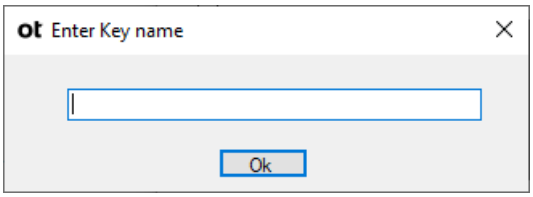
Read Custom Messages for Category and Key

This API is like the API [Read All Custom Message for Categories]

The user is first prompted to select the desired category.



The user is then prompted for the key.



Read Effective Policies of User

This REST call reads the effective policies for the currently logged in user.


```
  "Request": {
    "URL": "HTTP GET https://gmorris-aaf63.aaf-
test.tk/api/v1/users/6573f2a6f4317ec114f7ee15fc948c90/effective_policy?login_session_id=DUt81BG34sHSCBu2ibn9Hn6zGAQ1T
O9Z",
    "header": [
      "Accept: application/json",
      "Content-Type: application/json"
  "Reply": {
    "Status": {
      "HTTPStatus": {
        "m_Uri": "https://gmorris-aaf63.aaf-
test.tk/api/v1/users/6573f2a6f4317ec114f7ee15fc948c90/effective_policy?login_session_id=DUt81BG34sHSCBu2ibn9Hn6zGAQ1T
O9Z",
        "m_StatusCode": 200,
        "m_ContentLength": 25695,
        "m_Verb": "GET",
        "m_StatusDescription": "OK",
      "WebError": null,
      "AAFError": null
    "data": {
      "policy": {
        "FingerMethod": {
          "data": {
            "threshhold": 0,
            "captures_number_per_finger": 3,
            "fingers_number": 2
          },
          "component_id": "FingerMethod"
        },
        "BluetoothMethod": {
          "data": {
            "watch_on_device_removal": true
          },
          "component_id": "BluetoothMethod"
        },
        "EmailOTPMethod": {
          "data": {
            "html": "<!DOCTYPE html>\n<title>OTP</title>\n<body>Use OTP <b>{otp}</b>, #{number} to login as {user} from {endpoint}
to {event}</body>",
            "subject": "Login OTP",
            "body": "Use OTP {otp}, #{number} to login as {user} from {endpoint} to {event}",
            "otp_format": "dec6",
            "email_format": "text",
            "otp_period": 120,
            "max_sent_otp_count": 0,
            "sender_email": null
          },
          "component_id": "EmailOTPMethod"
        },
        "SwisscomMethod": {
          "data": {
            "cert_password": null,
            "mid_url": "https://mobileid.swisscom.com/rest/service",
            "certificate": null,
            "ap_pwd": null,
            "ap_id": "",
            "msg_prefix": ""
          },
          "component_id": "SwisscomMethod"
        },
        "PKIMethod": {
          "data": {
            "data": null
          },
          "component_id": "PKIMethod"
        },
```

```
"VoiceSender": {
  "data": {
    "enroll_no_phone_msg": null,
    "twilio": {
      "account_sid": "AC1c83adb864001816c51548a5e6aee77f",
      "sender_phone": "+18012511344",
      "public_server_url": null,
      "auth_token": null,
      "use_copilot": false,
      "service_sid": null
    },
    "enroll_no_phone": false
  },
  "component_id": "VoiceSender"
},
"CacheOptions": {
  "data": {
    "cache_enabled": true
  },
  "component_id": "CacheOptions"
},
"DeleteMeOptions": {
  "data": {
    "delete_me_enabled": true
  },
  "component_id": "DeleteMeOptions"
},
"LockoutOptions": {
  "data": {
    "failed_attempts": 3,
    "lock_in_repo": false,
    "lockout_period": 300,
    "is_enabled": false
  },
  "component_id": "LockoutOptions"
},
"ADPasswordFilter": {
  "data": {
    "update_on_change": true,
    "update_on_reset": true
  },
  "component_id": "ADPasswordFilter"
},
"SmartphoneMethod": {
  "data": {
    "server_url": null,
    "auth_salt_ttl": 60,
    "push_proxy_url": "https://proxy.authasas.com/OobProxy/servicejson.svc",
    "vendor": "NetIQ",
    "totp_step": 30,
    "google_project_id": null,
    "totp_length": 6,
    "push_salt_ttl": 30,
    "learn_timeout": 60,
    "totp_time_window": 300
  },
  "component_id": "SmartphoneMethod"
},
"U2fMethod": {
  "data": {
    "disable_builtin_attestation_cert": false,
    "check_attestation": false
  },
  "component_id": "U2fMethod"
},
"SyslogOptions": {
  "data": {
    "port": 514,
    "host": "syslog.server.ip",
    "is_enabled": true,
```

```
    "socktype": "UDP"
  },
  "component_id": "SyslogOptions"
},
"ServicesDirectorOptions": null,
"KerberosOptions": {
  "data": {
    "sso_repo_id": null
  },
  "component_id": "KerberosOptions"
},
"EndpointManOptions": {
  "data": {
    "create_need_auth": false
  },
  "component_id": "EndpointManOptions"
},
"HelpdeskOptions": {
  "data": {
    "require_user_credentials": false
  },
  "component_id": "HelpdeskOptions"
},
"MultitenancyOptions": {
  "data": {
    "multitenancy_enabled": false
  },
  "component_id": "MultitenancyOptions"
},
"GeoFencingOptions": {
  "data": {
    "geo_fencing_enabled": false
  },
  "component_id": "GeoFencingOptions"
},
"Saml2Options": null,
"TOTPMethod": {
  "data": {
    "otp_period": 30,
    "otp_window": 4,
    "otp_format": "dec6",
    "use_key_uri_format_qr": false
  },
  "component_id": "TOTPMethod"
},
"SmartcardMethod": {
  "data": {
    "tap_and_go_enabled": false
  },
  "component_id": "SmartcardMethod"
},
"RadiusMethod": {
  "data": {
    "send_reponame": false,
    "nas_identifier": "001",
    "server": "gmorris-aaf63.aaf-test.tk",
    "secret": null,
    "authport": 1812
  },
  "component_id": "RadiusMethod"
},
"EMERG_PASSWORD": {
  "data": {
    "password_min_length": 5,
    "password_age": 0,
    "allow_change": true,
    "password_check_complexity": false,
    "max_logon_count": 10
  },
  "component_id": "EMERG_PASSWORD"
```

```
},
"SMSOTPMethod": {
  "data": {
    "otp_period": 120,
    "max_sent_otp_count": 0,
    "body": "Use OTP {otp}, #{number} to login as {user} from {endpoint} to {event}",
    "otp_format": "dec6",
    "recipient_attr": null
  },
  "component_id": "SMSOTPMethod"
},
"WhitelistAdminUIOptions": null,
"VoiceMethod": {
  "data": {
    "pin_min_length": 3,
    "recipient_attr": null,
    "pin_max_age": 42
  },
  "component_id": "VoiceMethod"
},
"SMSSender": {
  "data": {
    "sender_service": "twilio",
    "twilio": {
      "account_sid": "AC1c83adb864001816c51548a5e6aee77f",
      "sender_phone": "+18012511344",
      "public_server_url": null,
      "auth_token": null,
      "use_copilot": false,
      "service_sid": ""
    },
    "is_debug": false,
    "generic": {
      "request_body": [],
      "request_method": "POST",
      "service_url": "",
      "auth_password": null,
      "request_body_secure_params": [],
      "auth_username": ""
    },
    "messagebird": {
      "password": null,
      "sender_name": "",
      "username": ""
    }
  },
  "component_id": "SMSSender"
},
"LoginOptions": {
  "data": {
    "default_repos": [
      "LOCAL",
      "GMADR2",
      "OES"
    ],
    "nondefault_repos": []
  },
  "component_id": "LoginOptions"
},
"VoiceOTPMethod": {
  "data": {
    "otp_period": 120,
    "max_sent_otp_count": 0,
    "body": "OTP #{number}: Your OTP code is {otp}",
    "otp_format": "dec4",
    "recipient_attr": null
  },
  "component_id": "VoiceOTPMethod"
},
"MailSender": {
```

```
  "data": {
    "tls": false,
    "sendmail_template": null,
    "debug": 0,
    "port": "25",
    "ssl": false,
    "username": "root",
    "default_sender": "systemuser@local.com",
    "host": "localhost",
    "keyfile": null,
    "sendmail_app": null,
    "password": null,
    "certfile": null,
    "queue_path": null
  },
  "component_id": "MailSender"
},
"SecQuestMethod": {
  "data": {
    "MinAnswerLength": 1,
    "TotalQuestionsForLogon": 5,
    "CorrectQuestionsForLogon": 5,
    "AllQuestions": {
      "AllQuestionsData": null
    }
  },
  "component_id": "SecQuestMethod"
},
"LogoOptions": {
  "data": {
    "use_mobile_image": false,
    "url": null,
    "logo_mobile_start": null,
    "use_image": true,
    "logo_mini": null,
    "text": null,
    "logo_mobile_about": null,
    "logo_lg": null
  },
  "component_id": "LogoOptions"
},
"LastLogonTrackingOptions": null,
"TemplateOptions": {
  "data": {
    "disable_reenrollment": false,
    "sharing_enabled": true
  },
  "component_id": "TemplateOptions"
},
"ADEnhancedFilter": {
  "data": {
    "filter_enabled": false
  },
  "component_id": "ADEnhancedFilter"
},
"LdapMethod": {
  "data": {
    "save_password": true
  },
  "component_id": "LdapMethod"
},
"HOTPMethod": {
  "data": {
    "otp_window": 10,
    "otp_format": "dec6"
  },
  "component_id": "HOTPMethod"
},
"HttpsOptions": {
  "data": {
```

```
      "tls_1_0_enabled": false,
      "compression_enabled": false
    },
    "component_id": "HttpsOptions"
  },
  "PasswordMethod": {
    "data": {
      "password_min_length": 5,
      "rename_to_pin": false,
      "password_check_complexity": false,
      "password_max_age": 42
    },
    "component_id": "PasswordMethod"
```


https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#policies-read-effective-policies-of-user-get

Read Effective Policies of Endpoint

This REST call will read the effective policies for the current endpoint session.


```
  "Request": {
    "URL": "HTTP GET https://gmorris-aaf63.aaf-
test.tk/api/v1/endpoints/42424242424242424242424242424242/effective_policy?endpoint_session_id=cuhezieObg7VoDin1iYIqxy
Wxpg8GqNV",
    "header": [
      "Accept: application/json",
      "Content-Type: application/json"
    "Reply": {
    "Status": {
      "HTTPStatus": {
        "m_Uri": "https://gmorris-aaf63.aaf-
test.tk/api/v1/endpoints/42424242424242424242424242424242/effective_policy?endpoint_session_id=cuhezieObg7VoDin1iYIqxy
Wxpg8GqNV",
        "m_StatusCode": 200,
        "m_ContentLength": 25695,
        "m_Verb": "GET",
        "m_StatusDescription": "OK",
      "WebError": null,
      "AAFError": null
    "data": {
      "policy": {
        "FingerMethod": {
          "data": {
            "threshhold": 0,
            "captures_number_per_finger": 3,
            "fingers_number": 2
          },
          "component_id": "FingerMethod"
        },
        "BluetoothMethod": {
          "data": {
            "watch_on_device_removal": true
          },
          "component_id": "BluetoothMethod"
        },
        "EmailOTPMethod": {
          "data": {
            "html": "<!DOCTYPE html>\n<title>OTP</title>\n<body>Use OTP <b>{otp}</b>, #{number} to login as {user} from {endpoint}
to {event}</body>",
            "subject": "Login OTP",
            "body": "Use OTP {otp}, #{number} to login as {user} from {endpoint} to {event}",
            "otp_format": "dec6",
            "email_format": "text",
            "otp_period": 120,
            "max_sent_otp_count": 0,
            "sender_email": null
          },
          "component_id": "EmailOTPMethod"
        },
        "SwisscomMethod": {
          "data": {
            "cert_password": null,
            "mid_url": "https://mobileid.swisscom.com/rest/service",
            "certificate": null,
            "ap_pwd": null,
            "ap_id": "",
            "msg_prefix": ""
          },
          "component_id": "SwisscomMethod"
        },
        "PKIMethod": {
          "data": {
            "data": null
          },
          "component_id": "PKIMethod"
        },
```

```
"VoiceSender": {
  "data": {
    "enroll_no_phone_msg": null,
    "twilio": {
      "account_sid": "AC1c83adb864001816c51548a5e6aee77f",
      "sender_phone": "+18012511344",
      "public_server_url": null,
      "auth_token": null,
      "use_copilot": false,
      "service_sid": null
    },
    "enroll_no_phone": false
  },
  "component_id": "VoiceSender"
},
"CacheOptions": {
  "data": {
    "cache_enabled": true
  },
  "component_id": "CacheOptions"
},
"DeleteMeOptions": {
  "data": {
    "delete_me_enabled": true
  },
  "component_id": "DeleteMeOptions"
},
"LockoutOptions": {
  "data": {
    "failed_attempts": 3,
    "lock_in_repo": false,
    "lockout_period": 300,
    "is_enabled": false
  },
  "component_id": "LockoutOptions"
},
"ADPasswordFilter": {
  "data": {
    "update_on_change": true,
    "update_on_reset": true
  },
  "component_id": "ADPasswordFilter"
},
"SmartphoneMethod": {
  "data": {
    "server_url": null,
    "auth_salt_ttl": 60,
    "push_proxy_url": "https://proxy.authasas.com/OobProxy/servicejson.svc",
    "vendor": "NetIQ",
    "totp_step": 30,
    "google_project_id": null,
    "totp_length": 6,
    "push_salt_ttl": 30,
    "learn_timeout": 60,
    "totp_time_window": 300
  },
  "component_id": "SmartphoneMethod"
},
"U2fMethod": {
  "data": {
    "disable_builtin_attestation_cert": false,
    "check_attestation": false
  },
  "component_id": "U2fMethod"
},
"SyslogOptions": {
  "data": {
    "port": 514,
    "host": "syslog.server.ip",
    "is_enabled": true,
```

```
    "socktype": "UDP"
  },
  "component_id": "SyslogOptions"
},
"ServicesDirectorOptions": null,
"KerberosOptions": {
  "data": {
    "sso_repo_id": null
  },
  "component_id": "KerberosOptions"
},
"EndpointManOptions": {
  "data": {
    "create_need_auth": false
  },
  "component_id": "EndpointManOptions"
},
"HelpdeskOptions": {
  "data": {
    "require_user_credentials": false
  },
  "component_id": "HelpdeskOptions"
},
"MultitenancyOptions": {
  "data": {
    "multitenancy_enabled": false
  },
  "component_id": "MultitenancyOptions"
},
"GeoFencingOptions": {
  "data": {
    "geo_fencing_enabled": false
  },
  "component_id": "GeoFencingOptions"
},
"Saml2Options": null,
"TOTPMethod": {
  "data": {
    "otp_period": 30,
    "otp_window": 4,
    "otp_format": "dec6",
    "use_key_uri_format_qr": false
  },
  "component_id": "TOTPMethod"
},
"SmartcardMethod": {
  "data": {
    "tap_and_go_enabled": false
  },
  "component_id": "SmartcardMethod"
},
"RadiusMethod": {
  "data": {
    "send_reponame": false,
    "nas_identifier": "001",
    "server": "gmorris-aaf63.aaf-test.tk",
    "secret": null,
    "authport": 1812
  },
  "component_id": "RadiusMethod"
},
"EMERG_PASSWORD": {
  "data": {
    "password_min_length": 5,
    "password_age": 0,
    "allow_change": true,
    "password_check_complexity": false,
    "max_logon_count": 10
  },
  "component_id": "EMERG_PASSWORD"
```

```
},
"SMSOTPMethod": {
  "data": {
    "otp_period": 120,
    "max_sent_otp_count": 0,
    "body": "Use OTP {otp}, #{number} to login as {user} from {endpoint} to {event}",
    "otp_format": "dec6",
    "recipient_attr": null
  },
  "component_id": "SMSOTPMethod"
},
"WhitelistAdminUIOptions": null,
"VoiceMethod": {
  "data": {
    "pin_min_length": 3,
    "recipient_attr": null,
    "pin_max_age": 42
  },
  "component_id": "VoiceMethod"
},
"SMSSender": {
  "data": {
    "sender_service": "twilio",
    "twilio": {
      "account_sid": "AC1c83adb864001816c51548a5e6aee77f",
      "sender_phone": "+18012511344",
      "public_server_url": null,
      "auth_token": null,
      "use_copilot": false,
      "service_sid": ""
    },
    "is_debug": false,
    "generic": {
      "request_body": [],
      "request_method": "POST",
      "service_url": "",
      "auth_password": null,
      "request_body_secure_params": [],
      "auth_username": ""
    },
    "messagebird": {
      "password": null,
      "sender_name": "",
      "username": ""
    }
  },
  "component_id": "SMSSender"
},
"LoginOptions": {
  "data": {
    "default_repos": [
      "LOCAL",
      "GMADR2",
      "OES"
    ],
    "nondefault_repos": []
  },
  "component_id": "LoginOptions"
},
"VoiceOTPMethod": {
  "data": {
    "otp_period": 120,
    "max_sent_otp_count": 0,
    "body": "OTP #{number}: Your OTP code is {otp}",
    "otp_format": "dec4",
    "recipient_attr": null
  },
  "component_id": "VoiceOTPMethod"
},
"MailSender": {
```

```
  "data": {
    "tls": false,
    "sendmail_template": null,
    "debug": 0,
    "port": "25",
    "ssl": false,
    "username": "root",
    "default_sender": "systemuser@local.com",
    "host": "localhost",
    "keyfile": null,
    "sendmail_app": null,
    "password": null,
    "certfile": null,
    "queue_path": null
  },
  "component_id": "MailSender"
},
"SecQuestMethod": {
  "data": {
    "MinAnswerLength": 1,
    "TotalQuestionsForLogon": 5,
    "CorrectQuestionsForLogon": 5,
    "AllQuestions": {
      "AllQuestionsData": null
    }
  },
  "component_id": "SecQuestMethod"
},
"LogoOptions": {
  "data": {
    "use_mobile_image": false,
    "url": null,
    "logo_mobile_start": null,
    "use_image": true,
    "logo_mini": null,
    "text": null,
    "logo_mobile_about": null,
    "logo_lg": null
  },
  "component_id": "LogoOptions"
},
"LastLogonTrackingOptions": null,
"TemplateOptions": {
  "data": {
    "disable_reenrollment": false,
    "sharing_enabled": true
  },
  "component_id": "TemplateOptions"
},
"ADEnhancedFilter": {
  "data": {
    "filter_enabled": false
  },
  "component_id": "ADEnhancedFilter"
},
"LdapMethod": {
  "data": {
    "save_password": true
  },
  "component_id": "LdapMethod"
},
"HOTPMethod": {
  "data": {
    "otp_window": 10,
    "otp_format": "dec6"
  },
  "component_id": "HOTPMethod"
},
"HttpsOptions": {
  "data": {
```

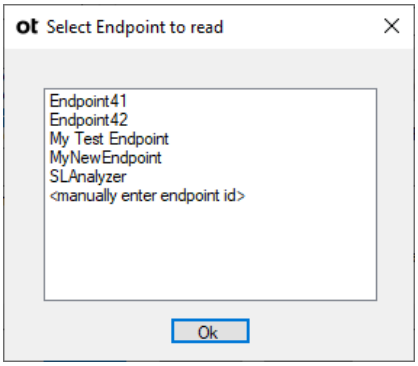
```
      "tls_1_0_enabled": false,
      "compression_enabled": false
    },
    "component_id": "HttpsOptions"
  },
  "PasswordMethod": {
    "data": {
      "password_min_length": 5,
      "rename_to_pin": false,
      "password_check_complexity": false,
      "password_max_age": 42
    },
    "component_id": "PasswordMethod"
```


https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#policies-read-effective-policies-of-endpoint-get

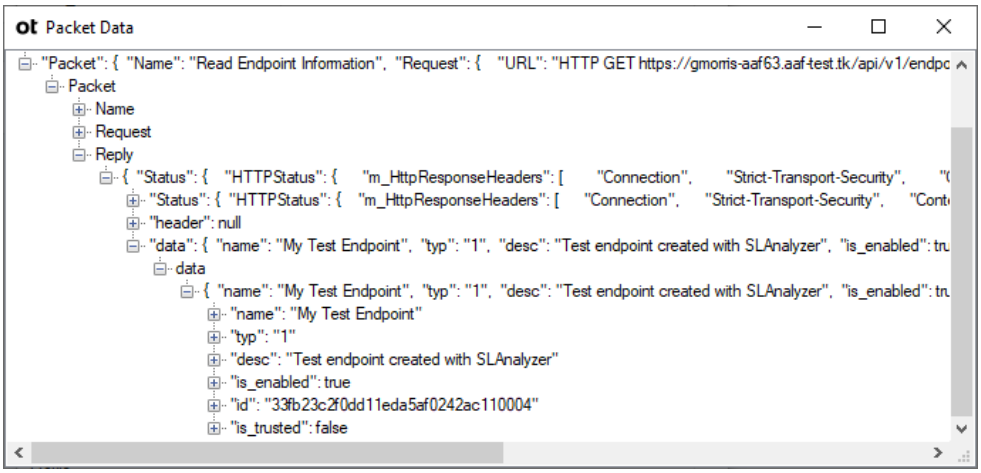
Read Endpoint Info

This REST call allows for the reading of an existing endpoint. SLAnalyzer will first display a list of known endpoints. This would include

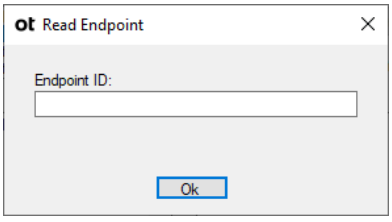
- Local Machine – If AAF client properties file exists
- Public endpoints – (Endpoint41 and EndPoint42)
- Custom endpoints – Cached endpoints created with Register New Endpont REST call
- SLAnalyzer endpoint – Diagnostic endpoint
- <manually enter endpoint id> - Read a private endpoint by id



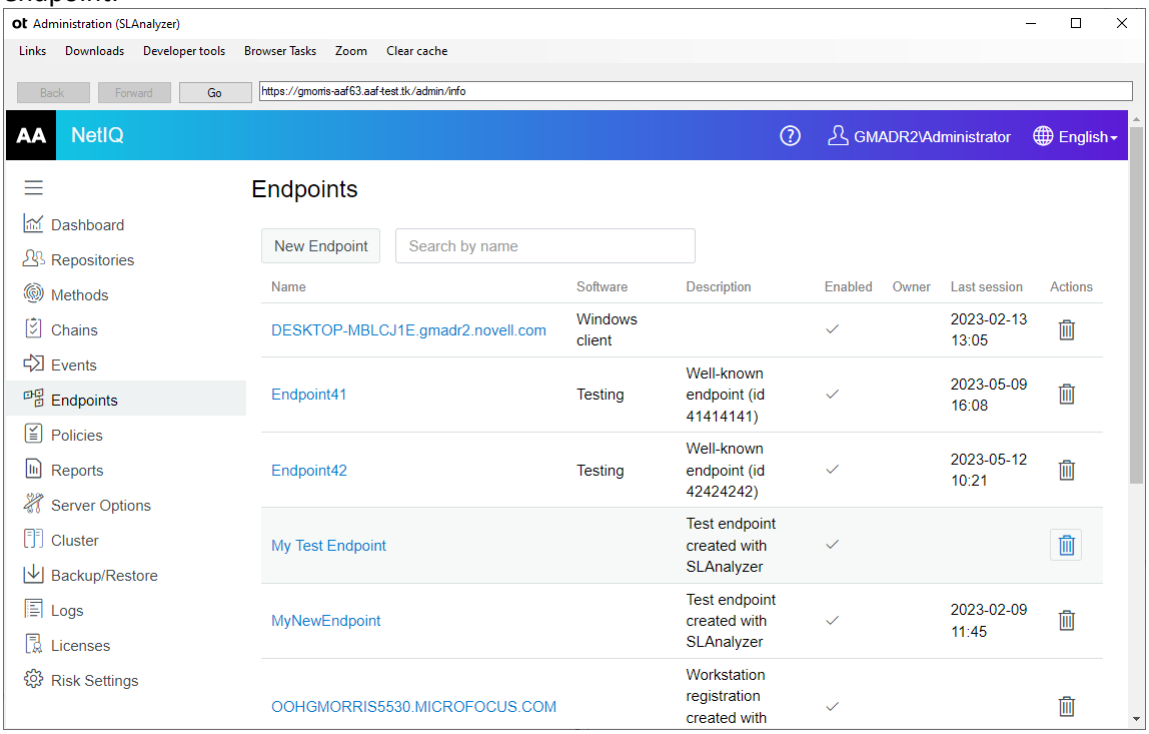
SLAnalyzer will send the request to the appliance to read the selected endpoint. The server returns the endpoint data.



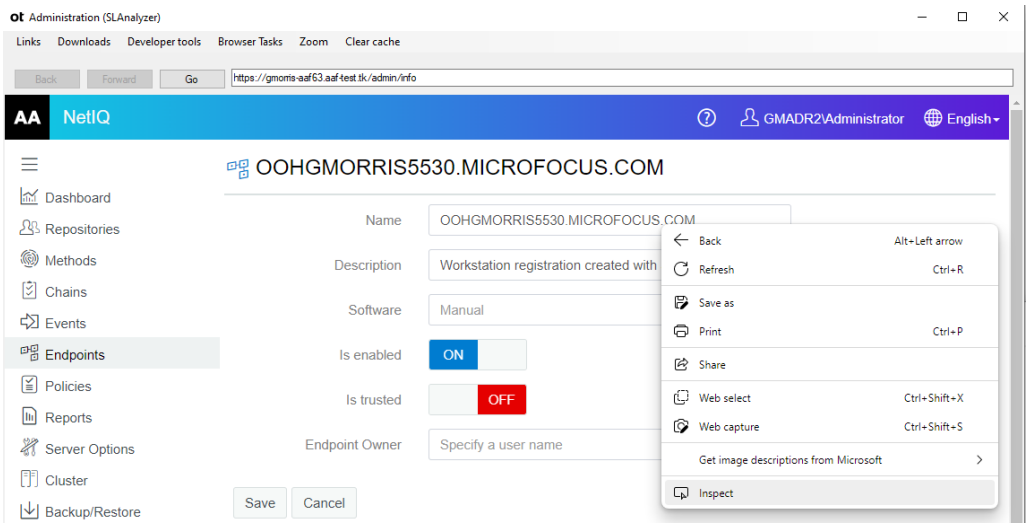
If the user selects the option <manually enter endpoint id> then SLAnalyzer will prompt for the endpoint ID.



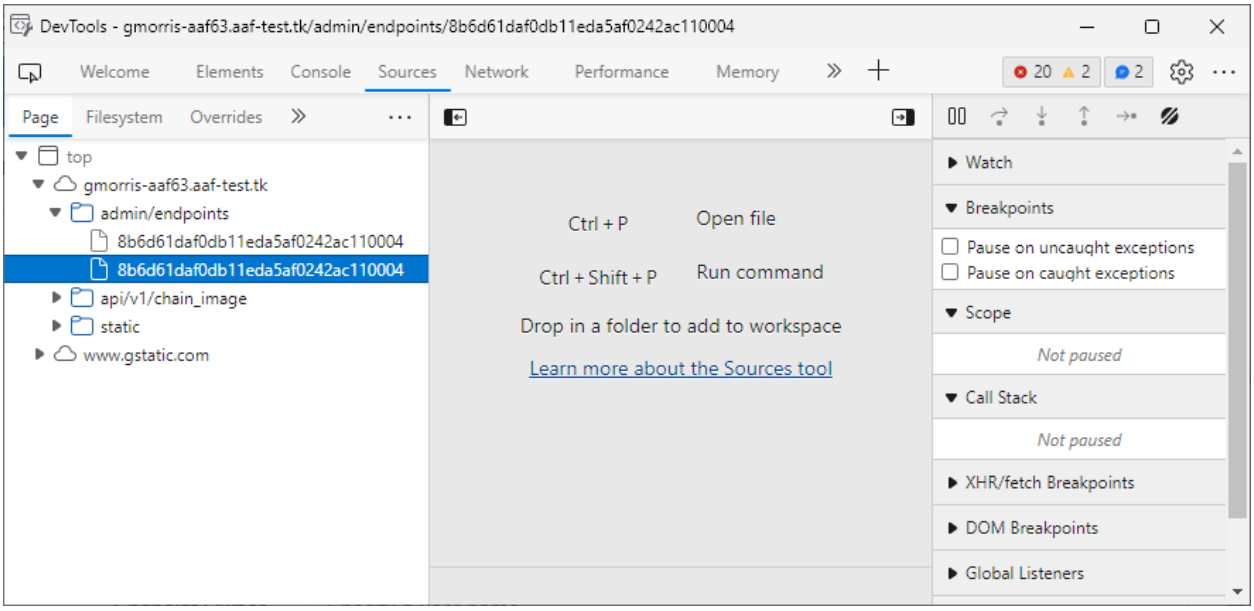
The endpoint ID can be found in the administration console. Click on Endpoints, then select the desired endpoint.



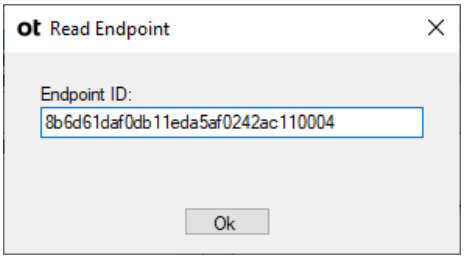
Right click anywhere in the form and select the option “Inspect”.



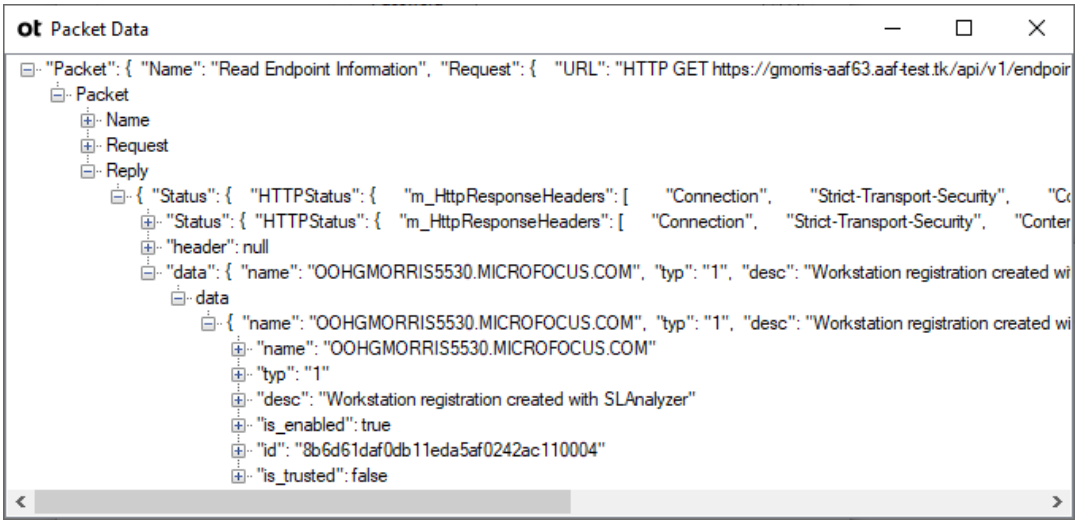
This brings up the developer tools. Click on the tab “Sources”, and then right click on the endpoint and select Copy filename.



Now execute the Read Endpoint info again and select the option “<manually enter endpoint id>”.



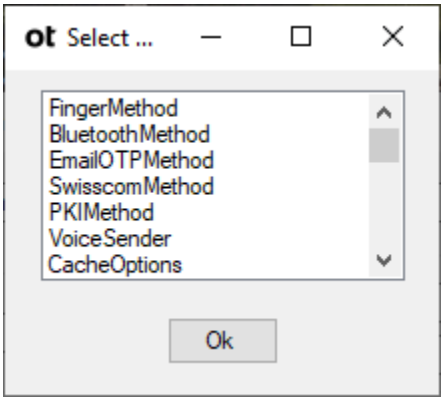
The server will then return the information about the endpoint with the specified ID.



https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#endpoints-read-endpoint-information-get

Read Info about Component of Endpont Policy

This REST call will return the information for a specific policy related to the current enpoint session.



Select the desired policy and click the Ok button to submit to the server.


```
  "Request": {
    "URL": "HTTP GET https://gmorris-aaf63.aaf-
test.tk/api/v1/endpoints/4242424242424242424242424242424242/effective_policy/BluetoothMethod?endpoint_session_id=cuhezieOb
g7VoDin1iYIqxyWxpg8GqNV",
    "header": [
      "Accept: application/json",
      "Content-Type: application/json"
    ],
    "data": null
  },
  "Reply": {
    "Status": {
      "HTTPStatus": {
        "m_Uri": "https://gmorris-aaf63.aaf-
test.tk/api/v1/endpoints/4242424242424242424242424242424242/effective_policy/BluetoothMethod?endpoint_session_id=cuhezieOb
g7VoDin1iYIqxyWxpg8GqNV",
        "m_StatusCode": 200,
        "m_ContentLength": 124,
        "m_Verb": "GET",
        "m_StatusDescription": "OK",
        "m_MediaType": null
      },
      "WebError": null,
      "AAFError": null
    "data": {
      "FingerMethod": null,
      "BluetoothMethod": {
        "policy": {
          "data": {
            "watch_on_device_removal": true
          },
          "component_id": "BluetoothMethod"
        }
      },
      "EmailOTPMethod": null,
      "SwisscomMethod": null,
      "PKIMethod": null,
      "VoiceSender": null,
      "CacheOptions": null,
      "DeleteMeOptions": null,
      "LockoutOptions": null,
      "ADPasswordFilter": null,
      "SmartphoneMethod": null,
      "U2fMethod": null,
      "SyslogOptions": null,
      "ServicesDirectorOptions": null,
```

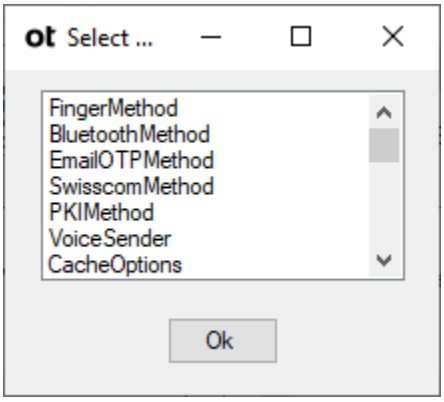
"KerberosOptions": null,
"EndpointManOptions": null,
"HelpdeskOptions": null,
"MultitenancyOptions": null,
"GeoFencingOptions": null,
"Saml2Options": null,
"TOTPMethod": null,
"SmartcardMethod": null,
"RadiusMethod": null,
"EMERG_PASSWORD": null,
"SMSOTPMethod": null,
"WhitelistAdminUIOptions": null,
"VoiceMethod": null,
"SMSSender": null,
"LoginOptions": null,
"VoiceOTPMethod": null,
"MailSender": null,
"SecQuestMethod": null,
"LogoOptions": null,
"LastLogonTrackingOptions": null,
"TemplateOptions": null,
"ADEnhancedFilter": null,
"LdapMethod": null,
"HOTPMethod": null,
"HttpsOptions": null,
"PasswordMethod": null

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#policies-read-info-about-specific-component-of-endpoint-effective-policy-get

Read Info About Component of User Policy

This REST call provides the ability to read information about a specific server policy of the currently logged in user.

When executing this REST call, SLAnalyzer will present the user with the list of server policies to gather information for.



Select the desired policy and then click the Ok button to submit the query to the server.


```
  "Request": {
    "URL": "HTTP GET https://gmorris-aaf63.aaf-
test.tk/api/v1/users/6573f2a6f4317ec114f7ee15fc948c90/effective_policy/BluetoothMethod
login_session_id=8DDh2KjT9eei15hYpYWHrgg0AzGdIReZ",
    "header": [
      "Accept: application/json",
      "Content-Type: application/json"
  "Reply": {
    "Status": {
      "HTTPStatus": {
        "m_Uri": "https://gmorris-aaf63.aaf-
test.tk/api/v1/users/6573f2a6f4317ec114f7ee15fc948c90/effective_policy/BluetoothMethod?login_session_id=8DDh2KjT9eei15hYp
YWHrgg0AzGdIReZ",
        "m_StatusCode": 200,
        "m_ContentLength": 124,
        "m_Verb": "GET",
        "m_StatusDescription": "OK",
      "WebError": null,
      "AAFError": null
    "data": {
      "FingerMethod": null,
      "BluetoothMethod": {
        "policy": {
          "data": {
            "watch_on_device_removal": true
          },
          "component_id": "BluetoothMethod"
        }
      },
      "EmailOTPMethod": null,
      "SwisscomMethod": null,
      "PKIMethod": null,
      "VoiceSender": null,
      "CacheOptions": null,
      "DeleteMeOptions": null,
      "LockoutOptions": null,
      "ADPasswordFilter": null,
      "SmartphoneMethod": null,
      "U2fMethod": null,
```

"SyslogOptions": null,
"ServicesDirectorOptions": null,
"KerberosOptions": null,
"EndpointManOptions": null,
"HelpdeskOptions": null,
"MultitenancyOptions": null,
"GeoFencingOptions": null,
"Saml2Options": null,
"TOTPMethod": null,
"SmartcardMethod": null,
"RadiusMethod": null,
"EMERG_PASSWORD": null,
"SMSOTPMethod": null,
"WhitelistAdminUIOptions": null,
"VoiceMethod": null,
"SMSSender": null,
"LoginOptions": null,
"VoiceOTPMethod": null,
"MailSender": null,
"SecQuestMethod": null,
"LogoOptions": null,
"LastLogonTrackingOptions": null,
"TemplateOptions": null,
"ADEnhancedFilter": null,
"LdapMethod": null,
"HOTPMethod": null,
"HttpsOptions": null,
"PasswordMethod": null

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#policies-read-info-about-specific-component-of-effective-user-policy-get

Read Login Session Information

This REST call will read the current login session information.


```
  "Request": {
    "URL": "HTTP GET https://gmorris-aaf63.aaf-
test.tk/api/v1/logon/sessions/wTBnvGY9rTY2PhW9l1J274Bhr3zfEUQi?endpoint_session_id=4JJDyhvVeL7mBKaQYH18pRfHZfhHn
CPK",
      "data": ""
  },
  "Reply": {
    "Status": {
      "HTTPStatus": {
        "m_Uri": "https://gmorris-aaf63.aaf-
test.tk/api/v1/logon/sessions/wTBnvGY9rTY2PhW9l1J274Bhr3zfEUQi?endpoint_session_id=4JJDyhvVeL7mBKaQYH18pRfHZfhHn
CPK",
        "m_StatusCode": 200,
        "m_ContentLength": 767,
        "m_Verb": "GET",
        "m_StatusDescription": "OK",
      "WebError": null,
      "AAFError": null
    },
    "data": {
      "event_name": "Authenticators Management",
      "repo_id": "655eb2fe9ae011ea83b00242ac110003",
      "user_id": "6573f2a6f4317ec114f7ee15fc948c90",
      "repo_obj_id": "3ab9e64a18d7e1459e03be37c5f07a55",
      "sid": null,
      "user_name": "GMADR2\\Administrator",
      "data_id": "AUTHENTICATORS MANAGEMENT"
    },
```


https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#login-sessions-read-information-about-login-session-get

Register Logon Domains for the Current Tenant

Used to specify the logon domain of multi-tenant configurations.

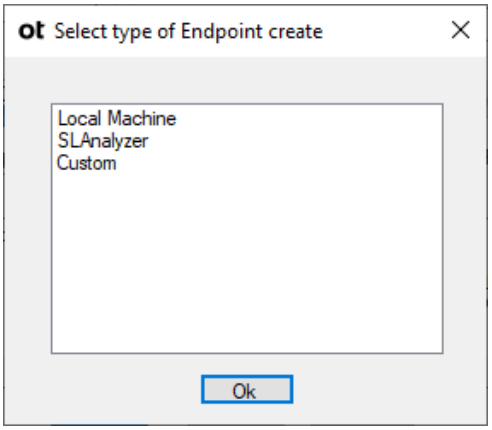
When selected the user will be allowed to manage the domains.



Register New Endpoint

SLAnalyzer allows the user to create 3 different types of endpoints.

- Local Machine – The registered endpoint for the workstation. Same as the endpoint created by the AAF Windows client.
- SLAnalyzer – Diagnostic endpoint for use with SLAnalyzer
- Custom – An endpoint with user specified name

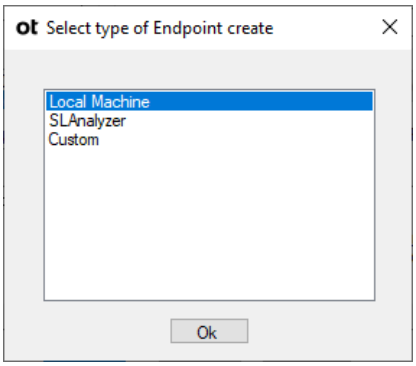


https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#endpoints-register-new-endpoint-post

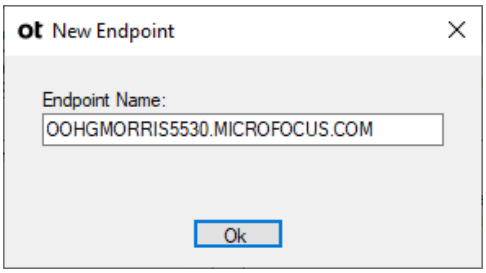
Local Machine endpoint

The local machine endpoint is an endpoint with the workstation name. The endpoint data is cached to AAF windows client configuration file. (C:\ProgramData\NetIQ\Windows Client\config.properties)

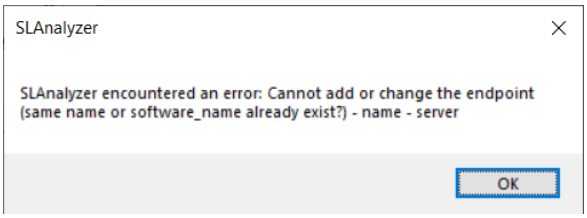
When registering a new workstation endpoint SLAnalyzer will update the config.properties file with the new endpoint information (ID and secret)

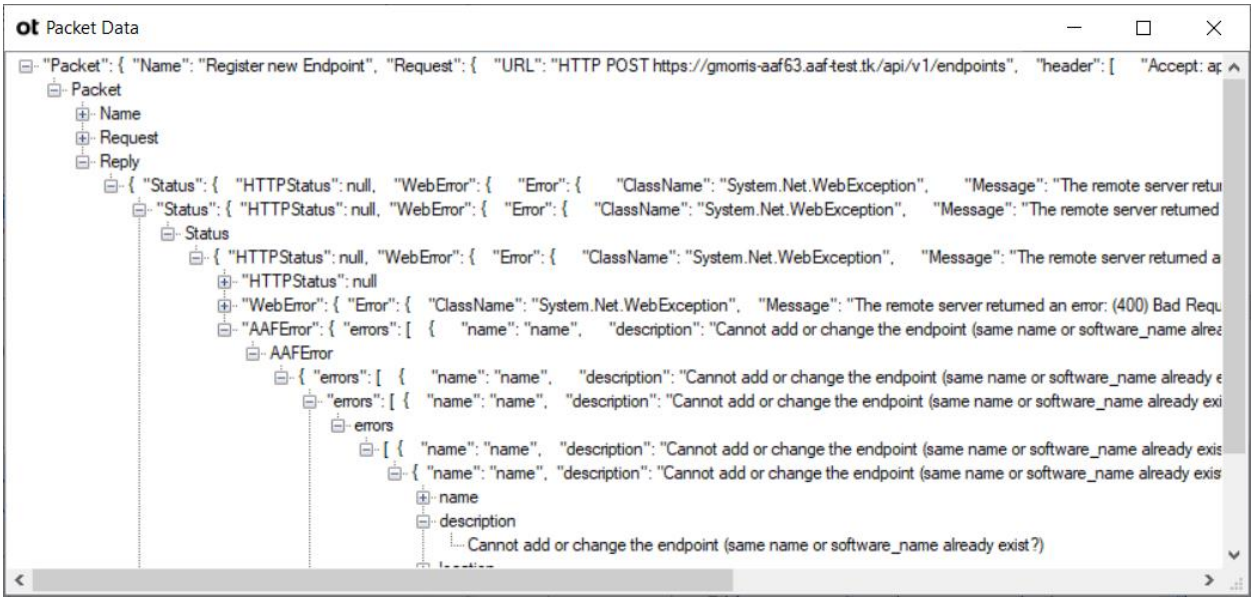


After selecting the Local Machine as the endpoint type then SLAnalyzer will prompt with the name of the endpoint. In the case of a Local Machine endpoint the name should be the workstation name with DNS context.



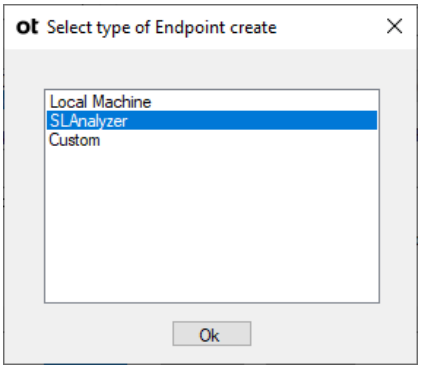
If the workstation has already been registered, then the server will return an error.



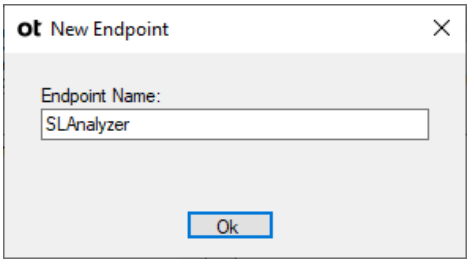

ot Packet Data
"Packet": { "Name": "Register new Endpoint", "Request": { "URL": "HTTP POST https://gmorris-aaf63.aaf-test.tk/api/v1/endpoints", "header": ["Accept: ap
Packet
Name
Request
Reply
{ "Status": { "HTTPStatus": null, "WebError": { "Error": { "ClassName": "System.Net.WebException", "Message": "The remote server retu
"Status": { "HTTPStatus": null, "WebError": { "Error": { "ClassName": "System.Net.WebException", "Message": "The remote server returned
Status
{ "HTTPStatus": null, "WebError": { "Error": { "ClassName": "System.Net.WebException", "Message": "The remote server returned a
"HTTPStatus": null
"WebError": { "Error": { "ClassName": "System.Net.WebException", "Message": "The remote server returned an error: (400) Bad Requ
"AAFError": { "errors": [{ "name": "name", "description": "Cannot add or change the endpoint (same name or software_name alrea
AAFError
{ "errors": [{ "name": "name", "description": "Cannot add or change the endpoint (same name or software_name already e
"errors": [{ "name": "name", "description": "Cannot add or change the endpoint (same name or software_name already exi
errors
[{ "name": "name", "description": "Cannot add or change the endpoint (same name or software_name already exis
{ "name": "name", "description": "Cannot add or change the endpoint (same name or software_name already exis
name
description
Cannot add or change the endpoint (same name or software_name already exist?)

SLAnalyzer endpoint

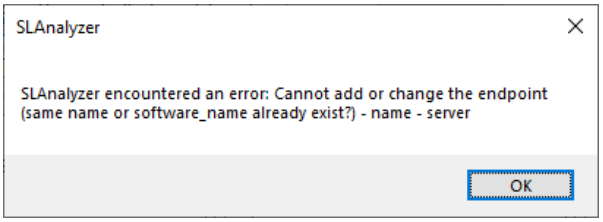
The SLAnalyzer endpoint is a diagnostic endpoint for use with SLAnalyzer.



After Selecting the SLAnalyzer endpoint type the user is prompted for the name.

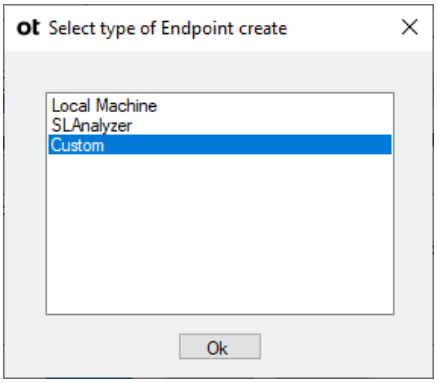


SLAnalyzer will first check the cached endpoint data for this appliance to see if the endpoint already exists. If the endpoint is found, then the following error is returned.

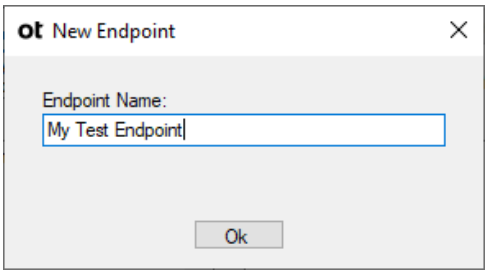


Custom Endpoint

The custom endpoint allows the user to provide a name for the endpoint.



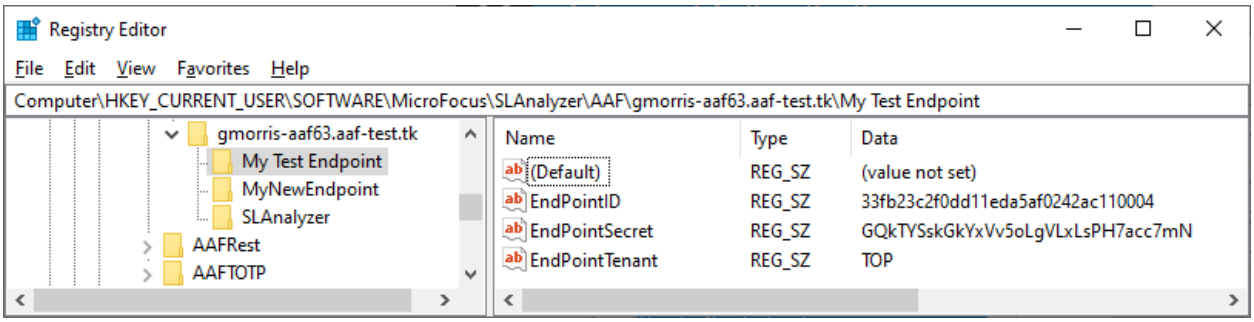
After selecting the custom endpoint type SLAnalyzer will prompt the user for an endpoint name.



If successful, the endpoint ID and Secret are returned by the server.



SLAnalyzer will cache the information returned from a successful endpoint registration to the registry of the workstation. HKCU\Software\MicroFocus\SLAnalyzer\AAF\<applianceName>\<endpointName>



Packet Data:

Request:

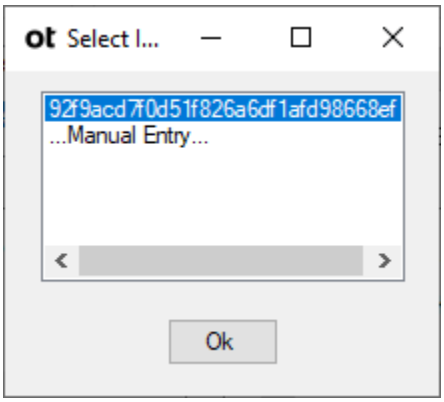
```
 "URL": "HTTP POST https://gmorris-aaf63.aaf-test.tk/api/v1/endpoints",
 "data": {
  "name": "My Test Endpoint",
  "typ": "3",
  "desc": "Test endpoint created with SLAnalyzer"
 }
```

Reply:

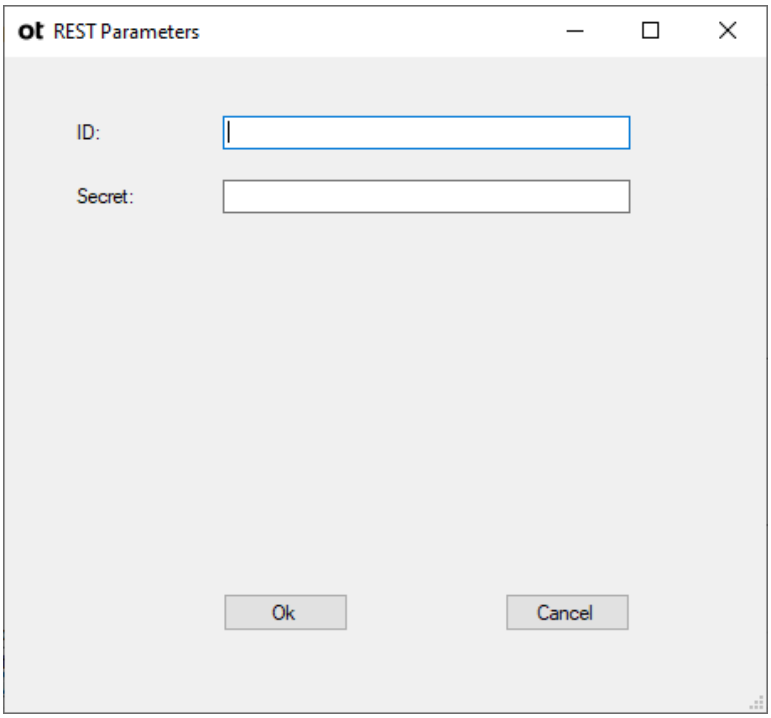
```
 "data": {
 "id": "33fb23c2f0dd11eda5af0242ac110004",
 "secret": "GQkTYSskGkYxVv5oLgVLxLsPH7acc7mN"
}
```

Remove Already Enrolled TOTP Template

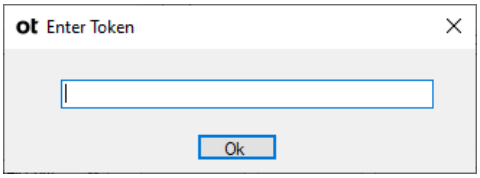
This API will attempt to remove any TOTP enrolled template that had been previously performed with SLAnalyzer. The user can also manually enter a TOTP template ID.



When selecting Manual Entry the following information is required.



Revoke OTP Token

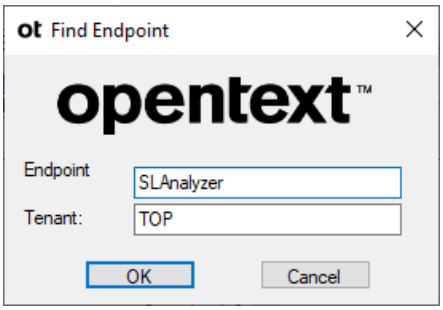


https://www.netiq.com/documentation/advanced-authentication-64/apidoc/data/apidoc.html#otp-tokens-revoke-otp-token-delete

Search for Endpoint

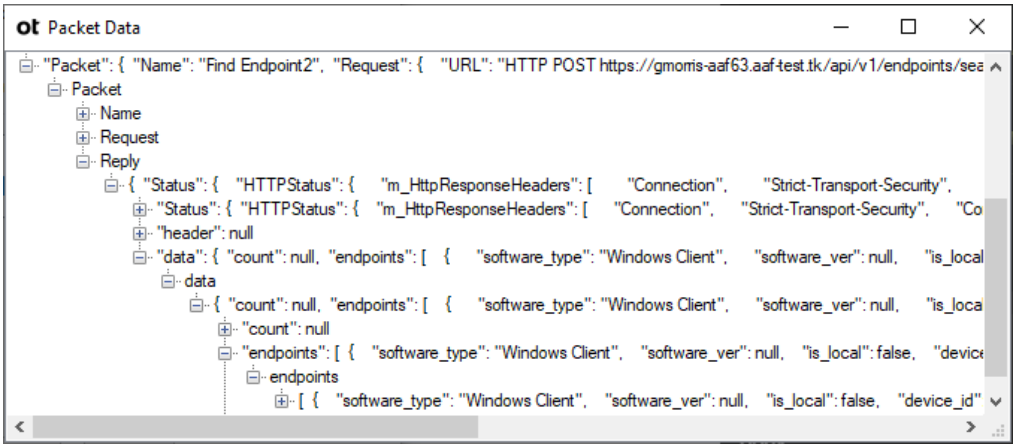
This REST call will search the endpoints defined on the server for a specific name.

The user will first be prompted for the name of the endpoint to find.



Click the Ok button to perform the search.

The packet data window will now display the information for the endpoint.



"software_type": "Windows Client",
"software_ver": null,
"is_local": false,
"device_id": "",
"is_enabled": true,
"desc": "Test endpoint created with SLAnalyzer",
"owner": null,
"name": "SLAnalyzer",
"typ": 1,
"id": "e329d40cf10e11eda62b0242ac110003",
"is_trusted": false,
"device_many_endpoints": false,
"last_session": null,
"os": null

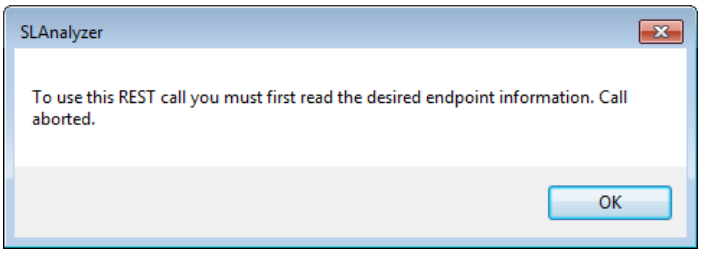
https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#endpoints-search-endpoints-by-name-post

Update Endpoint Info

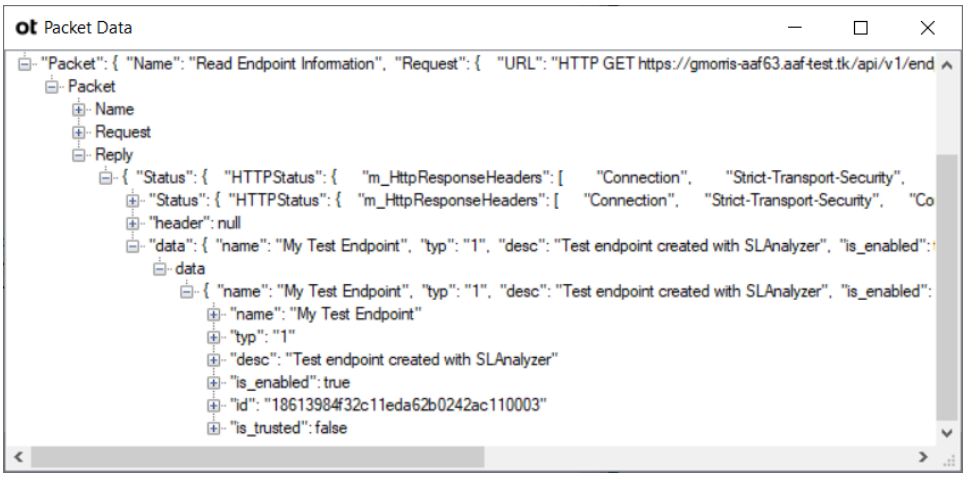
This REST call allows the user to change/update the endpoint information.

Prior to making this REST call you must first issue the Read Endpoint Info REST call.

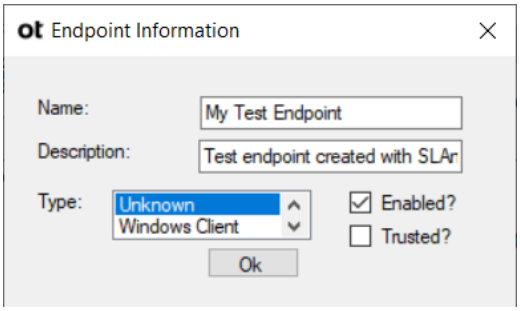
If the Read Endpoint REST call has not been made then SLAnalyzer will return the following error:



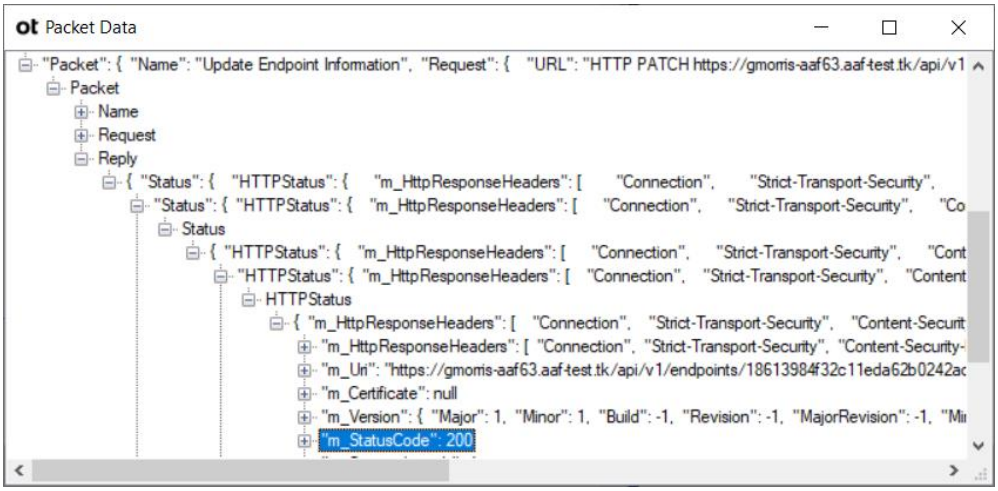
When executing Read Endpoint select the desired endpoint to update. In our example we selected the endpoint “My Test Endpoint”.



Then when executing Update Endpoint Info, SLAnalyzer presents the user with the endpoint information. The user can change any of the displayed data for the endpoint.



After the user changes the data and clicks the Ok button, SLAnalyzer sends the Update Endpoint Info REST call to the server.



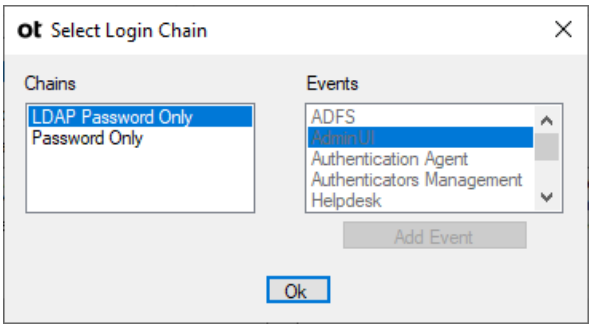
If successful, the server responds with an HTTPS status of 200.

https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#endpoints-update-endpoint-information-patch

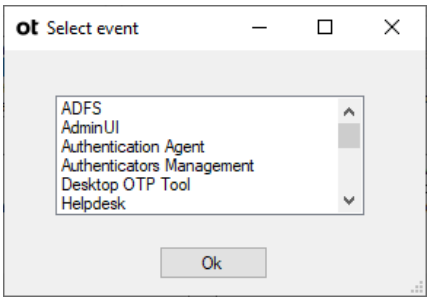
Update Event

This API will update an existing event.

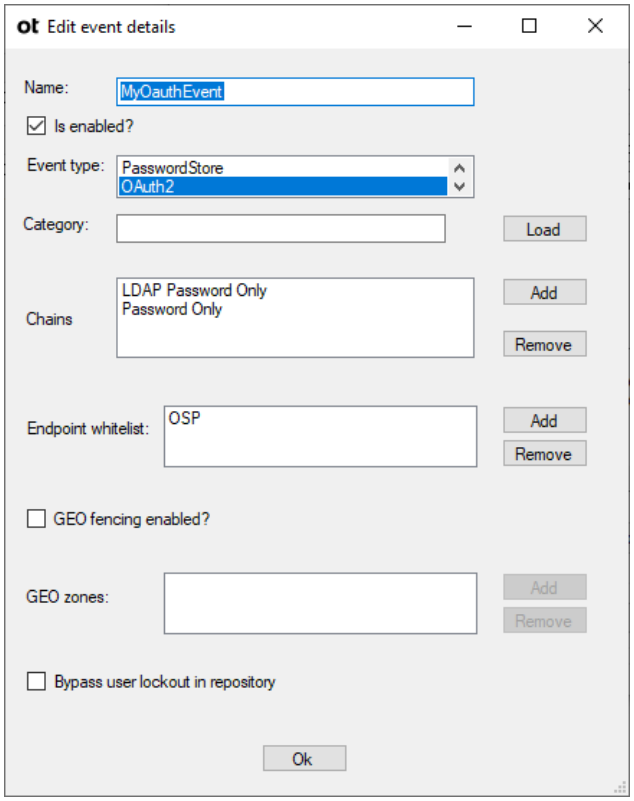
This API requires login to the AdminUI event.



Select event to edit



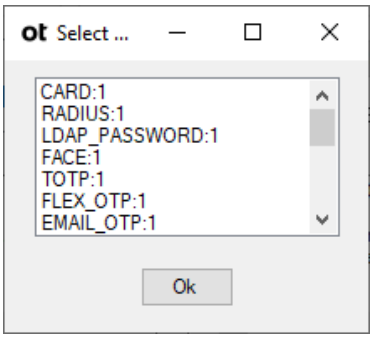
Edit event details

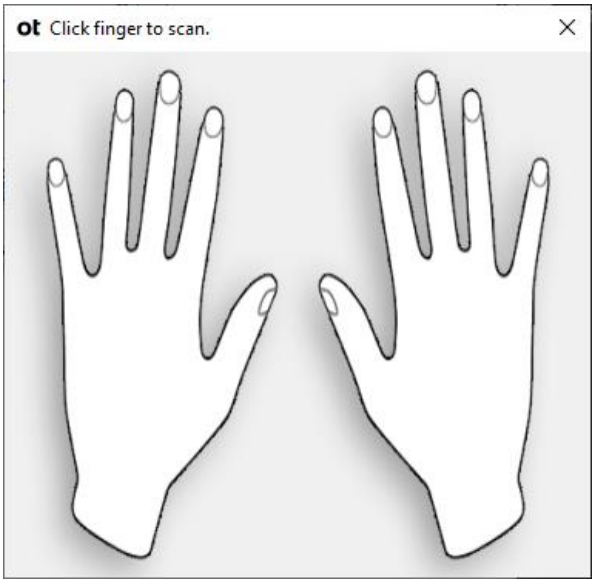


https://www.netiq.com/documentation/advanced-authentication-64/apidoc/data/apidoc.html#events-update-event-put

Update User Template

This API allows users to update/edit an enrolled method. For example, selecting Fingerprint, the user can re-scan their fingerprints.

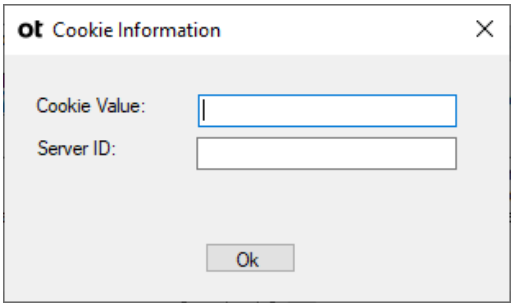




https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#user-templates-fill-auth-template-from-enroll-session-and-or-change-comment-put

Verify Cookie Value

Use cookie value and server_id from cookie-generation method. Will return logon session if cookie is valid. If you send server_id from other server to current server then current server will redirect request to first server. See Generate cookie value API.





https://www.netiq.com/documentation/advanced-authentication-63/apidoc/data/apidoc.html#cookie-and-ticket-services-verify-cookie-value-get

Examples:

The description of the advanced features references a login event called Reflection. To replicate this, create a new Event on the application server named Reflection. Enable this new event and add the Chains Password & SMS OTP.

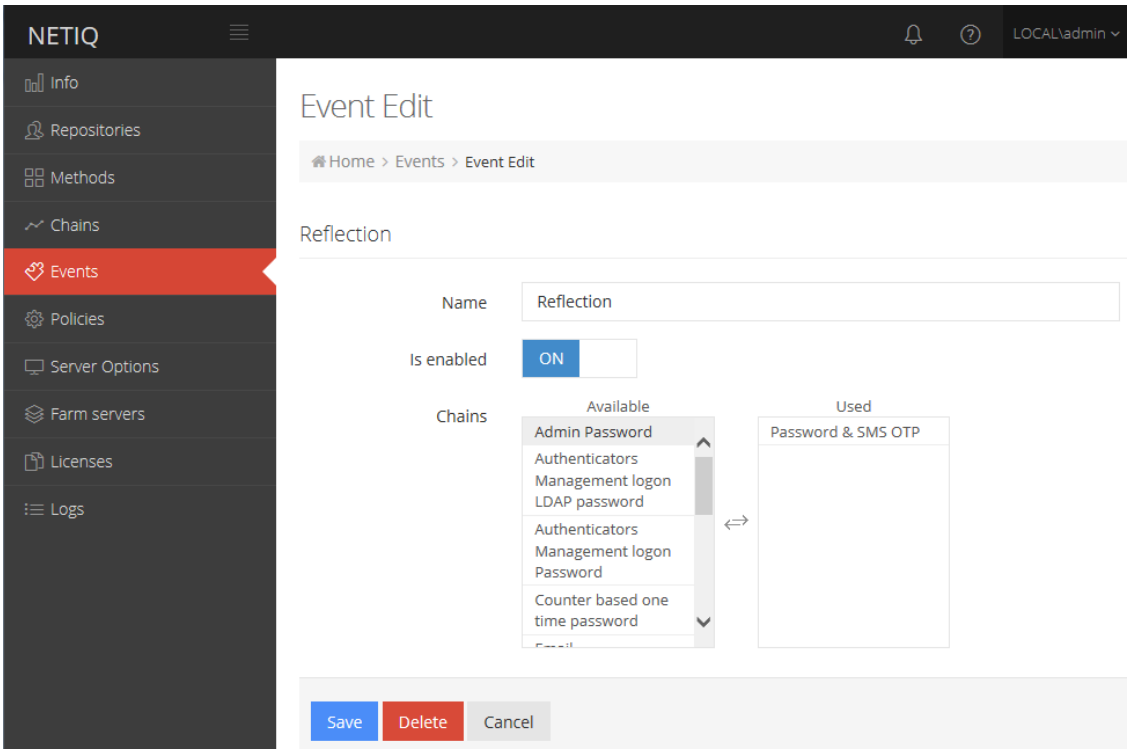


Figure 178 - Login Event Reflection

Create Session

The list of endpoint sessions is built from:

1. Local Machine – This is the endpoint session created by the AAF Windows client. If detected then SLAnalyzer will display this as a potential endpoint
2. Cached endponts – The endpoints listed in the example have been created with SLAnalyzer using the advanced REST call “Register New Endpoint”. When new endpoints are registered with SLAnalyzer, the tool will cache the information for this endpoint to the registry. If any cached data is found, then these items will be included in this list.
3. Public Endpoints – AAF provides two public endpoints called Endpoint41 and Endpoint42. These are available on the appliance but are disabled by default. To use these endpoints, you must enable from the appliance management console. Also note that the public endpoints are being depreciated and use of registered endpoints will be the preferred connection type in the future.

Before any REST calls can be made to the AAF appliance an endpoint session needs to be created.

An endpoint session defines a communications session between a device endpoint and the AAF appliance. Any device needing to communicate with an AAF appliance must do so using an endpoint. The first step in setting up the communications between an application and the AAF server is the creation of an endpoint.

SLAnalyzer will now read the endpoint used by the AAF Windows client (if installed), the public endpoint42 (if enabled), or create an endpoint with the name of SLAnalyzer. Prior to AAF 5.2, SLAnalyzer only used the public endpoint42. Note that if the public endpoint exists but is disabled then SLAnalyzer will display an error message indicating that the endpoint needs to be enabled. You can either enable the public endpoint or delete the endpoint definition. If you enable the public endpoint, then SLAnalyzer will use the public endpoint and not create the Diagnostic endpoint. If the public endpoint is deleted, then the new Diagnostic endpoint will be created as shown below.

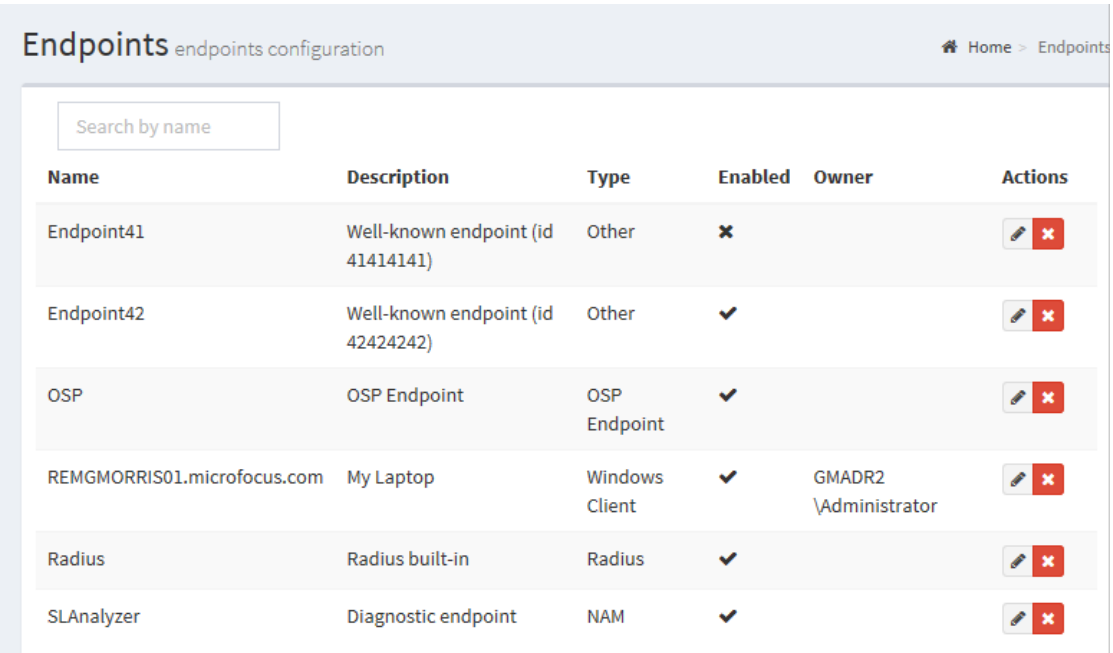


Figure 179 - SLAnalyzer endpoint

The SLAnalyzer endpoint is dynamically created when you execute the Create Session REST call for the first time. SLAnalyzer will detect that the appliance version is 5.2 or higher and will attempt to create this endpoint if there is no AAF Windows client endpoint (IE. REMGMORRIS01.microfocus.com) or public endpoint (Endpoint42) is not enabled.

When the endpoint is created the information associated with this endpoint is cached to the local workstation registry. This enables SLAnalyzer to reconnect to the same endpoint on future sessions.

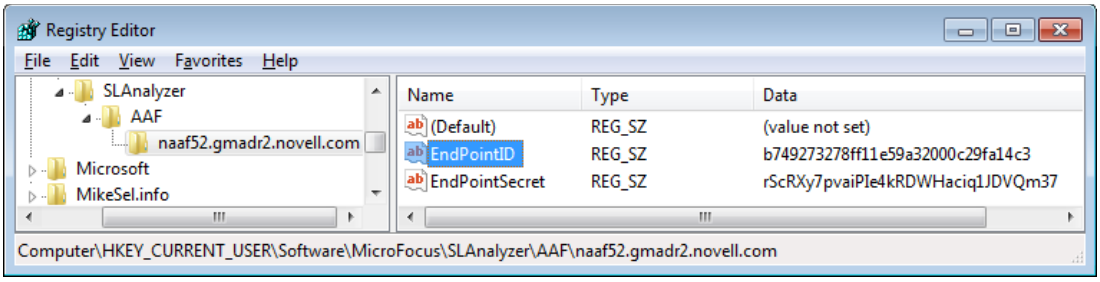


Figure 180 - Cached SLAnalyzer endpoint data

If you need to run SLAnalyzer on another workstation, then you will need to export this registry key from the workstation that performed the registration of the endpoint and then import the registry data to the second workstation. This will allow both workstations to access the same endpoint for diagnostic purposes. If only one workstation is needed, then you can delete the endpoint from the AAF administration console and then execute the Create Session REST call on the second workstation to create a new SLAnalyzer endpoint.

Get Session Info

This REST call retrieves the information associated with this endpoint session.

REST Call:
****
https://naaf54.gmadr2.novell.com/api/v1/endpoints/9c11d214898111e696ef000c296f406a/sessions/ER4soSHsr1rTBVJqNNrxQBNAvaOMxcYn?salt=2615c070937935246c6a91df70a8eb672b21d842a225621c9797a83bedf00a7b&endpoint_secret_hash=617017644b15920ba69ebc26e5feb55dd43ea9939033046e667331dc0752bb01
****

Response from Get Session Info:
****
JSON data:
****
{"endpoint_id": "9c11d214898111e696ef000c296f406a", "sid": "ER4soSHsr1rTBVJqNNrxQBNAvaOMxcYn", "session_data": {}}

Get Server Status

This REST call retrieves the version and current status of the AAF server.

****
Get Status
****
REST Call:
****
GET https://naaf54.gmadr2.novell.com/api/v1/status
****
Response from GET Status:
****
JSON data:
****
{"version": "5.5", "multitenancy_mode": false, "status": "OK"}

Get Full Server Status

This REST call retrieves the detailed version and current status of the AAF server.

****
Get Status
****

JSON data:
****
{"endpoint_session_id":"ER4soSHsr1rTBVJqNNrxQBNAvaOMxcYn","tenant_name":""}
REST Call:
****
POST https://naaf54.gmadr2.novell.com/api/v1/status
Body: {"endpoint_session_id":"ER4soSHsr1rTBVJqNNrxQBNAvaOMxcYn","tenant_name":""}
****
Response from POST Status:
****
JSON data:
****
{"fips_mode": false, "version": "5.5-326", "multitenancy_mode": false, "status": "OK"}

Delete Session

This REST call terminates the current endpoint session. Before any future REST calls can be made to the AAF appliance a new endpoint session will need to be created.

Get Authentication Chains

Before starting the login process or attempting to register a method you must first issue a Get Authentication Chains call to the server. The server will return a list of the defined methods and chains for each event configured on the appliance.

This call has parameters that define the event that you want to view the methods for.

Parameters

The logon parameters window displays the default login events.

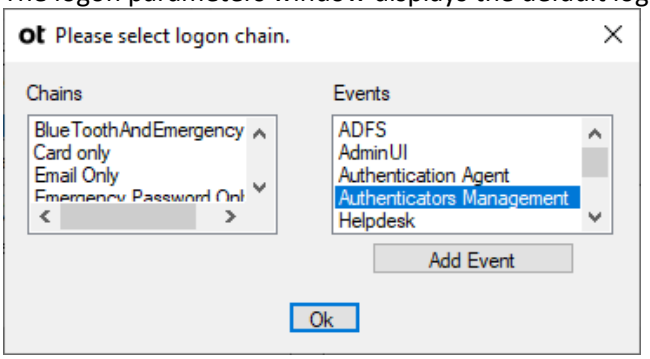


Figure 181 - AAF Logon parameters

If there are custom events configured, then click the Add Event button to add the custom event to the Events list.

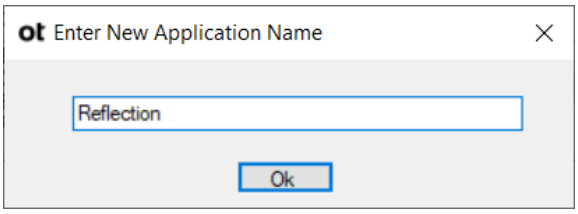


Figure 182 - AAF Add new event

Select the desired event and to return the list of configured chains for this event.

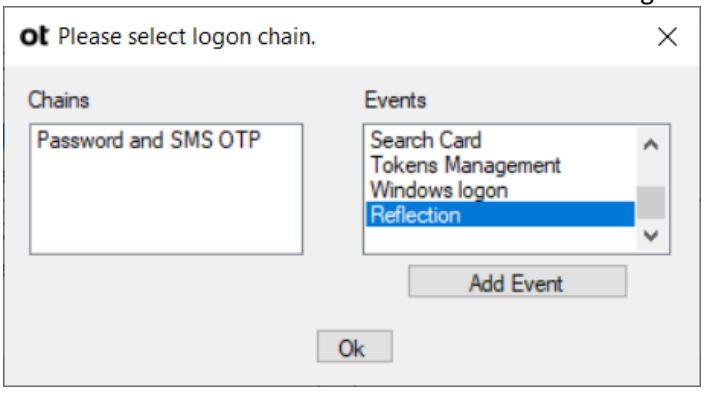


Figure 183 - AAF Update Methods

Response from: Get Authentication Chains

****

Number of Chains: 1

name = Password & SMS OTP
Number of Methods: 2
method = LDAP_PASSWORD:1
method = SMS_OTP:1
short name =
is trusted = True
****

We can see from this information that there is one chain for this login event which includes two methods LDAP_PASSWORD and SMS_OTP. This means that to properly perform an authentication with this login event the user would need to successfully provide their LDAP password and perform the SMS OTP.

Logon

Logon allows us to test the login event and methods assigned.

When executing this call SLAnalyzer will prompt the user for the event and chain they would like to perform the logon with. This is the same window seen in the Get Authentication Chains parameters.

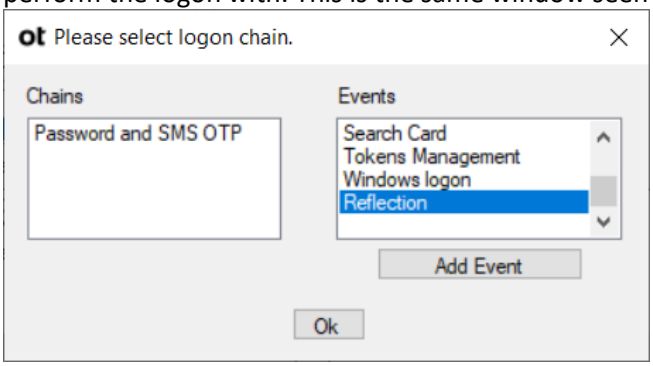


Figure 184 - Logon select event and method

We will use the custom event Reflection in this test (See Get Authentication Parameters). We already know that this is a single login chain with two methods LDAP password and SMS_OTP.

Select Reflection. This lists the chain Password and SMS OTP. Select the chain and then click the Ok button.

SLAnalyzer now sends the first login method request to the appliance. The appliance processes the request and then returns a status indicating what type of information is needed to complete the process. With the LDAP password the user is not prompted because on the main AAF REST window we have provided to SLAnalyzer the user credentials. SLAnalyzer simply takes this information and sends it to the appliance to perform the LDAP logon without user interaction.

If both chains are completed successfully then the reply window of the AAF REST window will display “Login completed successfully”. Otherwise, the reply window will contain information as to why the logon process failed.

Read Login Session Information

This call returns information about the current login session. This information is required for other calls that are related to a specific logon session.

Response from: Get Logon Information

```
**********
application name = Reflection
application id =
repository id = cfe44de416c111e5846f000c29b9e140
repository object id = d5bce061b3f30946ea9cd5bce061b3f3
user id = 4238540c16c311e5846f000c29b9e140
user name = OESTREE\NAAFUser
sid = VzIuQGEQAZmg0P2FYHF8LJEsqbNbR57F
**********
```

Delete Login Session Information

Delete Login Session Information will delete an aborted logon session.

Read User Data

Reads any user defined data associated with this logon session.
This feature is currently designed for the NAM or NCA events. Ensure you are logged into one of these events before attempting to manipulate user data.

If there is no user data created by SLAnalyzer or some other application then the reply window will display.

```
Response from: Read User Data
**********
{"appdata": {}}
**********
```

If there has been user information created by either SLAnalyzer or some other application then the data will display in the reply window.

```
Response from: Read User Data
**********
{"appdata": {"test3": "value 3", "test2": "value 2", "test1": "value 1"}}
**********
```

Modify User Data

The modify call will create the user data of
{"appdata": {"test3": "value 3", "test2": "value 2", "test1": "value 1"}}

The reply window will display.

```
Response from: Modify User Data
**********
HTTP Status code: OK
**********
```

Delete User Data

Deletes any user data defined on this login even.

```
Response from: Delete User Data
**********
HTTP Status code: OK
**********
```

Enroll

This call brings up the methods list. The user can select the desired method for further testing.

Delete Enroll

Delete Enroll is to delete an aborted enrollment session.

Get User Template

Before you can issue the Get User Template call, you must first is a call to Logon and login to the Authenticators Management event. Then execute the call Read Login Session Information to populate the necessary structures to call Get User Template.

This call returns the information about each possible method and their status.

Response from: Get User Template

****

{"templates": [{"method_id": "LDAP_PASSWORD:1", "comment": "Modified with SLAnalyzer", "method_title": "LDAP password", "id": "423b69e416c311e5846f000c29b9e140", "is_enrolled": true}, {"method_id": "PASSWORD:1", "comment": "Enrolled with SLAnalyzer", "method_title": "Password", "id": "be8708d4324111e58bd2000c29b9e140", "is_enrolled": true}, {"method_id": "SMS_OTP:1", "comment": "Enrolled with SLAnalyzer", "method_title": "SMS OTP", "id": "15704e8a324211e58bd2000c29b9e140", "is_enrolled": true}, {"method_id": "VOICE:1", "comment": "Enrolled with SLAnalyzer", "method_title": "Voice", "id": "bdf575ea326e11e59c89000c29b9e140", "is_enrolled": true}, {"method_id": "EMAIL_OTP:1", "comment": "Enrolled with SLAnalyzer", "method_title": "Email OTP", "id": "c21bd984326e11e59c89000c29b9e140", "is_enrolled": true}, {"method_id": "RADIUS:1", "comment": "Enrolled with SLAnalyzer", "method_title": "Radius Client", "id": "899f9a68326f11e59c89000c29b9e140", "is_enrolled": true}, {"method_id": "TOTP:1", "comment": "Enrolled with SLAnalyzer", "method_title": "TOTP", "id": "c9f7680c326f11e59c89000c29b9e140", "is_enrolled": true}, {"method_id": "HOTP:1", "comment": "Enrolled with SLAnalyzer", "method_title": "HOTP", "id": "d69599e4326f11e59c89000c29b9e140", "is_enrolled": true}, {"method_id": "SECQUEST:1", "comment": "Enrolled with SLAnalyzer", "method_title": "Security questions", "id": "39ea9fe0327411e59c89000c29b9e140", "is_enrolled": true}, {"method_id": "SMS_OTP:1", "comment": "Enrolled with SLAnalyzer", "method_title": "SMS OTP", "id": "9e2026e8346711e5831f000c29b9e140", "is_enrolled": true}, {"method_id": "EMAIL_OTP:1", "comment": "Enrolled with SLAnalyzer", "method_title": "Email OTP", "id": "a75f7b78346711e5831f000c29b9e140", "is_enrolled": true}, {"method_id": "SECQUEST:1", "comment": "Enrolled with SLAnalyzer", "method_title": "Security questions", "id": "b7e05b70346711e59a30000c29b9e140", "is_enrolled": true}, {"method_id": "RADIUS:1", "comment": "Enrolled with SLAnalyzer", "method_title": "Radius Client", "id": "be8edabe346711e5831f000c29b9e140", "is_enrolled": true}, {"method_id": "SMARTPHONE:1", "comment": "Enrolled with SLAnalyzer", "method_title": "Smartphone", "id": "55efa0d4347511e5b5d7000c29b9e140", "is_enrolled": true}]}

****

Create User Template

After executing the Enroll call and successfully enrolling a method, the information is not really saved until you execute the Create User Template call. This call will save the enrollment data for the currently selected enroll method.

Use these steps to create a user template

- Login to the authenticator management event
- Now read the login session information
- Enroll a method
- Create the user template for that method

Assign User Template

Assign a user template to a different user object in the repository.

Use these steps to assign a user template to another user.

- Login with source user
- Read the login session information
- Enroll a method
- Login as destination user
- Assign user template

Update User Template

The Update User Template call will modify an already enrolled method.

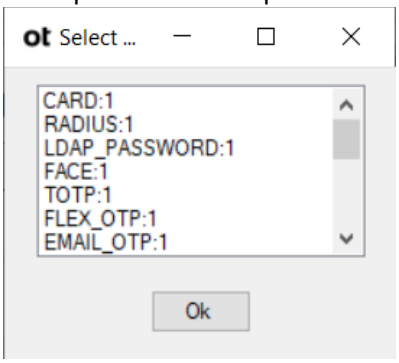


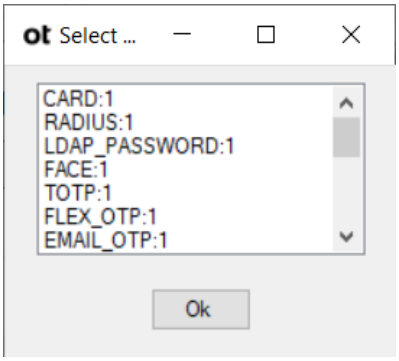
Figure 185 - Select Method to update

Each method selected will prompt for the required information that it requires. For example, if you selected to modify the Password:1 method then you would be prompted to enter a new password.

To abort click the X in the upper right-hand corner.

Delete User Template

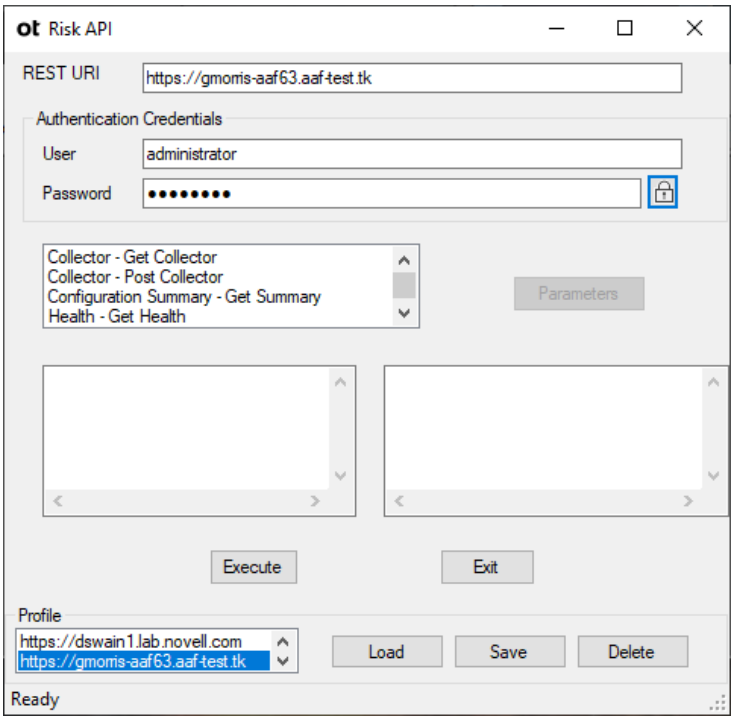
Delete User Template deletes an enrolled method from a user.



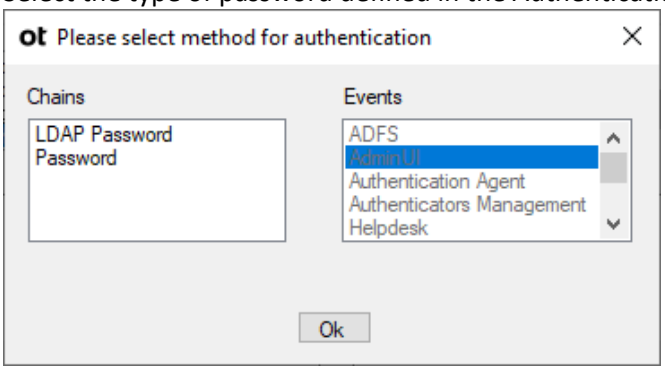
Highlight the method to delete and click the done button. To abort click the X in the upper right-hand corner.

Risk Services

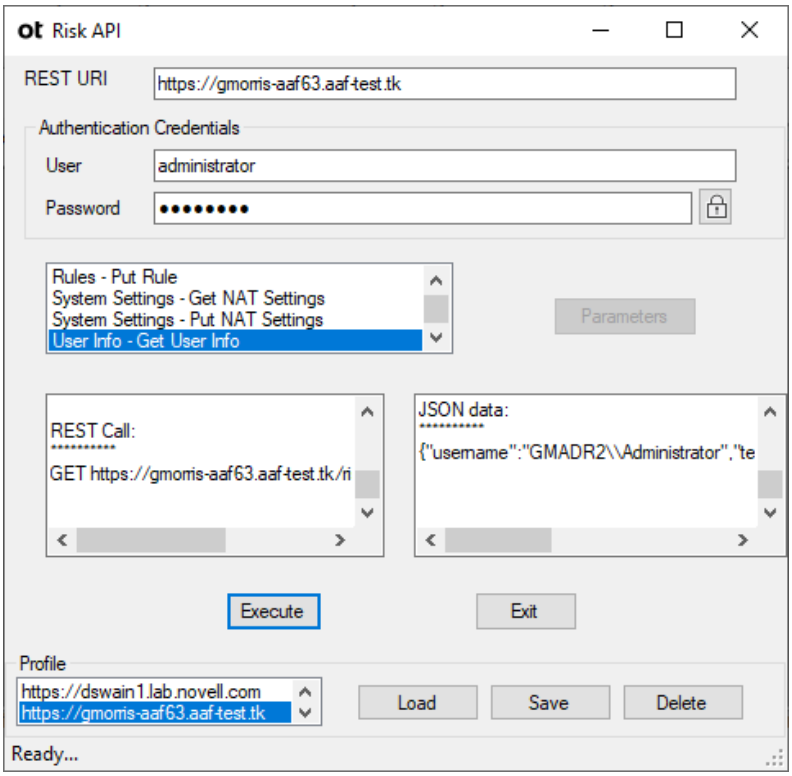
This tool functions much like the Advanced Authentication REST client. Select the desired REST call and then click the execute button.



Select the type of password defined in the Authentication Credentials box.



After login the REST call will be sent to the server.



The REST call request and reply structures can be seen in the packet window.

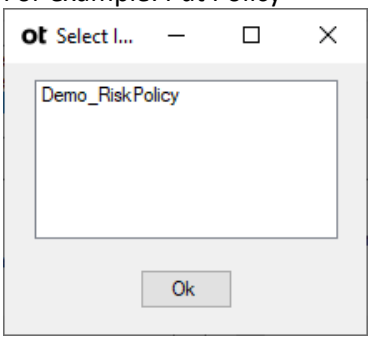


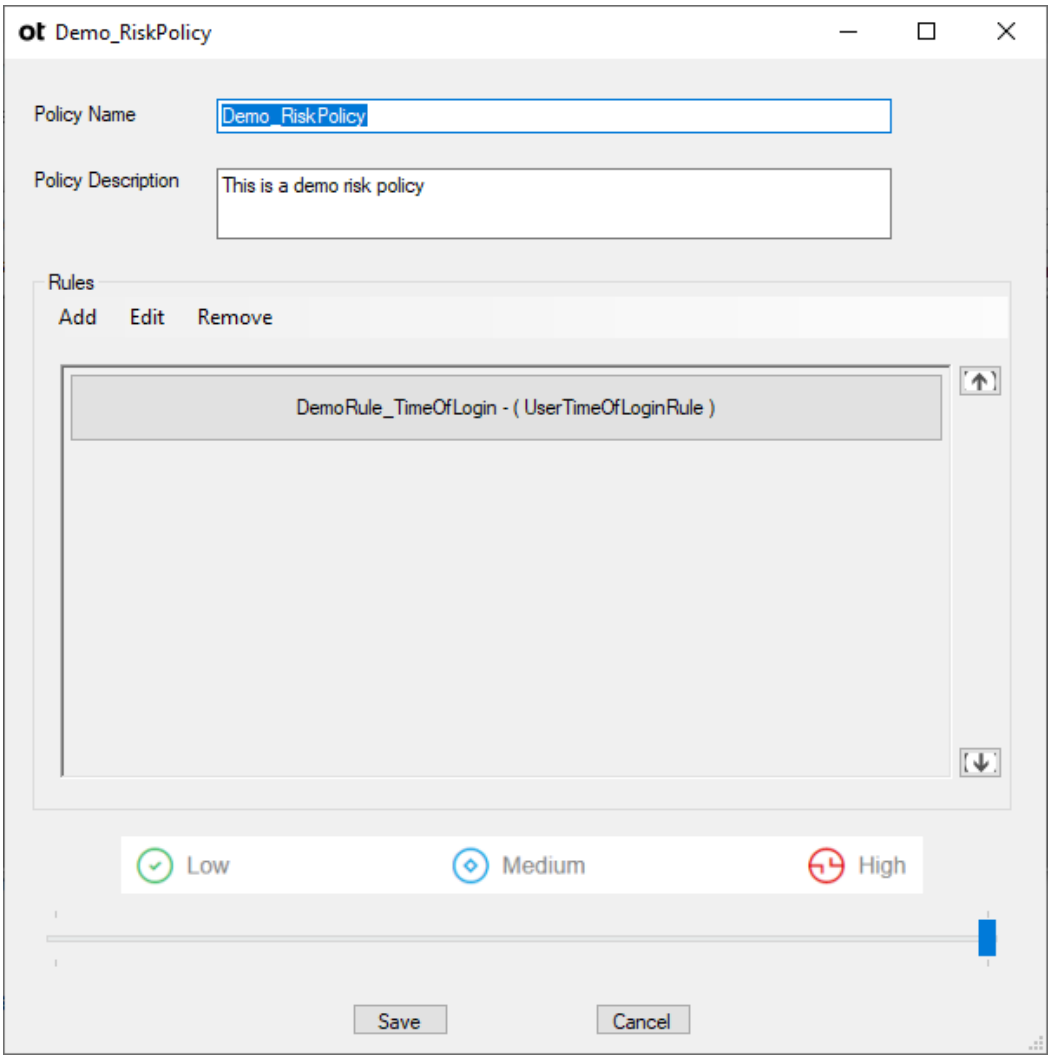
Get REST calls will return the requested information (IE rules, policies, etc.)
The Post and Put calls are for creating new or updating existing data.

For Policies, if you create a new or edit an existing policy then you will see a dialog similar to what you would see on an AAF admin console.

Post Policies – Create a new policy
Put Policy – Edit an existing policy

For example: Put Policy

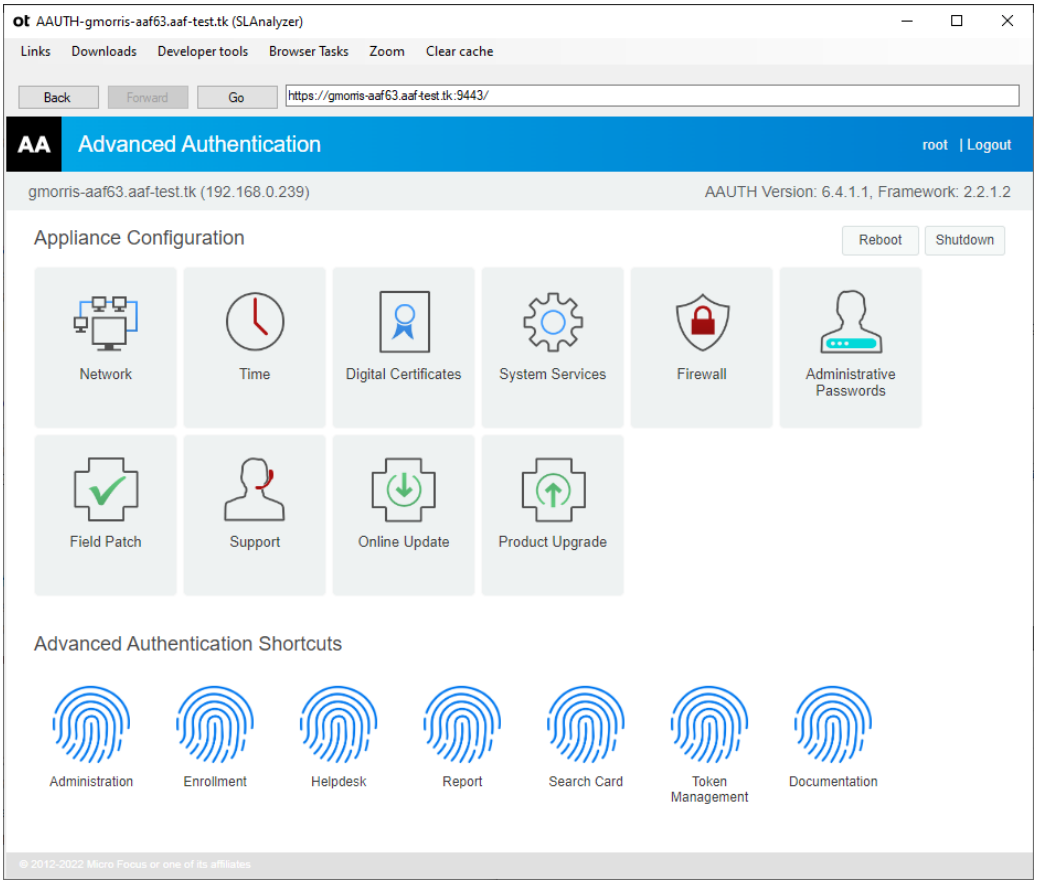




You can add new or existing rules with the Add menu.
Edit a rule or its action from the list from the Edit menu.
Remove a single rule or all rules from the Remove menu.
Change the order of the rules with the up/down arrows.
Set the risk failure rate with the slider bar.

Reset Local Admin Pwd

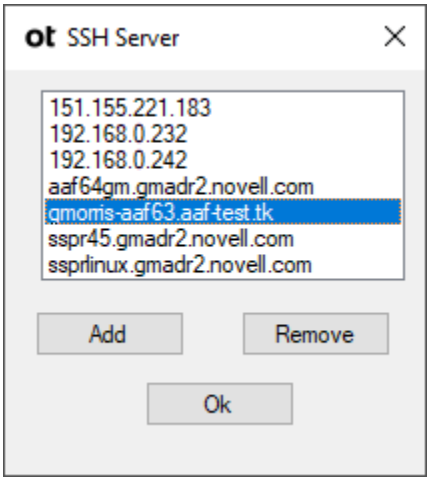
This option will allow the reset of the admin password in the AAF local repository. Note that this option requires SSH access to the appliance. If you are unable to access the appliance console, login to the session at the VMWare host and use YAST to enable the SSH service. If you can login to the appliance console, then click on the system services tile and enable/start the SSH service.



Remote Admin

The remote admin functions communicate directly with the AA PostGres database. This feature Is not meant to be a replacement for the normal AA admin portal. The purpose of these features is to allow reconfiguration of the server in cases where the admin portal cannot be accessed.

When executing the remote admin options SLAnalyzer will first request the SSH credentials to access the AA database. After successfully connecting via SSH, SLAnalyzer will directly send PostGreSQL commands to the server.





The features of the remote admin include:

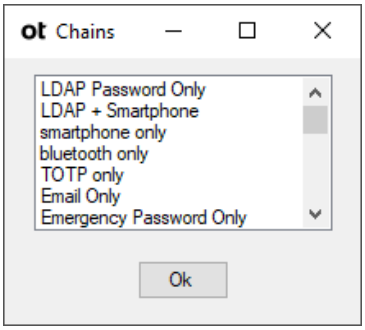
- Edit Chains
- Edit Endpoints
- Edit Events
- Edit User Roles
- View enrollment data
    - By User
    - By Method
- View license data
- User license consumption
- Initialize default event/chains
- Initialize default endpoints
- Repair Cached Groups

Edit Chains

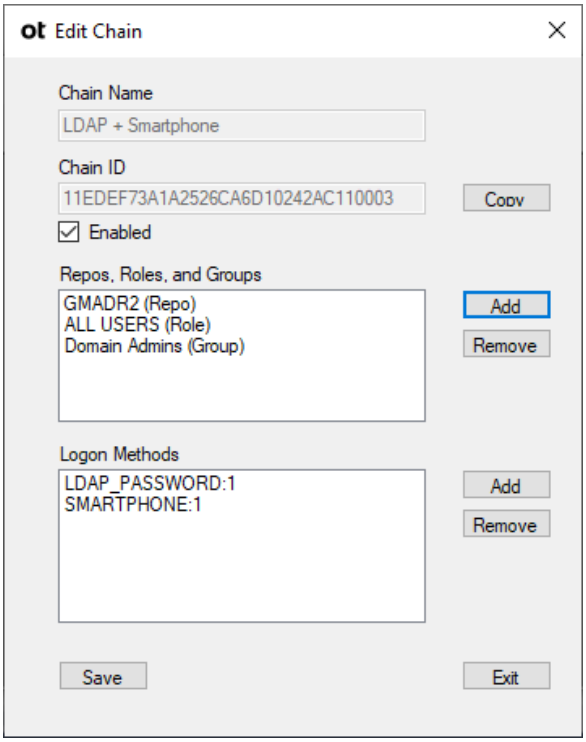
This option provides the ability to edit the configuration of a logon chain. The information that can be modified includes:

- Enabled/Disable
- Repo, Roles, and Groups
- Logon Methods

SLAnalyzer will first prompt for the chain to be edited. Select the desired chain and click Ok.



Edit the desired fields and then click the Save button.

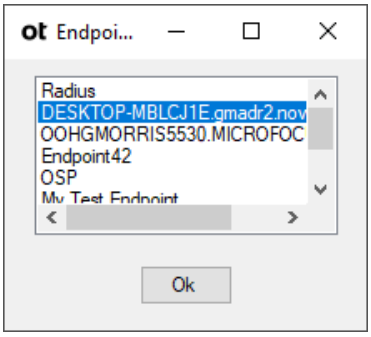


Edit Endpoints

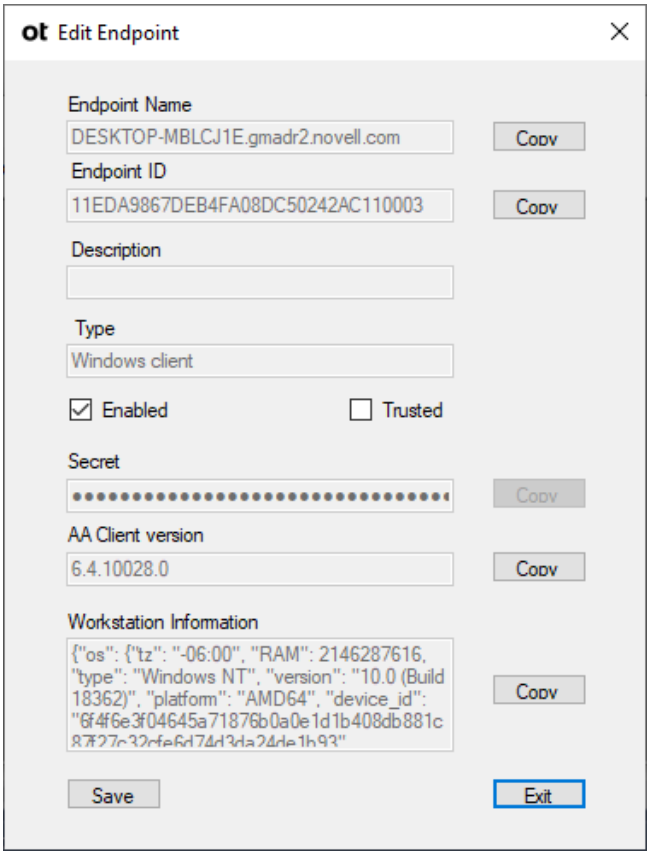
This option provides the ability to edit the configuration of an endpoint. The information that can be modified includes:

- Enabled/Disable
- Trusted/Untrusted

SLAnalyzer will first prompt for the endpoint to be edited. Select the desired endpoint and click Ok.



Edit the desired fields and then click the Save button.

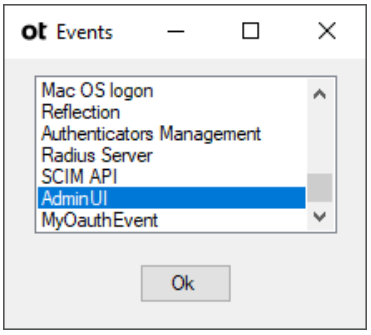


Edit Events

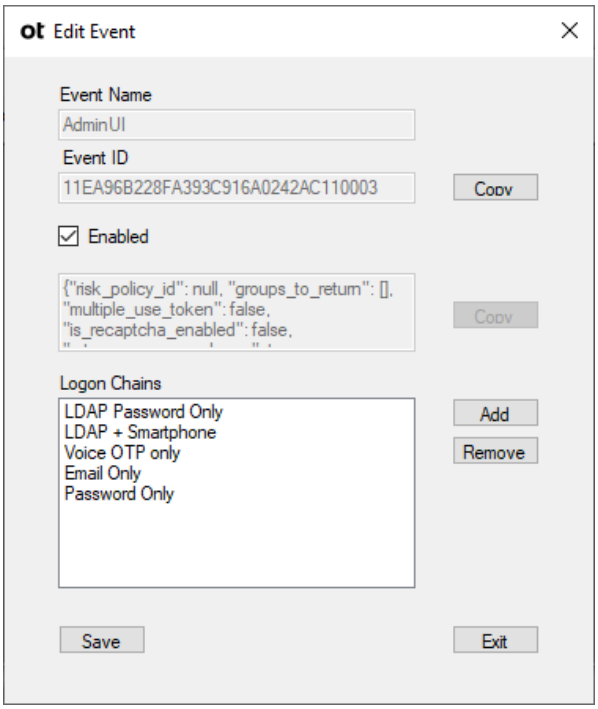
This option provides the ability to edit the configuration of an endpoint. The information that can be modified includes:

- Enabled/Disable
- Logon Chains

SLAnalyzer will first prompt for the event to be edited. Select the desired event and click Ok.



Edit the desired fields and then click the Save button.

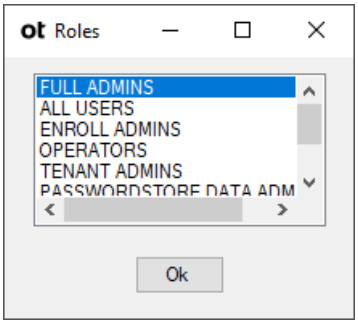


Edit User Roles

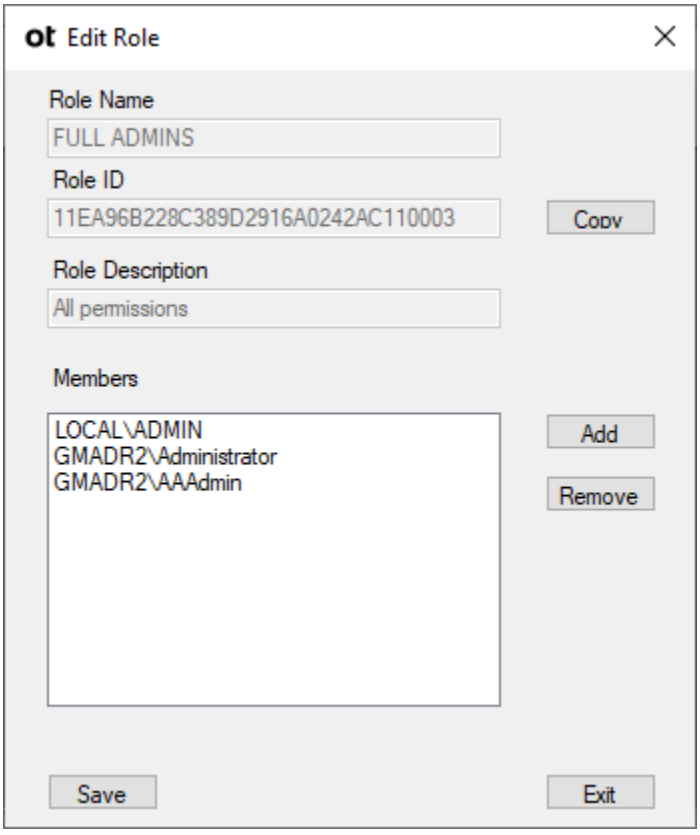
This option provides the ability to edit the configuration of a role. The information that can be modified includes:

- Members

SLAnalyzer will first prompt for the role to be edited. Select the desired role and click Ok.



Add or Remove Members and then click the Save button.



Note that only enrolled users can be added to a role assignment. If the user isn't displayed, then login to the enrollment portal as the user. After login then the user should then be available.

View enrollment data

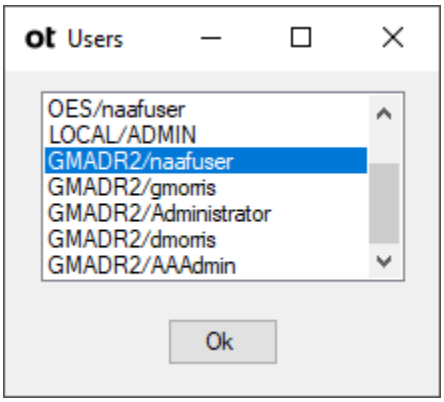
This option provides a view of the enrollments for a user or method.

- By User
- By Method

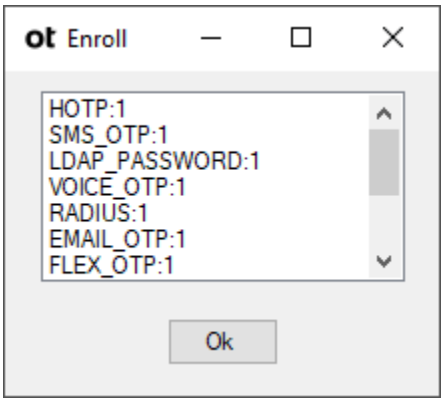
By User

This option will display all the enrollments by a specific user.

SLAnalyzer will first prompt for the user. Select the desired user and click Ok.



SLAnalyzer will query the database and report the enrollments found for the selected user.

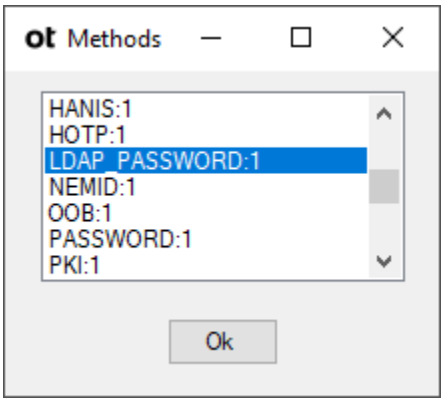


Right click within the table to save list to a file.

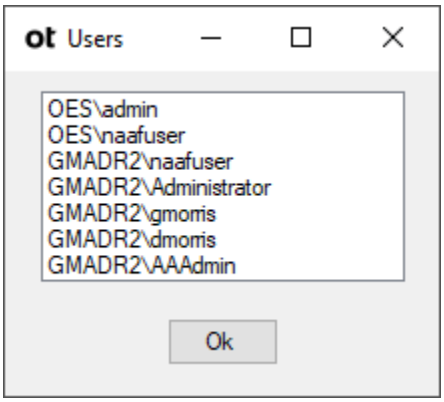
By Method

This option will display all the enrollments by a specific method.

SLAnalyzer will first prompt for the method. Select the desired method and click Ok.



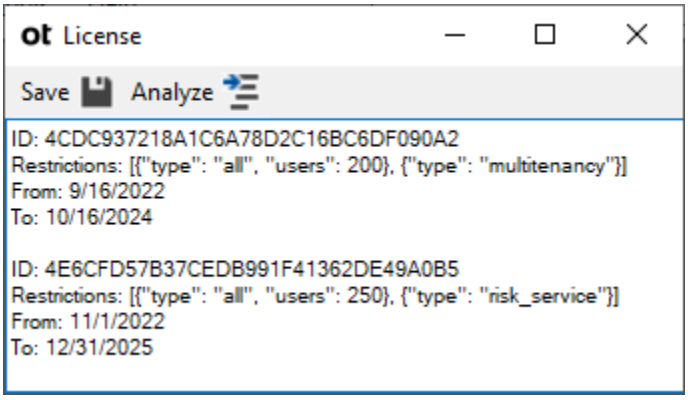
SLAnalyzer will query the database and report the users enrolled for the selected method.



Right click within the table to save list to a file.

View license data

This option provides the ability to view the installed licenses on the AA server.

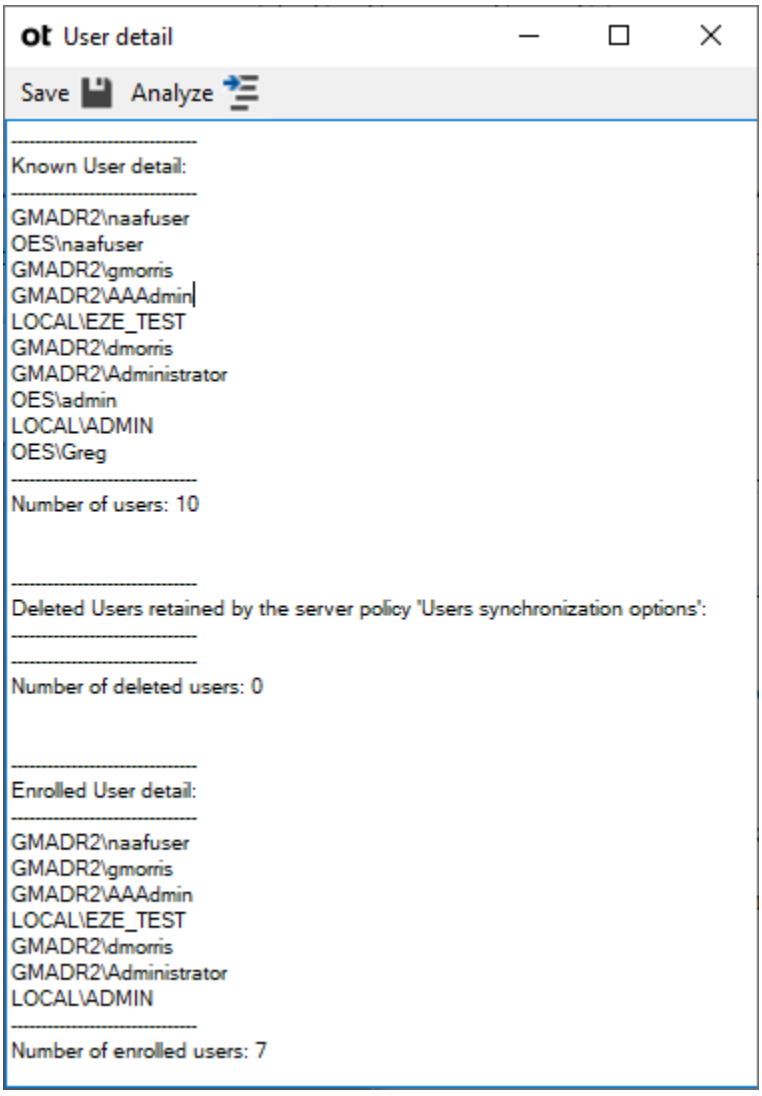


User license consumption

This option will query the database to determine the total number of licensed users.

The following information is displayed.

1. Known users – Users who have logged in at least once to the AA server
2. Deleted users – Users who have been deleted in the repository but are being retained by AA for a period of time as defined in the server policy 'Users synchronization options'
3. Enrolled users – The list of users who have 1 or more enrollments in the system



Note that the license consumption is based on the current AA 6.4 license modal. The information displayed in the admin portal should be considered as the authoritative source. If this report and the server have descrepencies, please use the admin portal values. For method based licensing (purchase x number of licenses for a specific method), then use the option View enrollment data by method report.

Initialize default event/chains

This option will recreate the default events and chains on the AA server. This option should be used when one of the default events or chains have been deleted or renamed. For example, if the password only chain has been deleted then logon with local\admin will result in an access denied message. This option would recreate the password only chain and assign it to the adminui event.

Initialize default endpoints

This option will recreate the default endpoints on the AA server. This option should be used when one of the default endpoints has been deleted or renamed. For example, if the Radius chain had been deleted then logon with the Radius event will fail. This option would recreate the endpoint so that internal processes will be able to properly connect via the Radius endpoint.

Repair Cached Groups

This option will analyze the cached groups for each repository and cleanup the cached group database table.

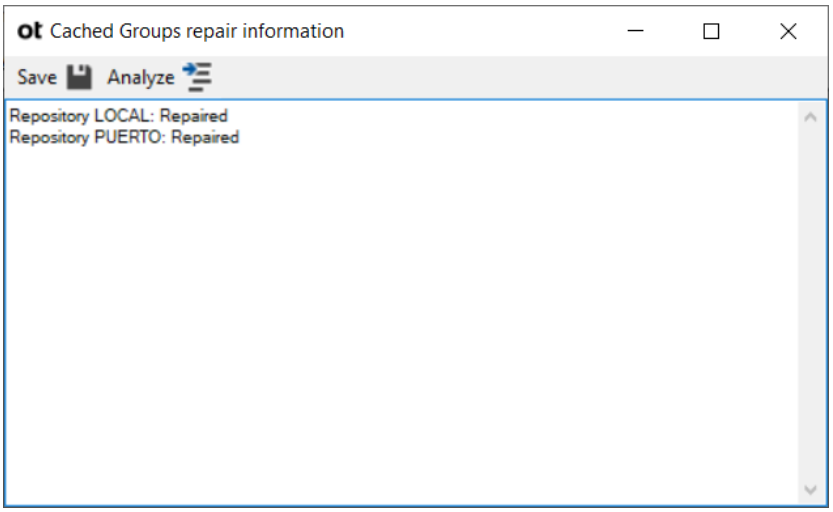
One symptom of the condition that this option is meant to resolve is the error “Multiple rows were found for one()” message being returned when performing a full sync on a repository in the admin portal.

Last fast synchronization |
| 18 minutes ago (2023-07-21 12:04 UTC)
| Last error: 18 minutes ago (2023-07-21 12:05 UTC)
| Multiple rows were found for one()

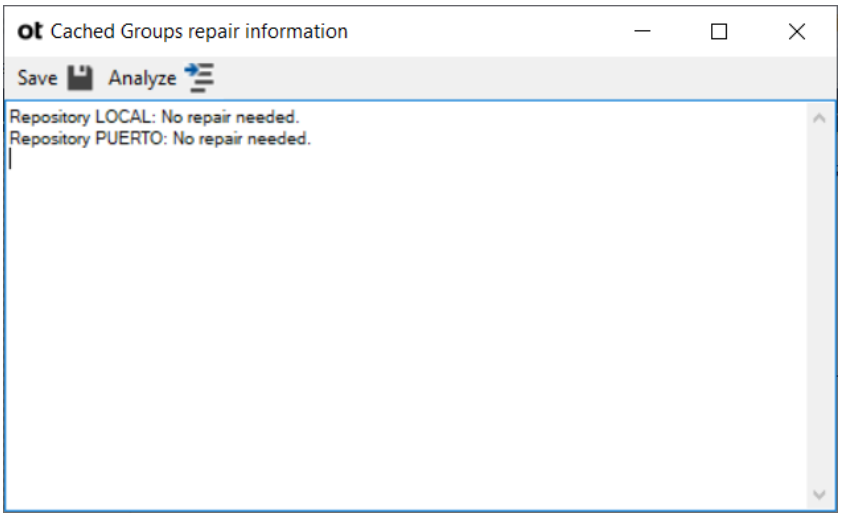
If duplicate records are found, then the cached groups for the repository are deleted. After this option is ran then a full sync of the affected repo needs to be performed to rebuild the list of cached groups.

After SLAnalyzer completes the cleanup process, it will then display a report to indicate what cached groups for repositories were repaired.

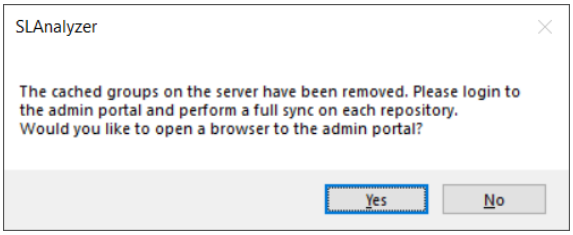
Duplicate cached groups found and repaired

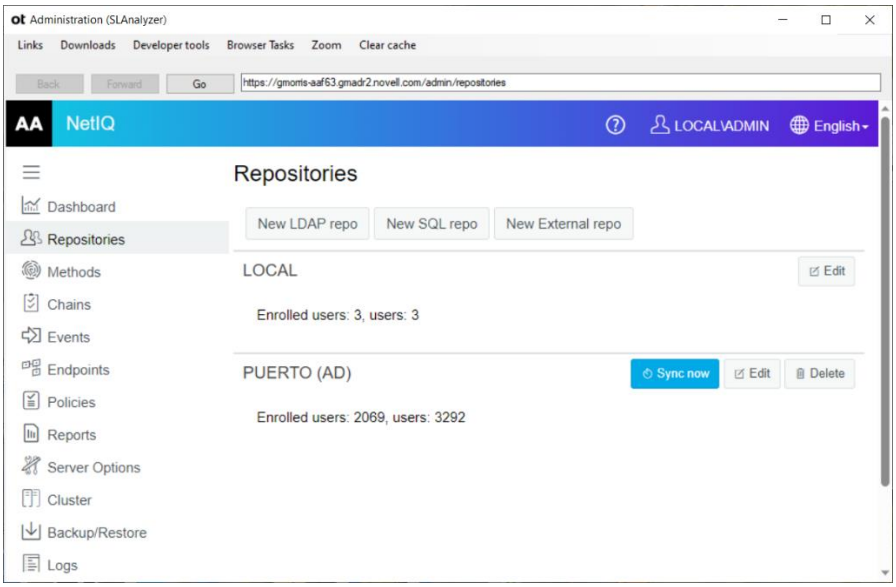


No duplicate cached groups found and no repair



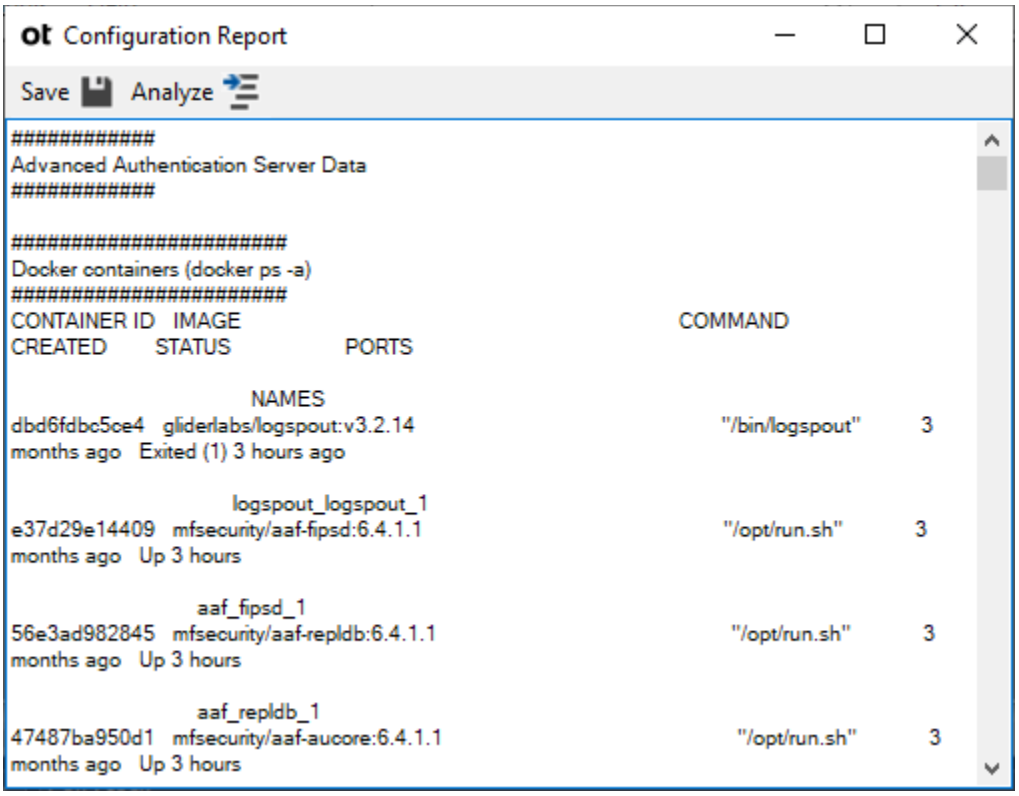
Once the report window is closed the user is prompted to open a browser window to the repository tab of the admin portal.





Gather Server Stats

This option will connect to the AAF server via SSH and gather information about the server. Note that this option requires SSH access to the appliance. If you are unable to access the appliance console, login to the session at the VMWare host and use YAST to enable the SSH service. If you can login to the appliance console, then click on the services icon and enable SSH.



Monitor Server Performance

This option creates a cron job that periodically generates performance related logs. These logs can then be analyzed to identify performance related issues.

There are several sub options for this option.

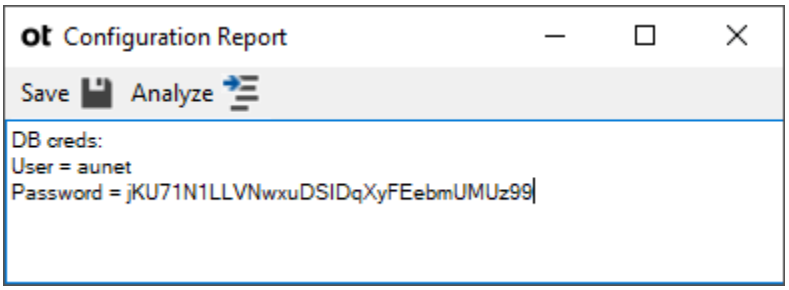
- Add – This option adds the cronjob to the server to start monitoring performance
- Check – This option checks for any current cronjobs configured on the server
- Remove – This option removes the cronjob from the server
- Download Logs – This option downloads the performance logs for analysis

Note that this option requires SSH access to the appliance. If you are unable to access the appliance console, login to the session at the VMWare host and use YAST to enable the SSH service. If you can login to the appliance console, then click on the services icon and enable SSH.

Find PostGres User

The AAF server utilizes a PostGres database. This database is protected by a random password generated at installation. If access to the PostGres database is needed (IE SQL Browser tool) then the user will need to know the user credentials to access the database. This option will login via SSH and read the appropriate configuration file to obtain the database credential data.

Note that this option requires SSH access to the appliance. If you are unable to access the appliance console, login to the session at the VMWare host and use YAST to enable the SSH service. If you can login to the appliance console, then click on the services icon and enable SSH.



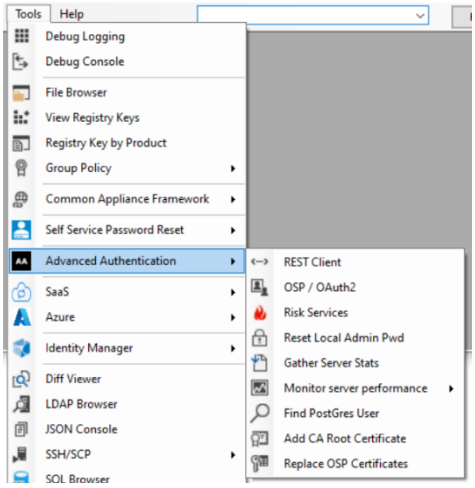
Add Root CA Certificate

By default, an AAF server will not trust a certificate from a local CA. This option allows the configuration of a local CA as a trusted root for the AAF server. The certificate to trust must be provided in PEM format.

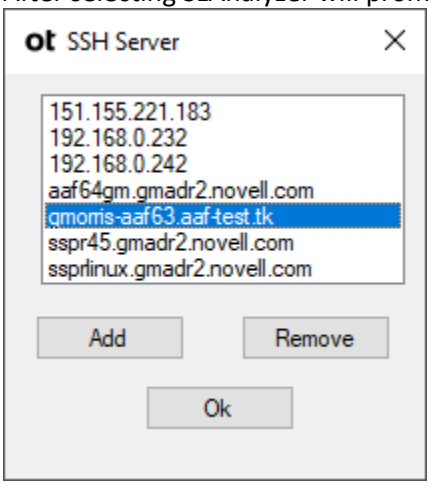
Note that this option requires SSH access to the appliance. If you are unable to access the appliance console, login to the session at the VMWare host and use YAST to enable the SSH service. If you can login to the appliance console, then click on the services icon and enable SSH.

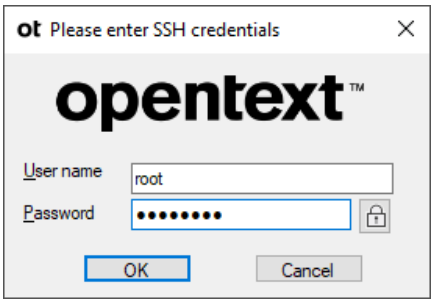
Replace OSP Certificates

[How to use commercial or custom certificates for OSP integration on an Advanced Authentication server (microfocus.com)]

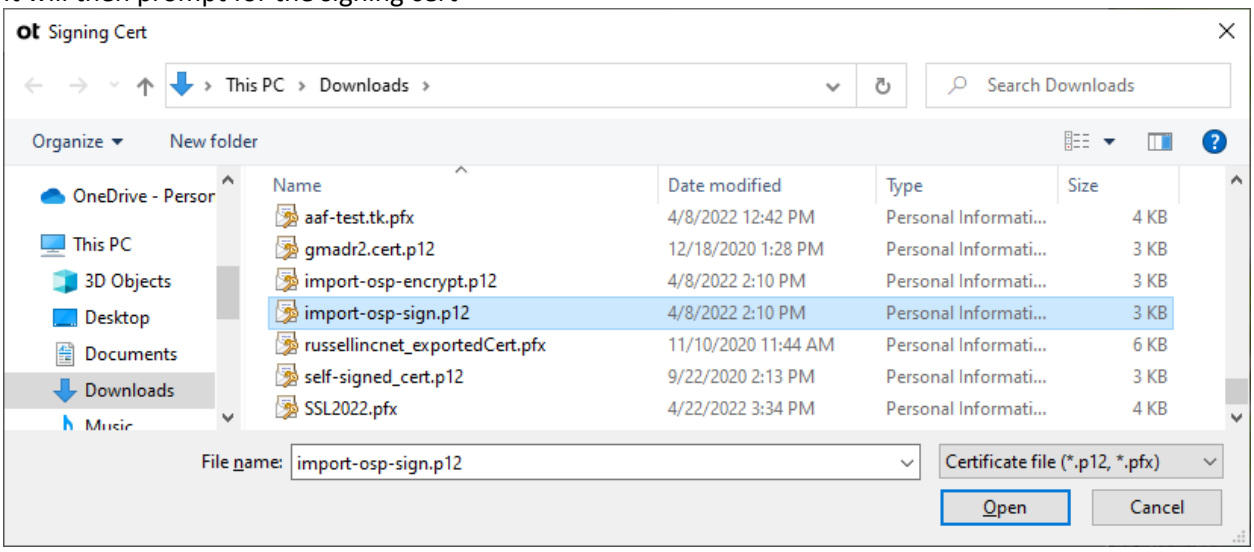


This feature will update the 2 certificates for OSP. Sign and encrypt.
After selecting SLAnalyzer will prompt for the SSH connection information.

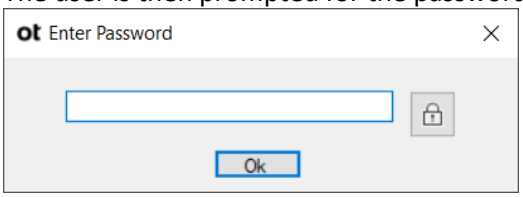




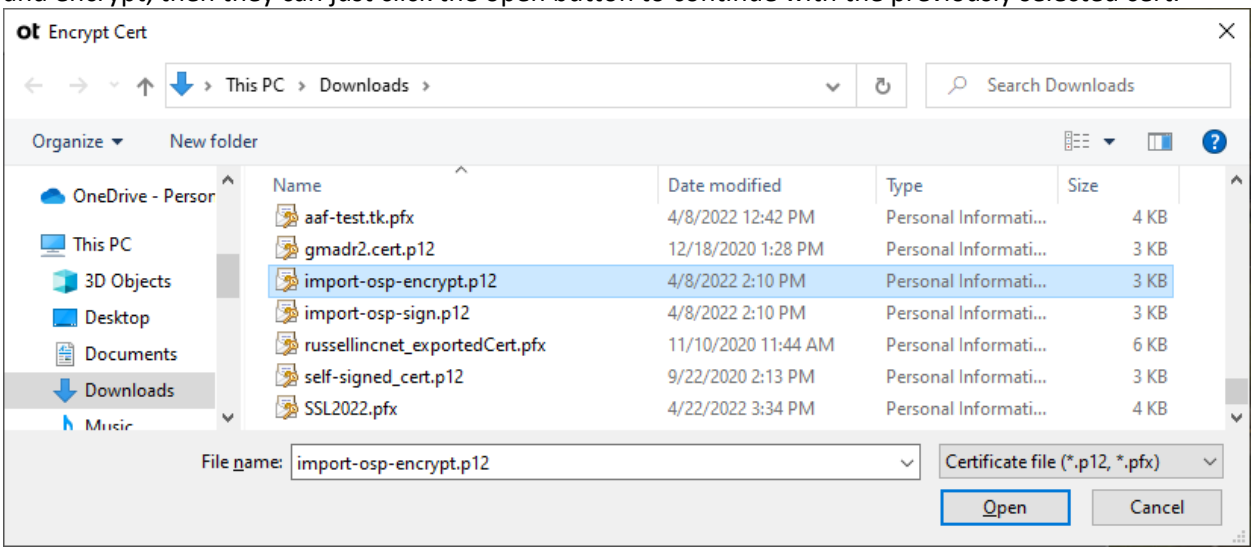
It will then prompt for the signing cert



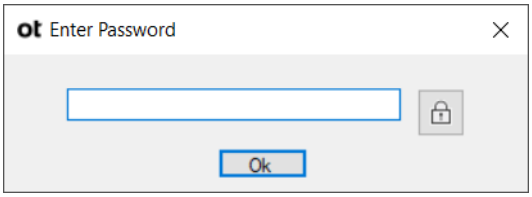
The user is then prompted for the password of the selected cert file.



This process is repeated for the encrypt cert. If the customer will be using the same cert for both sign and encrypt, then they can just click the open button to continue with the previously selected cert.



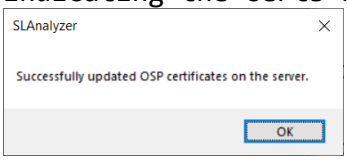
The user will again be prompted for the password for the cert file.



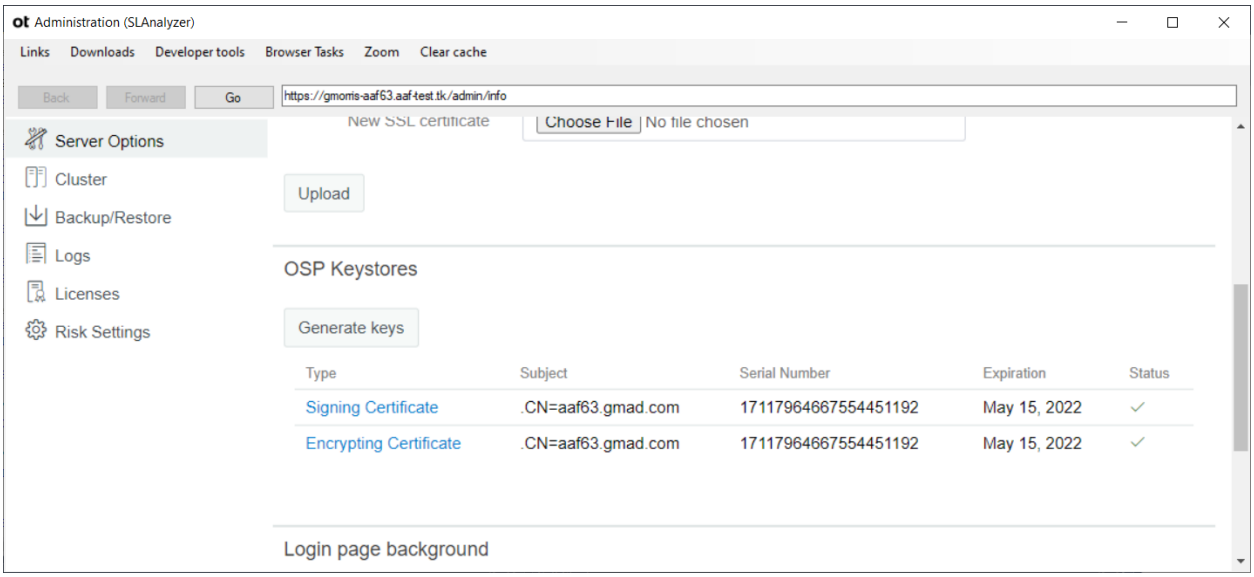
The certs will then be uploaded to the appliance.
The certs will then be processed and a simple name be set to osp
The certs password will also be changed to password
The cert names will be changed to the required names of:
`import-osp-sign.p12`
`import-osp-encrypt.p12`

After the certs have been processed then the script `/opt/AuCore/aucore/scripts/upload_osp_keystores.pyt` is executed on the `aaf_aucore_1` image.

If the process completes without error, then a message is displayed indicating the certs have been updated.



Server will now show the new certs for OSP. Note that you might have to refresh the admin page to see the new certs.



Reset Local Admin Pwd

This option allows for reseting the local\admin password.

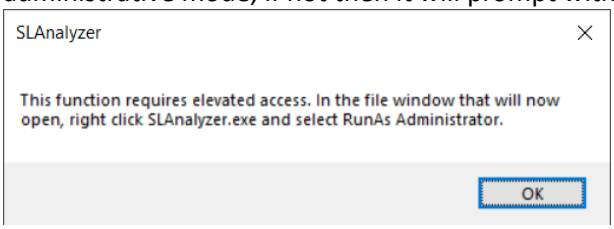
Note that this option requires SSH access to the appliance. If you are unable to access the appliance console, login to the session at the VMWare host and use YAST to enable the SSH service. If you can login to the appliance console, then click on the services icon and enable SSH.

OSP / OAuth2

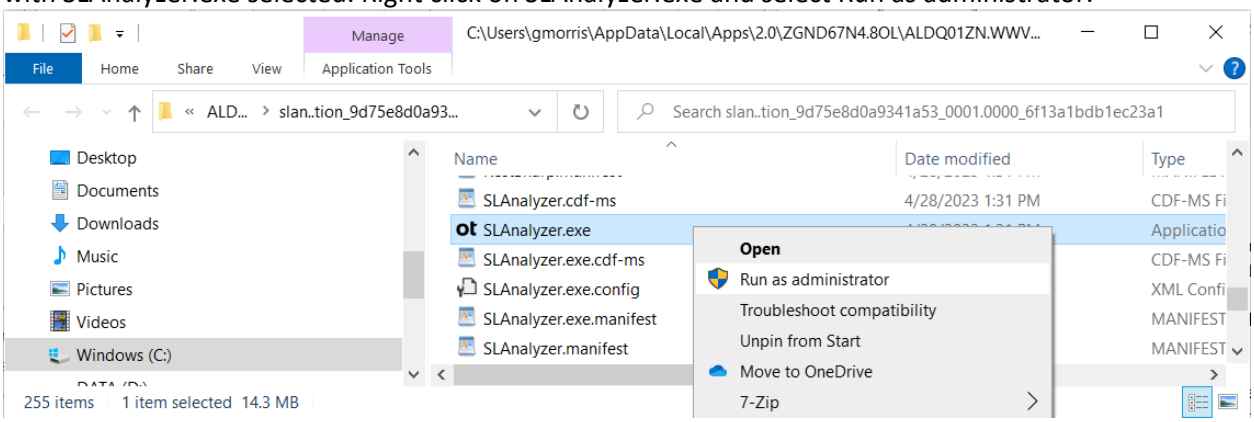
The OAuth2 tool demonstrates all the functionalities supported by OAuth 2.0 integration included in Advanced Authentication Framework and other equivalent products (IE NAM, IDM). OAuth 2.0 server is an authorization and resource server. As an authorization server the user goes through an authentication chain. As a resource server some user details are provided. The first 2 options can be used to test IDM/OSP/OAuth2 functionalty.

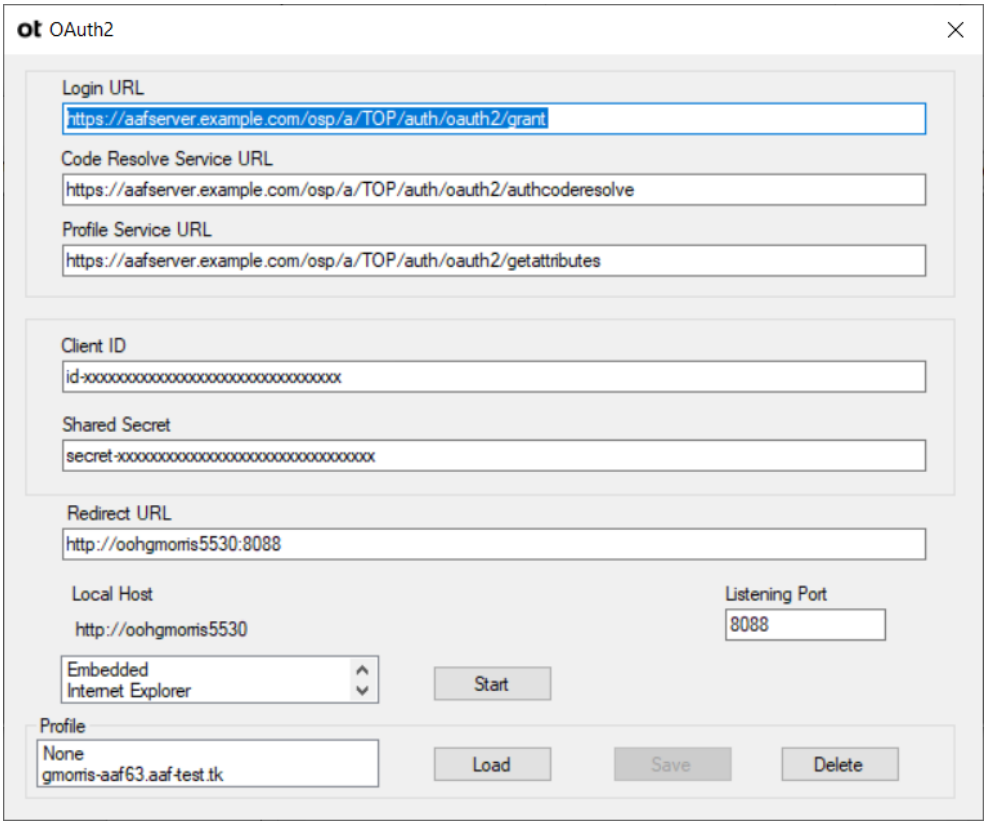
The OAuth2 tool is built using the sample Python code documented in the AAF administration guide. https://www.netiq.com/documentation/advanced-authentication-56/server-administrator-guide/data/t42zd5ff2xn7.html

This tool requires administrative access. When selected SLAnalyzer will evaluate if it is running in administrative mode, if not then it will prompt with this message…



After clicking the Ok button, SLAnalyzer will automatically close, and an explorer window will appear with SLAnalyzer.exe selected. Right click on SLAnalyzer.exe and select Run as administrator.





When you launch the OAuth2 tool the user will need to fill in the necessary information for the API. You can store and retrieve information with the Profile data options. Please refer to the profile options documented in the SSPR REST client.
Profile data is stored at: HKEY_CURRENT_USER\Software\MicroFocus\SLAnalyzer\OAuth2

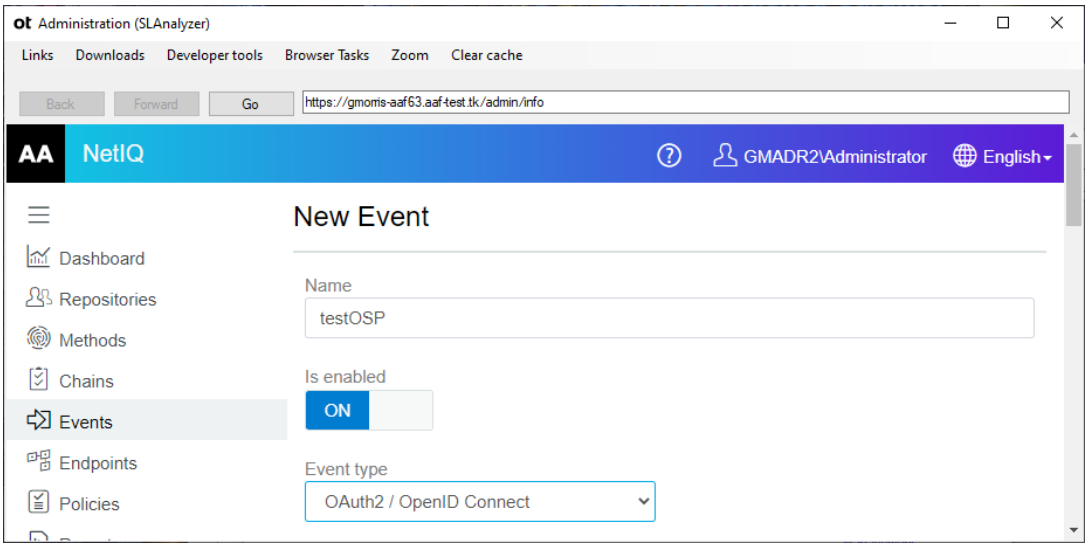
To setup OAuth2 you must perform the following steps.

1. Create OAuth Event on AAF server console
    a. Event type = OAuth2
    b. Enable Used chains for authentication
    c. Copy Client ID and Client Secret
    d. Specify Redirect URI
2. Enable OAuth services on AAF console (AAF 5.x)
3. Configure SLAnlyzer OAuth2 settings
4. Click Start button
5. Navigate OAuth2 test page

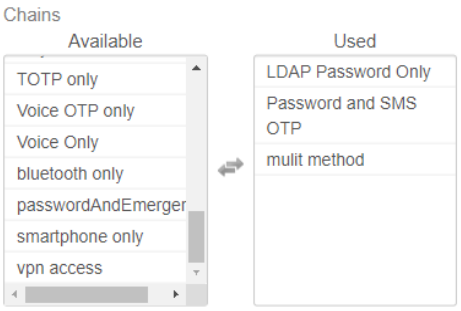
Create OAuth2 Event

First login to the AAF server console and create a new event.

You can name the event anything you like. In our test we will create one with the name testOSP.
Make sure “Is enabled” is set to ON
Click on the Event type drop down and select OAuth2

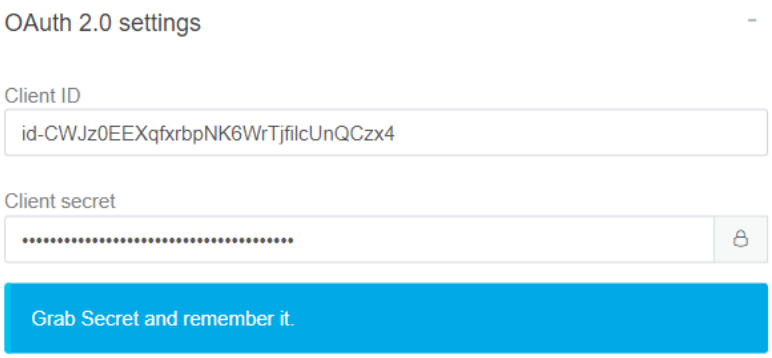


The next step is to indentify the chains required for user authentication. The “Available” box displays the chains that could be selected. The “Used” box displays the events that will be presented to the user. For our testing we will be using the LDAP Password only chain.

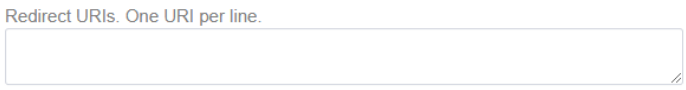


For the user to pass OAuth2 authentication then they will need to successfully authenticate with one of the defined chains. We could define a chain that requires multiple methods but for our test we will limit our methods to one.

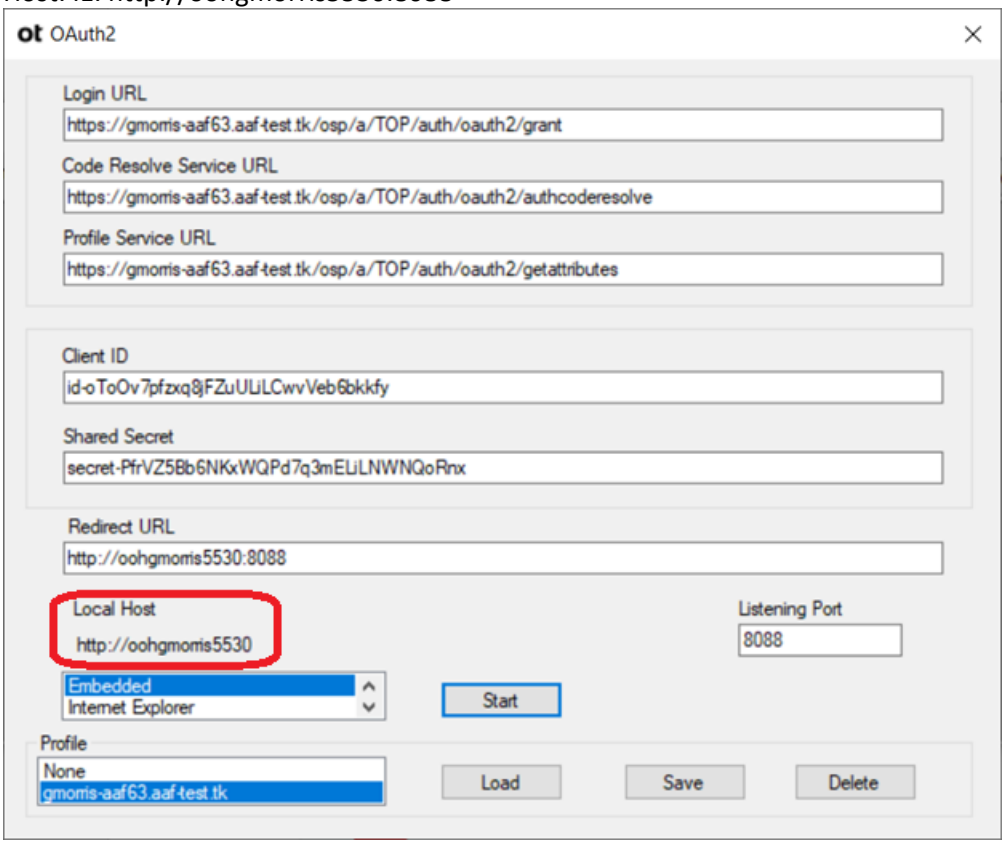
When creating the event, the fields Client ID and Client secret need to be copied down so that we can enter them into SLAnalyzer or application being setup for OAuth2.



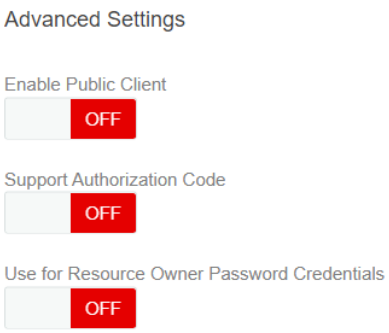
The final setting to configure is the Redirect URL. When the OAuth2 request is made to the server, part of the request includes a redirectURL. The OAuth2 server will redirect to the URL specified after a successful user authentication. For testing with SLAnalyzer we will need the redirect URL to point back to the workstation running SLAnalyzer. For testing of URL redirection this value could be set to forward to another website. (IE. https://www.google.com).



You can see the redirect url for the SLAnalyzer test page on the main OAuth2 window labeled as Local Host. IE. http://oohgmorris5530:8088



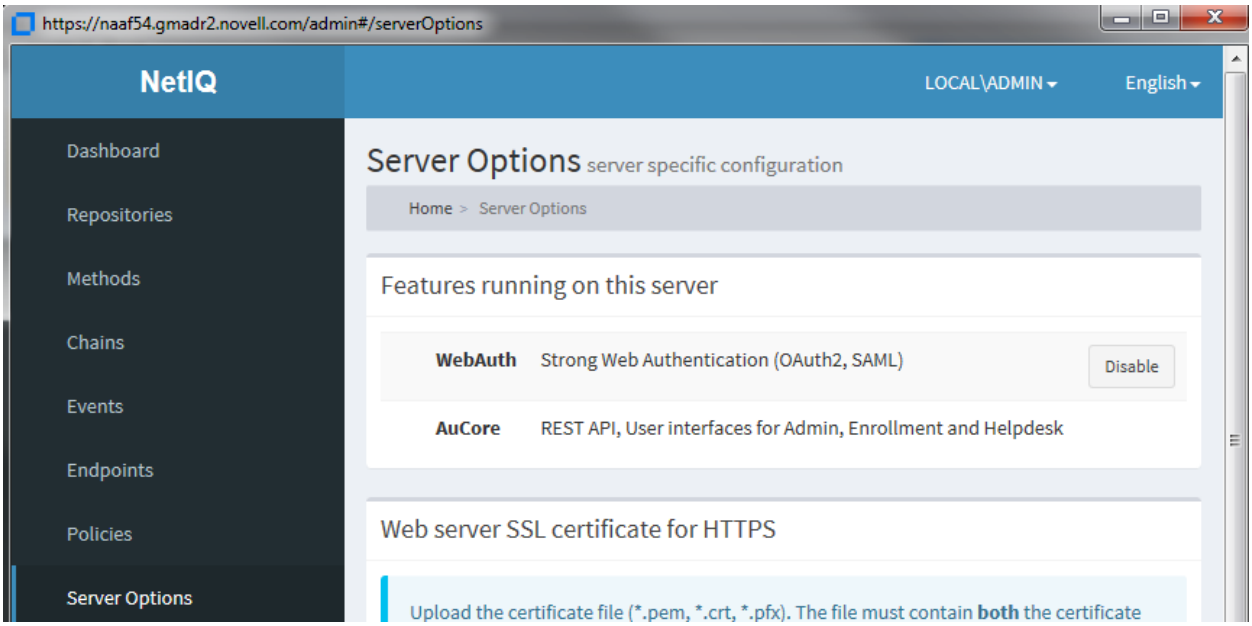
There are multiple “Advanced settings” for OAuth2. The SLAnalyzer OAuth2 tool provides 3 options. The first two options require the setting “Use for Resource Owner Password Credentials” to be turned OFF. The 3rd option requires this setting to be turned ON.



In AAF 5.x, after configuring the event then the service needs to be enabled.

Enable OAuth services

In AAF 5.x, by default the WebAuth service is not enabled. You must enable this feature for OAuth2 to function. For AAF 6.x servers the WebAuth service is always enabled and this section can be ignored.



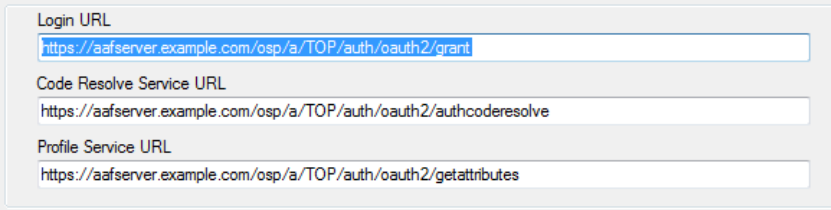
Now the AAF server should be configured properly for OAuth2 communications. Now configure SLAnalyzer to communicate with this new event.

SLAnalyzer OAuth2 settings

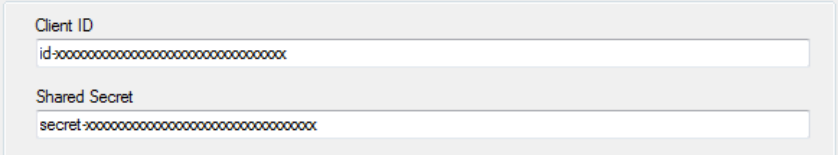
To configure OAuth2 we must specify the following information

- URLS
- Client application
- Redirect URL and Port

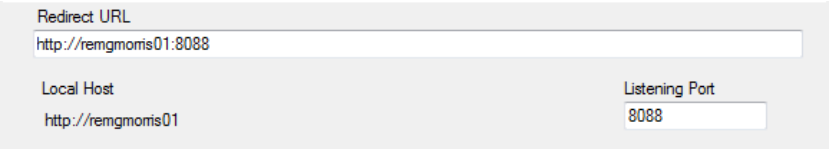
The URLs are common across all OSP platforms. This would include AAF and/or IDM. Change the URL data to reflect the OAuth2 server being used. Only change the server DNS/IP information.
For example, aafserver.example.com to myserver.mycompany.com.



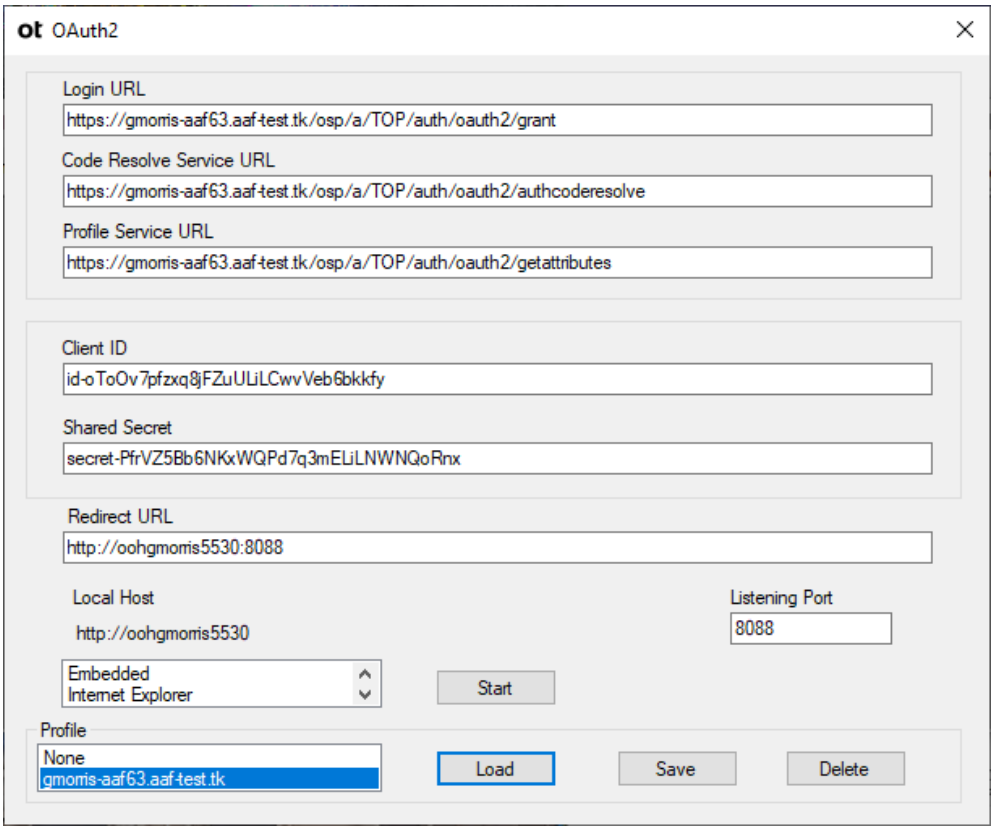
The Client ID and Shared Secret were provided when creating the AAF event. For IDM the ID is found in the xml files.



The Redirect URL is built from the defined listening port. If you change the Listening port then the Redirect URL will also change. The Redirect URL must match the Redirect URL specified in the OAuth2 event created earlier. For testing redirection this event could point to another web service/page. IE https://www.google.com.



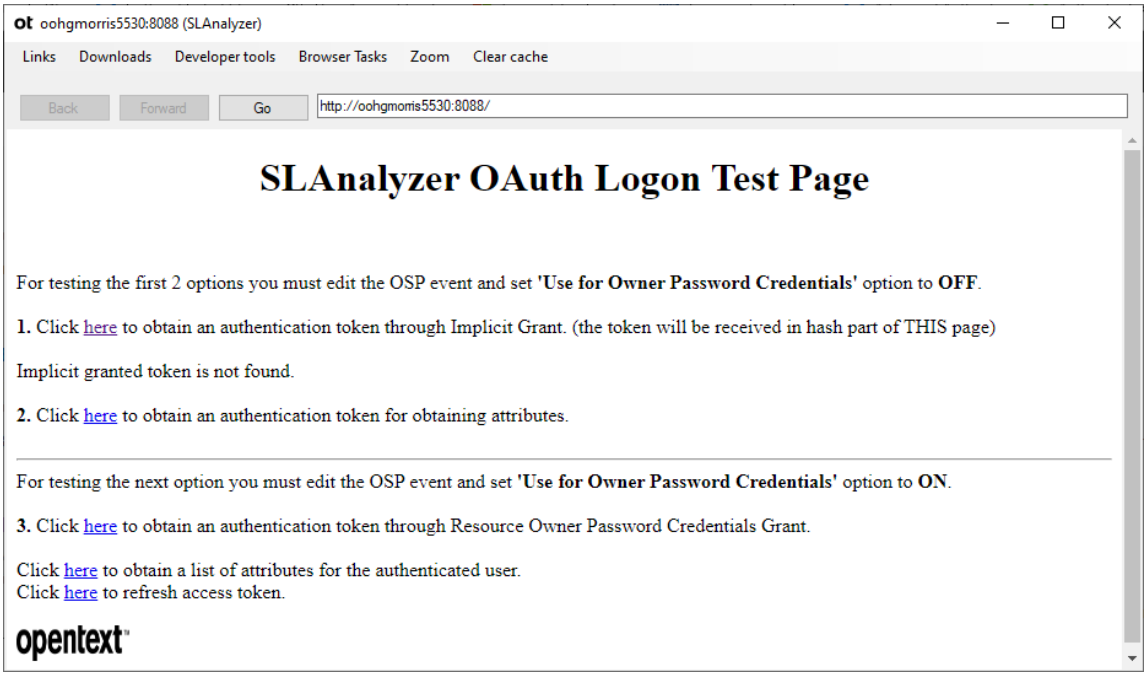
By default, the embedded browser will be used when clicking the Start button. Optionally the user can select a different browser to invoke Internet Explorer, Edge, FireFox, or Chrome.



After configing the OAuth2 settings then click the start button. SLAnalyzer will start listening on the specified port for OAuth2 requests. It will also launch the selected browser with the SLAnalyzer OAuth Logon Test Page. If the browser is not selected, then the embedded browser will be utilized.

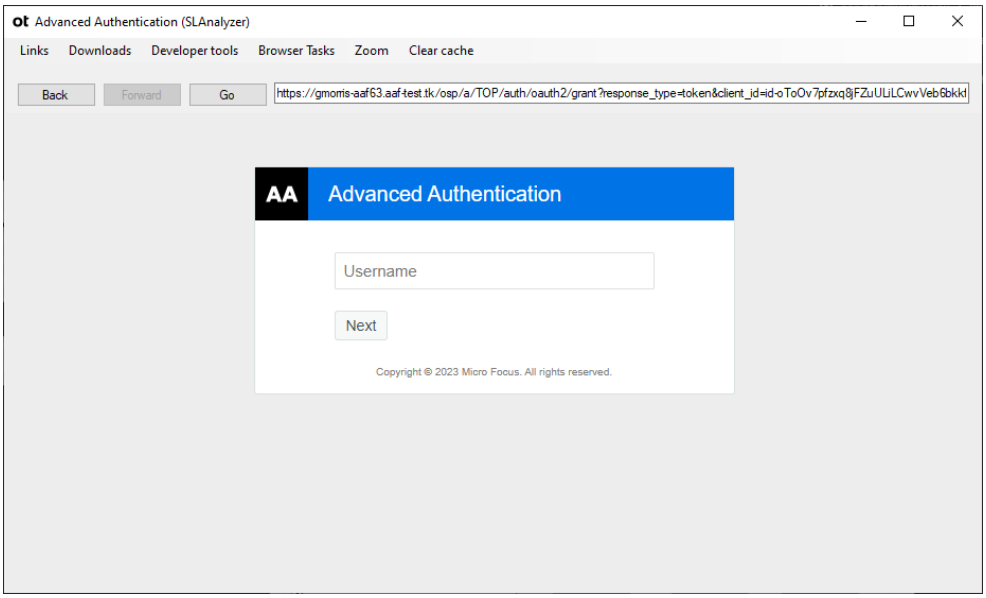
Navigating the SLAnalyzer OAuth2 Logon Test Page

After the page loads successfully, there are 3 login options presented.

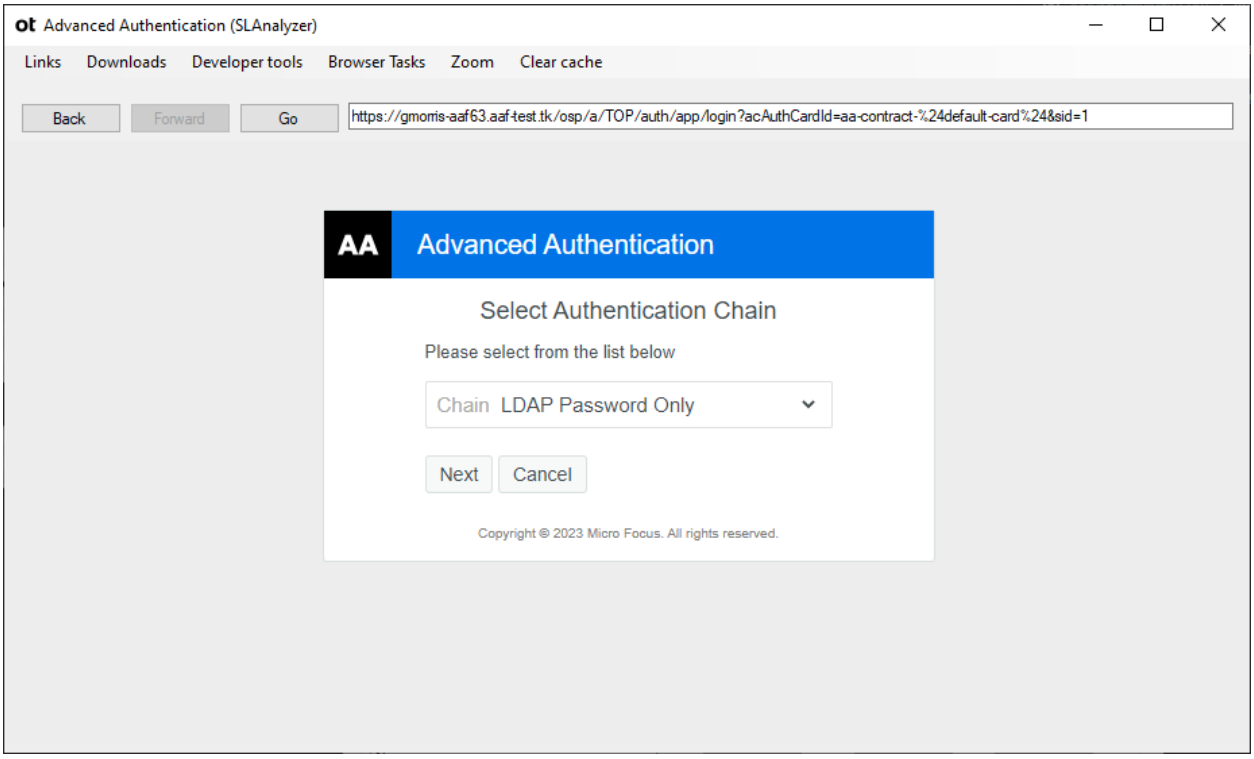


Item 1 will return the access token in the returned URL. This information is then displayed within the page for easy viewing.

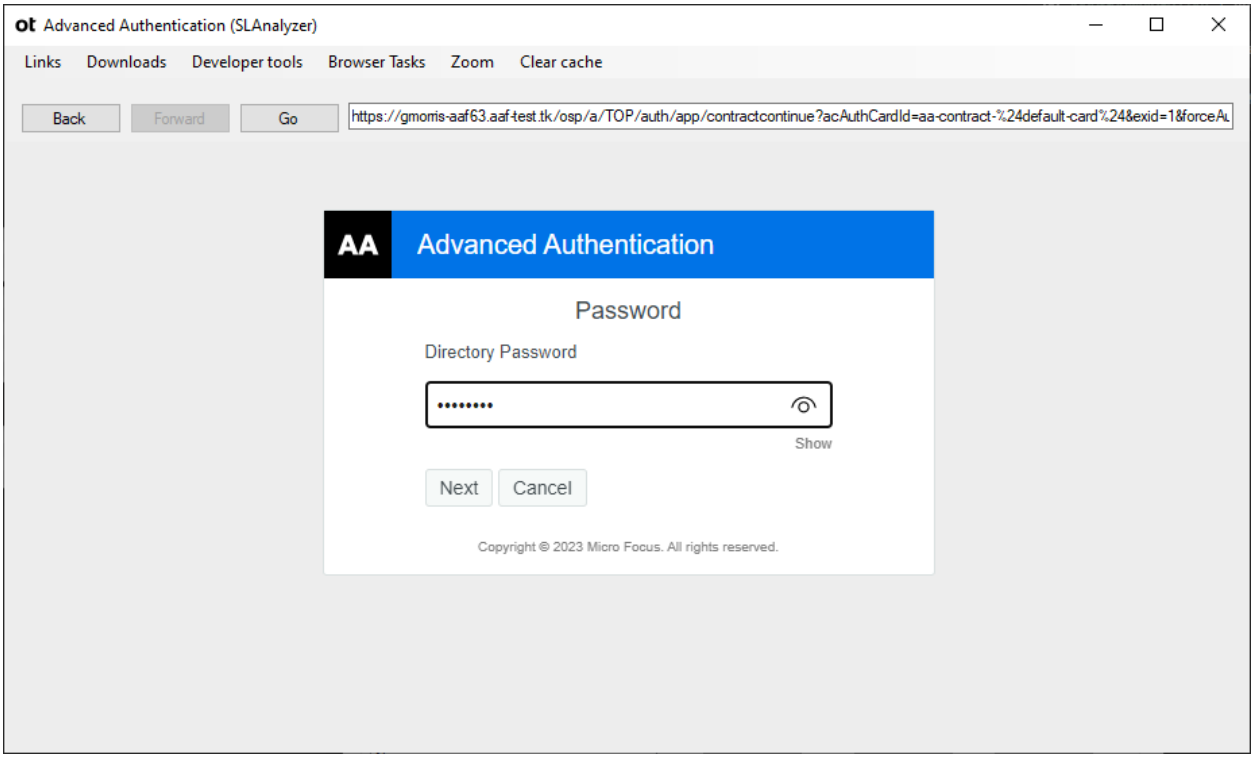
First the Oauth server needs to obtain the users name.



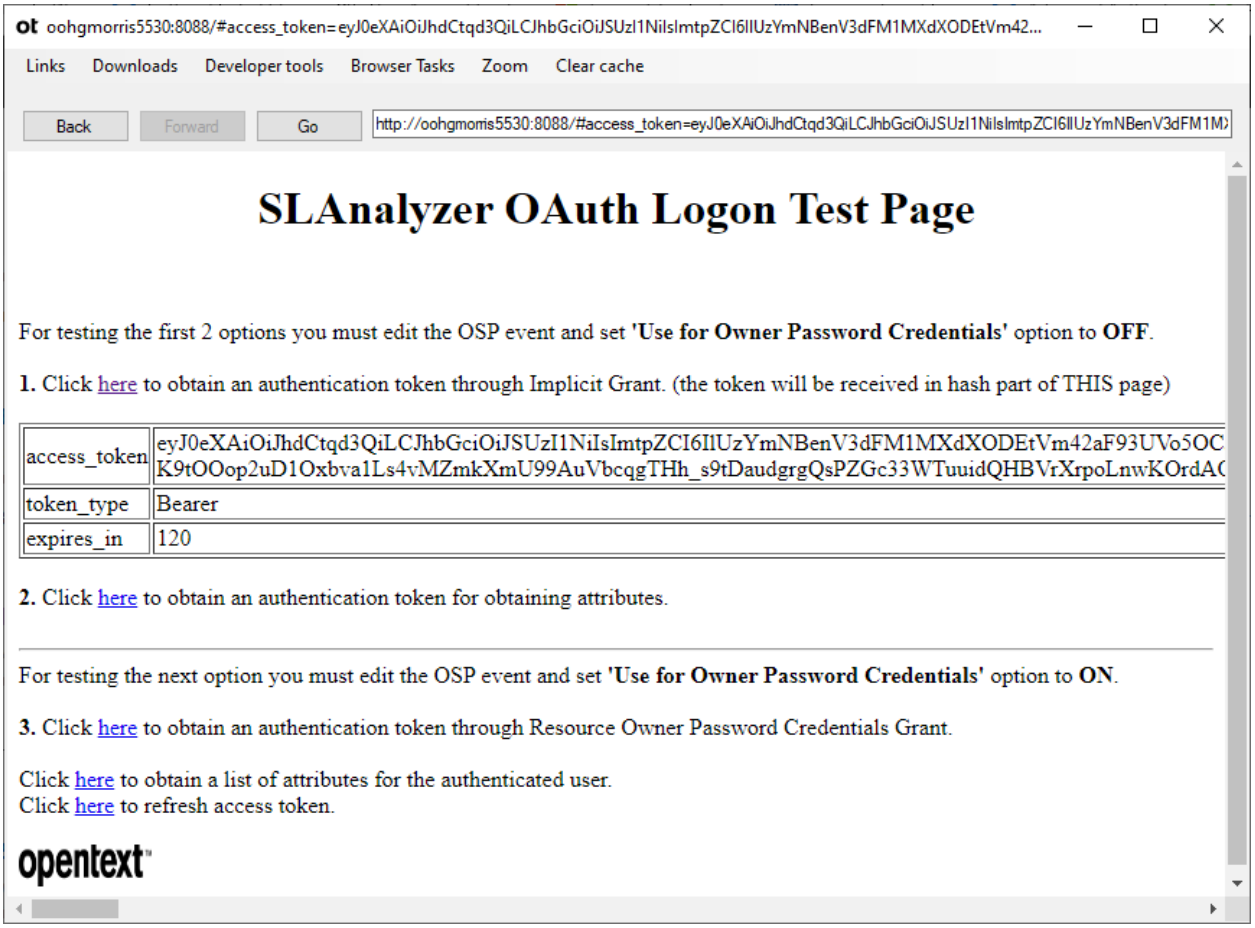
The Oauth server will now prompt the user to select the desired chain.



The user is then prompted to provide the input for the selected logon chain.

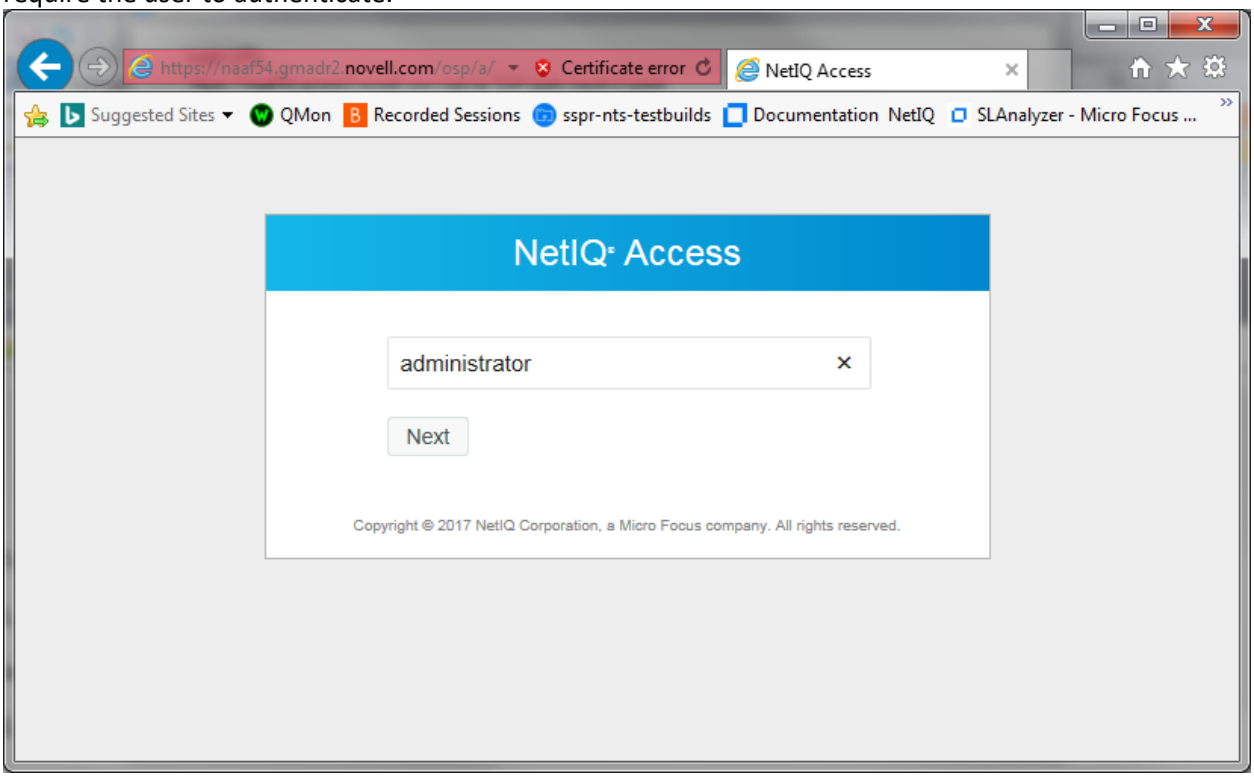


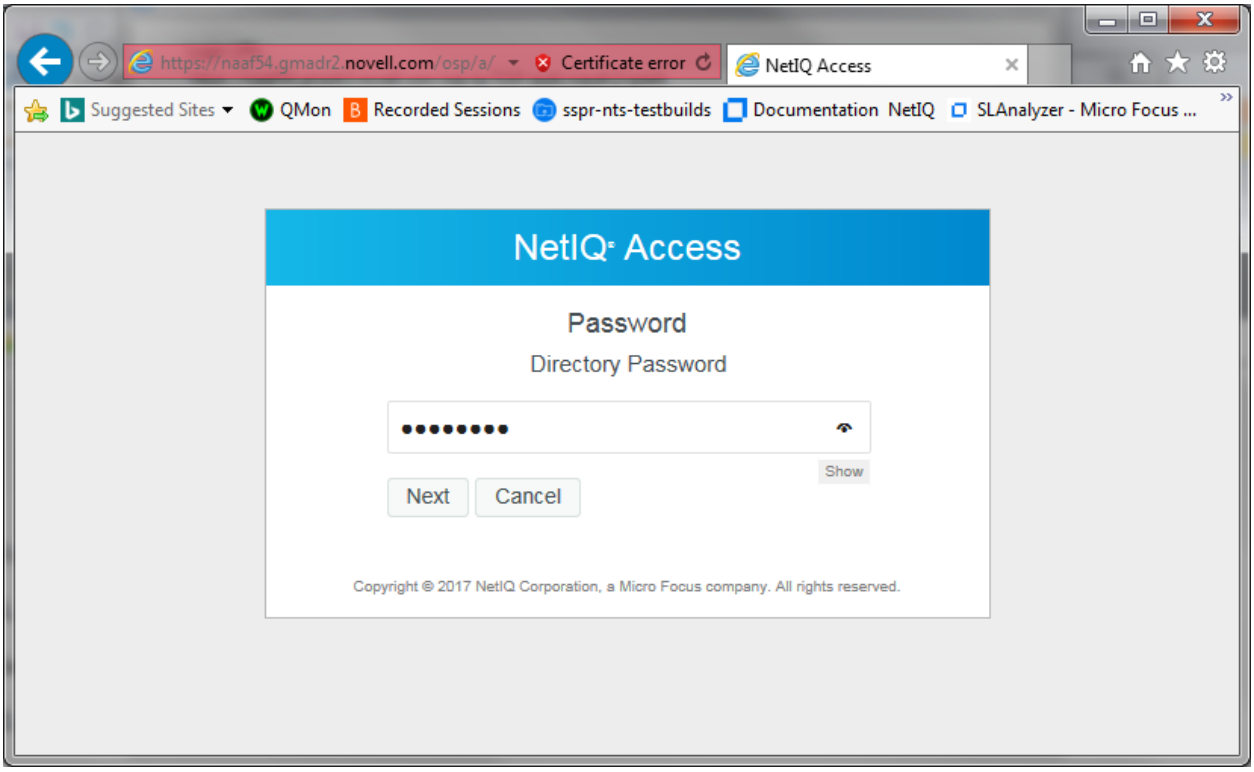
Once logged in, the test page is updated with the received access token.



Logon and obtaining an access token

Options 1 and 2 require the event Advanced setting “Use for Owner Password Credentials” set to ‘OFF”. Click on Option 2 to obtain an access token we can use for getting attribute data. The server will require the user to authenticate.



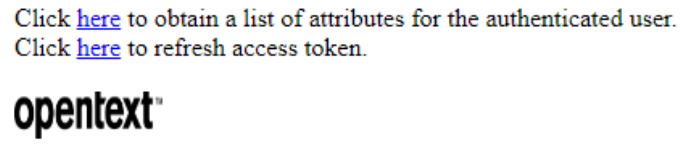


After user authentication completes then the OSP server returns an access token. SLAnalyzer will popup a window with the token information

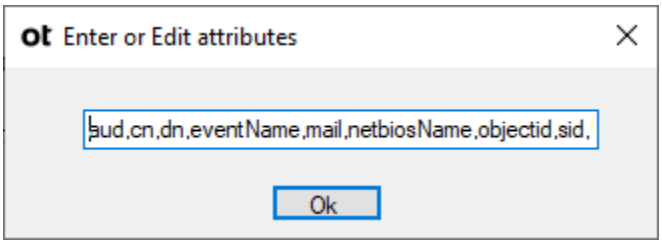


Obtaining attribute data:

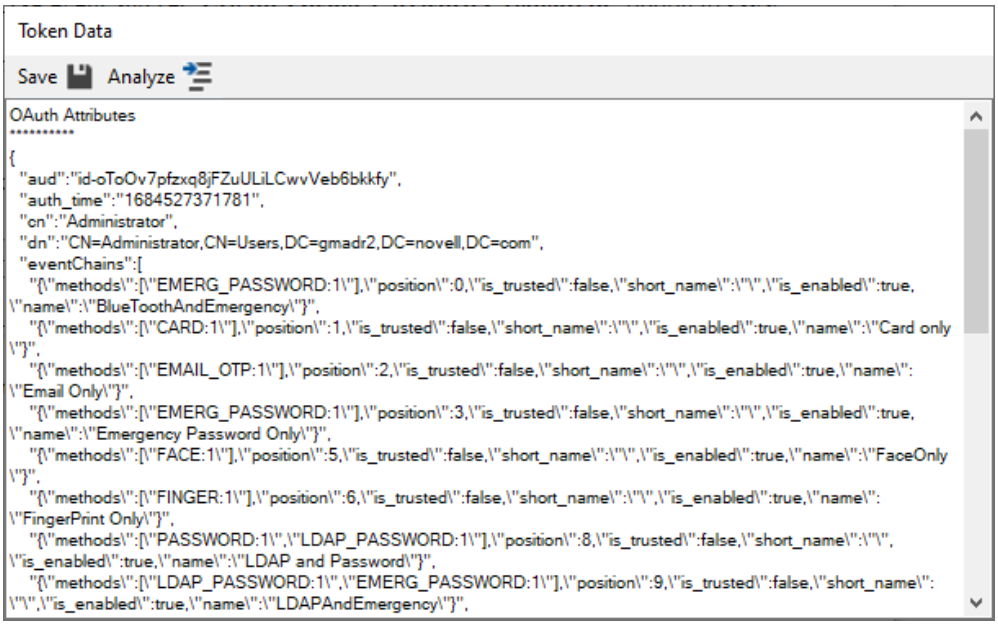
At the bottom of the SLAnalyzer OAuth Logon Test Page click on the option to obtain a list of attributes.



opentext™

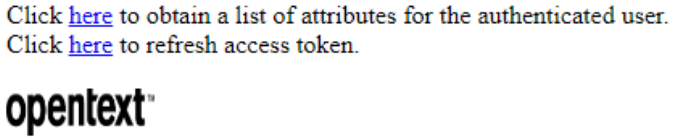


The SLAnalyzer popup window will display the attribute information returned from the OSP server.



Refreshing the access token

Click on the last option to refresh the access token



opentext™

SLAnalyzer updates the popup window with the new access token information.

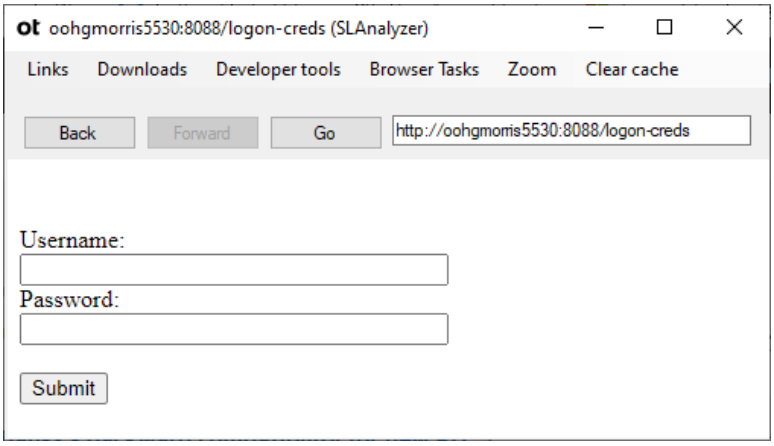
Token Data

Save Analyze

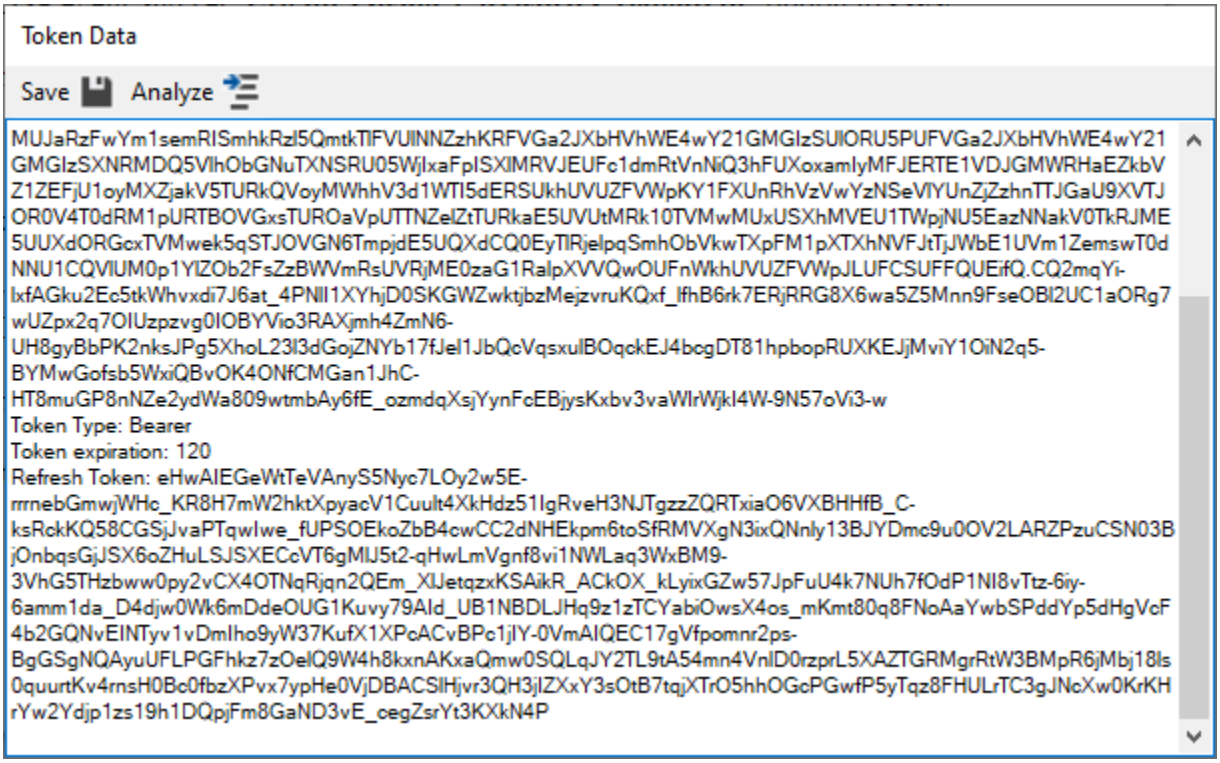
Access Token:
eyJ0eXAiOiJhdCtqd3QiLCJhbGciOiJSUzI1NiIsImtpZCI6IlUzYmNBenV3dFM1MXdXODEtVm42aF93UVo5OCJ9.eyJpc3MiOiJodHRwczovL2dtb3JyaXMtYWFmNjMuYWFmLXRlc3QudGsvb3NwL2EvVE9QL2F1dGgvb2F1dGgyliwiZXhwIjoxNjg0NTI3NTYwLCJuYmYiOjE2ODQ1Mjc0NDAsImlhdCI6MTY4NDUyNzQ0MCwianRpIjoiRVQ5cGNCdnpUZjJQbnh1ZDlmN0FuQSIsImNsaWVudF9pZCI6ImlkLW9Ub092N3BmenhxOGpGWnVVTGlMQ3d2VmViNmJra2Z5liwic3ViIjoiYXNcXC1hYS02NTczZjJhNmY0MzE3ZWMxMTRmN2VlMTVmYzk0OGM5MCIsInR4bil6ImhIR3pIVy0xUmFLaHRKVFVBNy1GWVEiLCJhdWQiOiJpZC1vVG9PdjdwZnp4cThqRlp1VUxpTEN3dlZlYjZia2tmeSIsImF1dGhfdGltZSI6MTY4NDUyNzA2MiwiYW1yIjpbInB3ZCJdLCJfcHZ0IjoiQUM0QllnSlFBTnJGbHdFZ05qVTNNMll5WVRabU5ETXhOMlZqTVRFMFpqZGxaVEUxWm1NNU5EaGpPVEFOWVdSdGFXNXBjM1J5WVhSdmNnMUJaRzFwYm1semRISmhkRzl5QmtkTlFVUlNNZ29KRFVGa2JXbHVhWE4wY21GMGIzSXlORU5PUFVGa2JXbHVhWE4wY21GMGIzSXNRMDQ5VlhObGNuTXNSRU05WjIxaFpISXlMRVJEUFc1dmRtVnNiQ3hFUXoxamlyMFJERTE1VDJGMWRHaEZkbVZ1ZEFjU1oyMXZjakV5TURkQVoyMWhhV3d1WTI5dERSUkhUVUZFVWpKY1FXUnRhVzVwYzNSeVlYUnZjZzhnTTJGaU9XVTJOR0V4T0dRM1pURTBOVGxsTUROaVpUTTNZelZtTURkaE5UVUtMRk10TVMwMUxUSXhMVEU1TWpjNU5EazNNakV0TkRJME5UUXdORGcxTVMwek5qSTJOVGN6TmpjdE5UQXdCQ0EyTlRjelpqSmhObVkwTXpFM1pXTXhNVFJtTjJWbE1UVm1ZemswT0dNNU1CQVlUM0p1YlZOb2FsZzBWVmRsUVRjME0zaG1RalpXVVQwOUFnWkhUVUZFVWpMTUFDb0FCd0EifQ.8NNydrClq_2vurOztxhO6OSmadhrzPWiJtv-xOaaeSv_qlTfyiq1RdY5ESHPQ53_s6GC-vk5mkl0CPU3_hQ09fxHRcYwaUxII7wLx5odzF3lvtgR5QDOeFmhKzJfh_q6C0nypV6VUGF-TZdfHRx0fYAmygjIVbPReUQbglZHxNod0tQ4X9IF6XCLiM5btg1ZdCSdW9QA4SxQXr2m0_RoJg3XaH8CudxyW5bQf7nXvhD9PTkAWfMzZrrgQzQ_w5nERK8X0MFOvQPZaC2Wvbh1GPxP3TRhTC_GS3zv9klfycK5agyhch3Vzy21zKYSFGoR2bAKbEg7I1n4a-YKcGD1Mw
Token Type: Bearer
Token expiration: 120

Logon through Resource Owner Password Credentials Grant

Option 3 requires the event Advanced setting “Use for Owner Password Credentials” set to “On”.



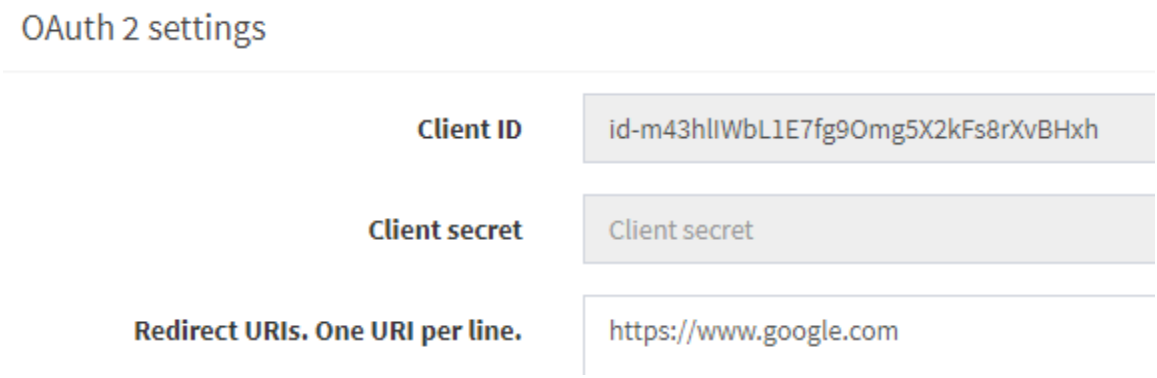
After successful authentication, the OSP server returns the access token.



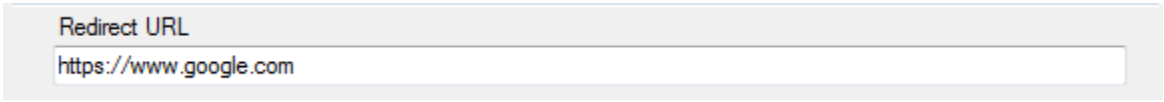
Redirecting to an external resource

As mentioned in previous sections the redirect URL can redirect the user to another web resource after successful authentication. The below example shows changing the redirect URL setting and the results.

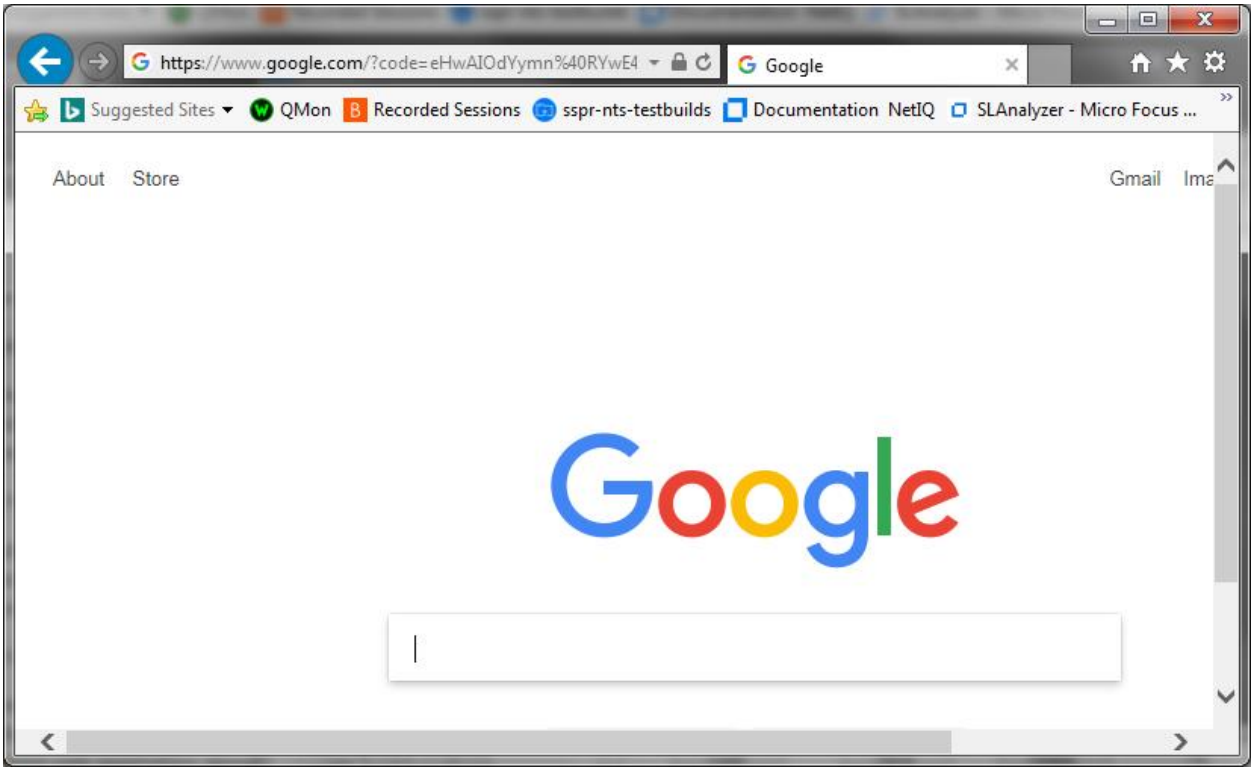
In the AAF event change the URL to an external resource location. (IE. https://www.google.com)



Now on the SLAnalyzer OAuth2 settings page set the Redirect URL to the same location

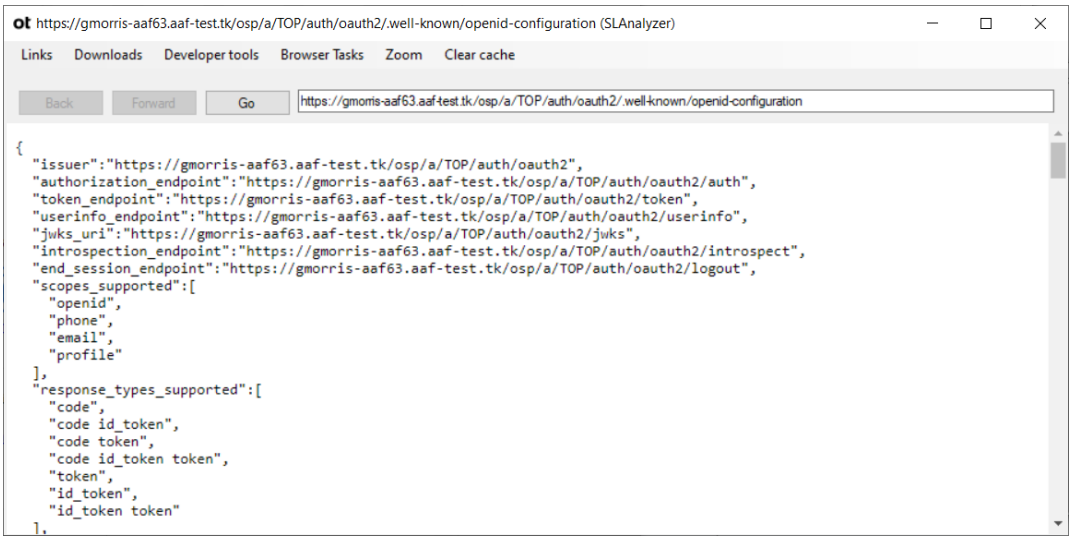


Now click start and select on of the first 3 grant options for authentication. After successful authentication the user is redirected to the specified resource.



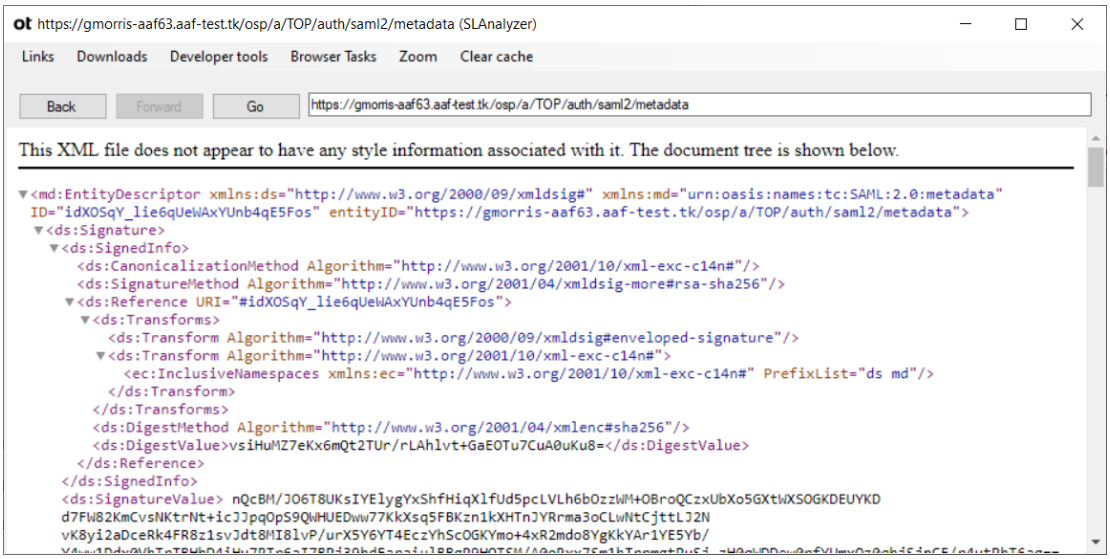
Get OpenId Config

SLAnalyzer will display a list of known hosts (saved profiles). Select the appropriate server or add the server to obtain the OpenId information.

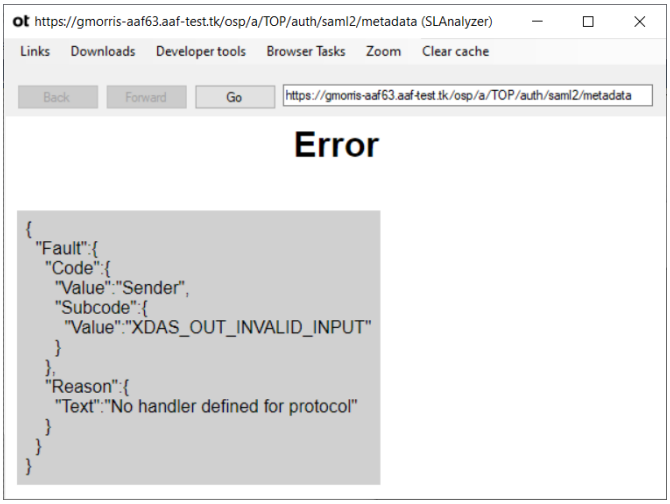


Get SAML metadata

SLAnalyzer will display a list of known hosts (saved profiles). Select the appropriate server or add the server to obtain the SAML information.

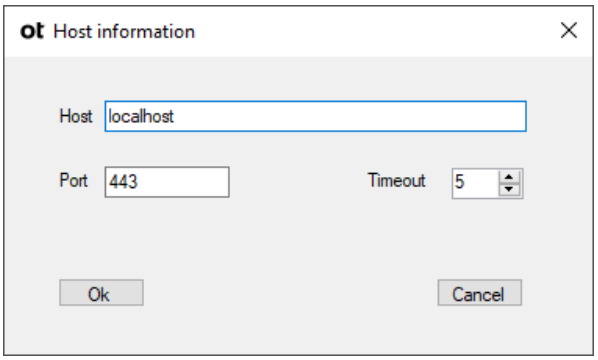


The feature will only return the SAML metadata if a SAML event is created on the server. If no SAML event exists, then the server will return an error “XDAS_OUT_INVALID_INPUT”.

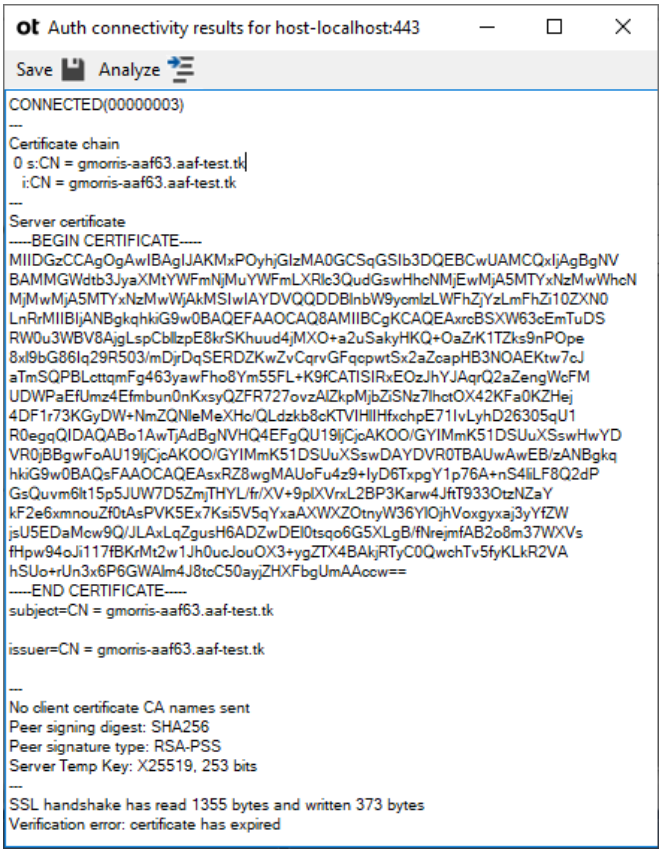


Check AAuth connectivity

This option provides the ability to validate connectivity between the AA service and a remote host. This utilizes OpenSSL to test the connectivity to the remote host. This option can be used to validate if the AA service can communicate with a LDAP, SAML, or OSP host. It can also be used to obtain the current certificate for the AA server itself.



Enter the IP address or DNS name of the host, the port address the host is listening on, and the timeout value. The application defaults to a timeout of 5 seconds but for environments where there are longer response times this value can be adjusted.



SaaS

This option contains supported operations for Software as a Service.

CBA

AAF in a SaaS environment includes a Cloud Bridge Agent. This server provides the interconnect between AAF running in the cloud to a repository located at the customer site. (On Prem)

Gather CBA Stats

This option will open an SSH connection to the CBA and gather statistical information. This information can be analyzed to identify possible issues with a failing CBA.

Start CBA

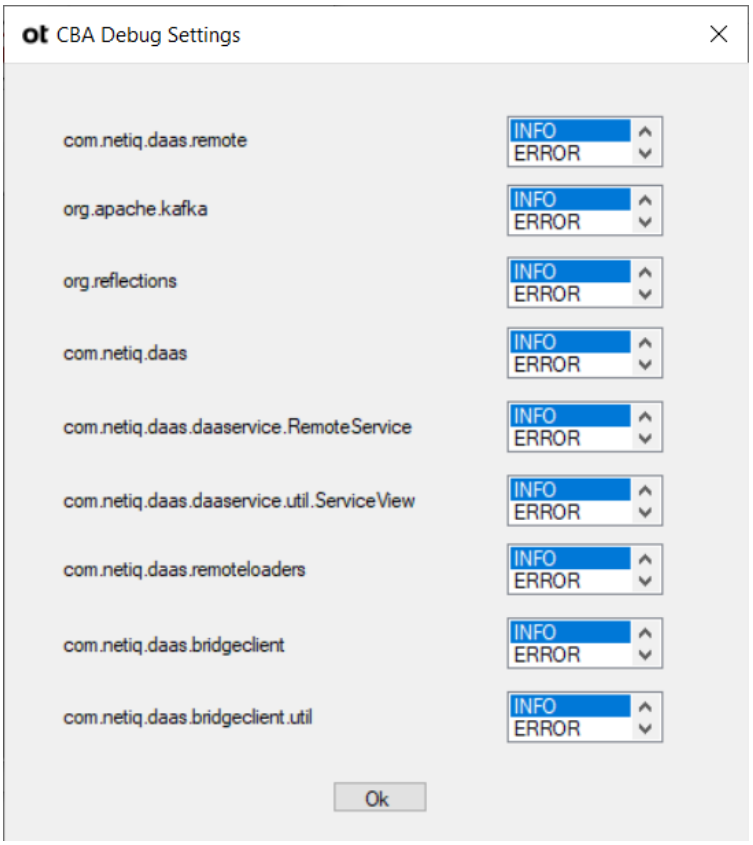
This option will open an SSH connection to the CBA and start the CBA.

Stop CBA

This option will open an SSH connection to the CBA and stop the CBA.

Debug Settings

This option will open an SSH connection to the CBA and read the current debug settings.



The debug log settings can be modified on this screen and then applied to the CBA by clicking the Ok button. Warning: enabling trace as a debug option can generate a lot of information in the CBA debug logs. Only set trace for items as instructed by support.

Get Install Log

This option will open an SSH/SCP connection to the server and download the install log.

Get Debug Logs

This option will open an SSH/SCP connection to the server and download the debug logs on the CBA. When selected the user will be prompted if they would like to download the current debug log alone or with the archived logs.

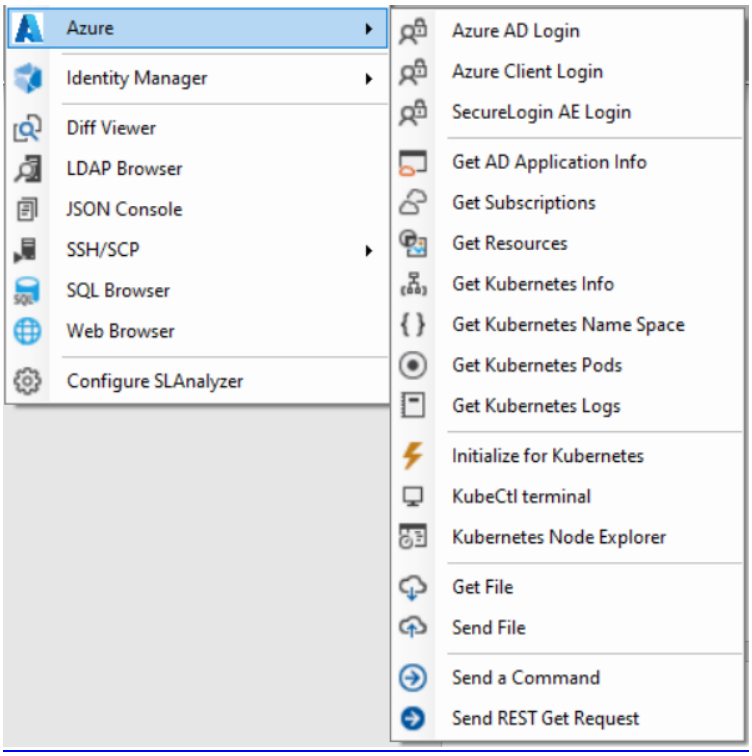
Azure

This option provides several items to help troubleshoot issues in the Microsoft Azure environment.

SLAnalyzer requires an Azure service principal. This object provides the entry point into Azure and establishes the necessary rights needed to access Azure information

Note that the service principal is created within Azure AD. Kubernetes clusters and other resources are defined in Azure. These two different environments require different configuration for proper access.

When SecureLogin Advanced Edition is installed in Azure then SLAnalyzer will leverage the SecureLogin service principal for access to Azure. When SecureLogin Advanced Edition is not installed in Azure then a service principal will need to be created and configured.



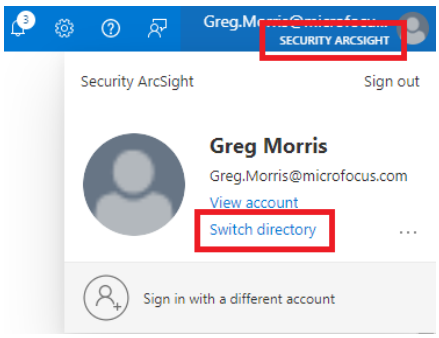
For more information about Azure Kubernetes see: [Concepts - Kubernetes basics for Azure Kubernetes Services (AKS) - Azure Kubernetes Service | Microsoft Docs]

Prerequisites – Creating a service principal

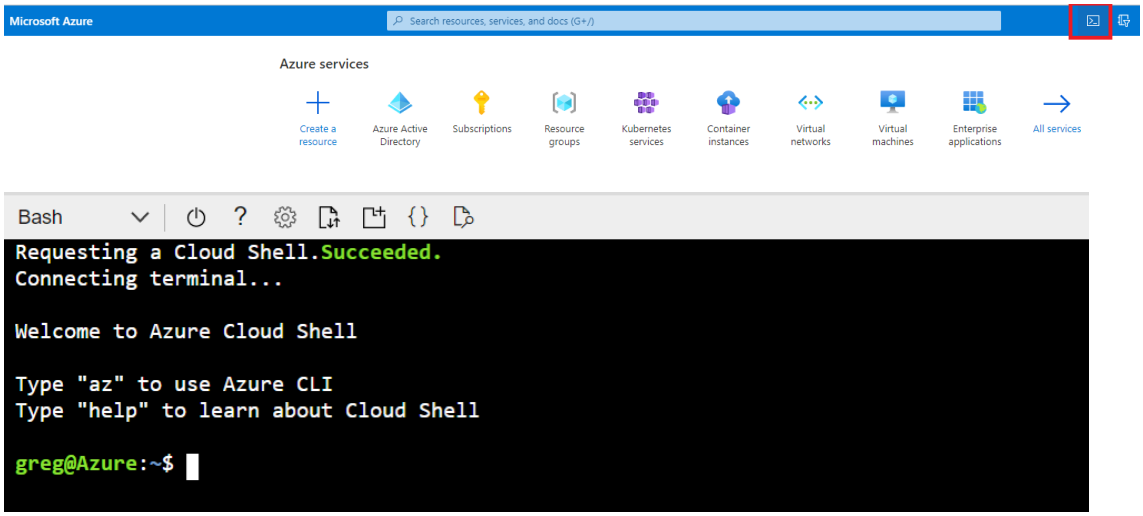
The following steps can be used to create the service principle for SLAnalyzer to access Azure. These steps are optional in environments where SecureLogin Advanced Edition is installed in Azure.

1. Login to portal.azure.com

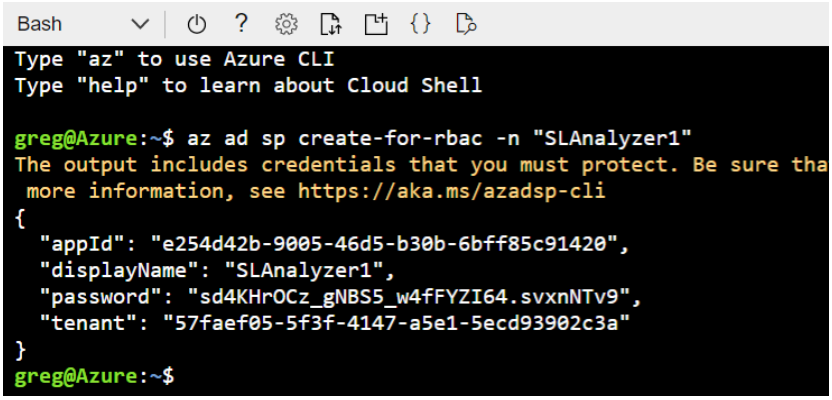
2. Verify and if necessary, switch to the desired directory for the subscription where the Azure information is stored.



3. Open a Cloud Shell session by clicking the icon shown in the picture below highlighted with the red box.



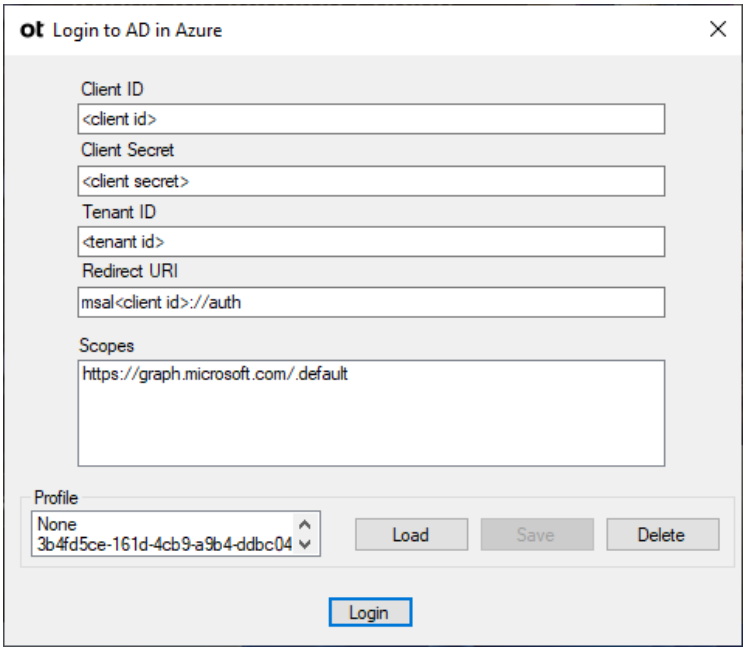
4. Type ***az ad sp create-for-rbac -n "SLAnalyzer1"*** to create the service principal named SLAnalyzer1. Please note that any name can be used.



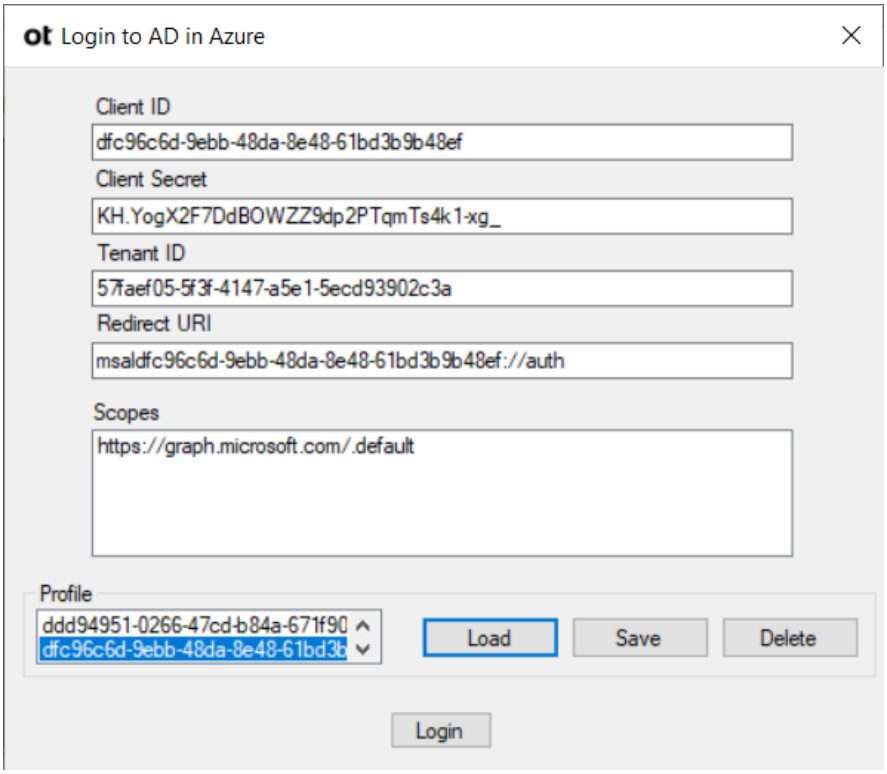
Important: Save the information returned. We will be using it to connect to Azure with SLAnalyzer.

4a. The service principal information can be stored in SLAnalyzer.

Tools->Azure->Azure AD Login



Replace <client id> with appId value, <client secret> with password value, <tenant id> with tenant value, and then modify the Redirect URI replacing <client id> with the appId value.



After entering the service principal information, then click the Save button to save the profile for future use.

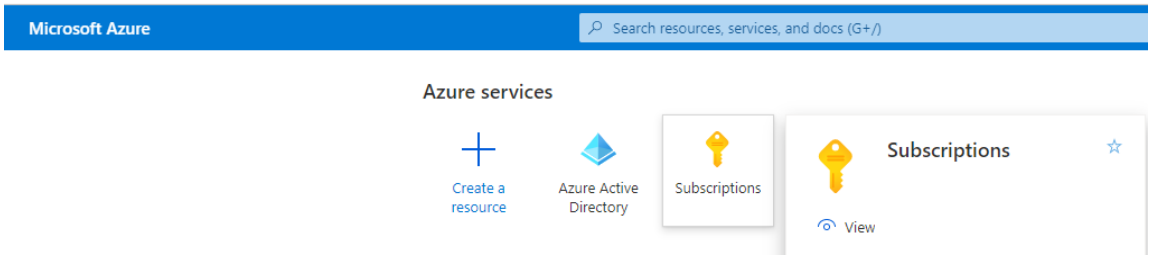
After creating a service principal, permissions will need to be granted for Azure and Azure AD. Access to Azure AD is only needed if the user wants to read the service principal configuration or other information stored in Azure AD.

For more information on ways to create a service principal see:
https://docs.microsoft.com/en-us/cli/azure/create-an-azure-service-principal-azure-cli

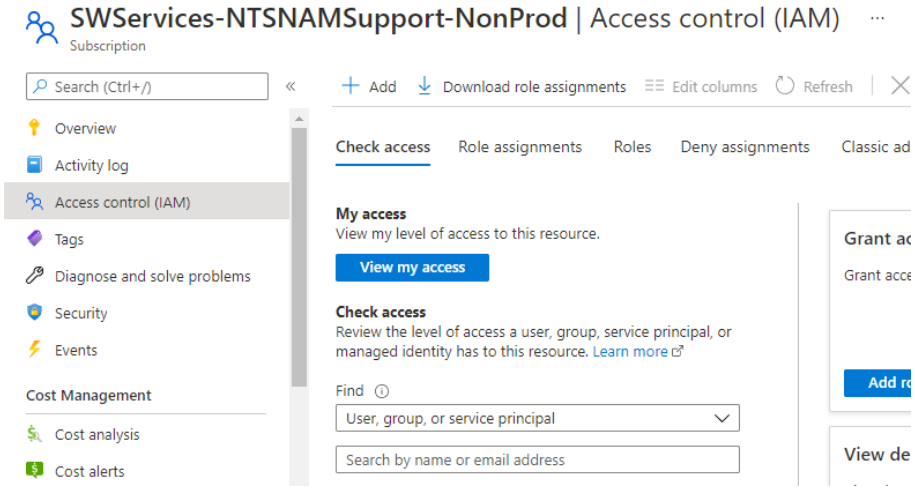
Prerequisites – Granting access to a service principal for Azure access

After creating a new service principal, access rights need to be granted so that SLAnalyzer can read configuration information from Azure. The steps below outline the process necessary for granting access to a service principal.

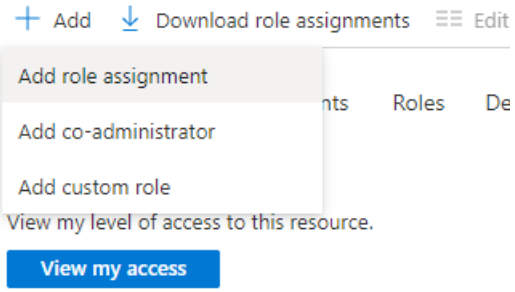
1. Back in the Azure Portal page click home, Subscriptions and then select the subscription for the Azure resource needing to be accessed. For example, our Kubernetes cluster.



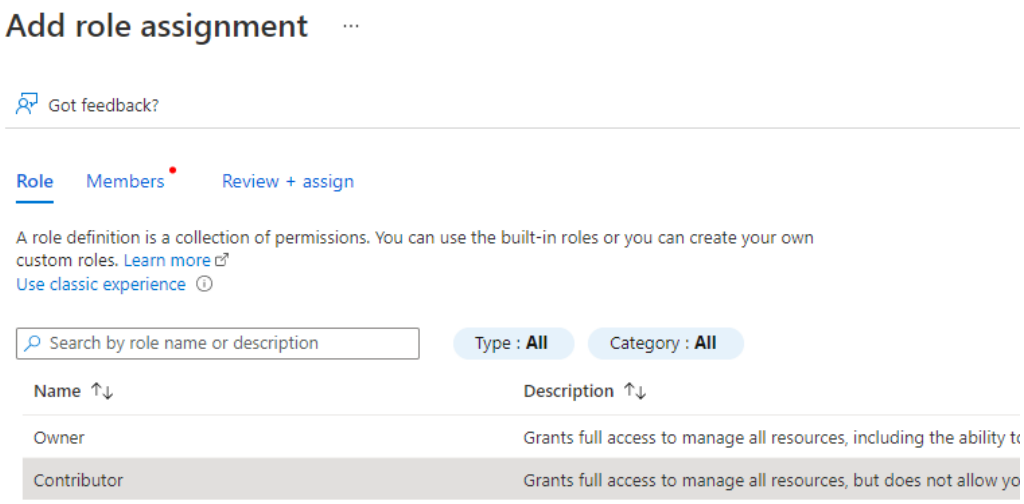
2. Click on Access control (IAM)



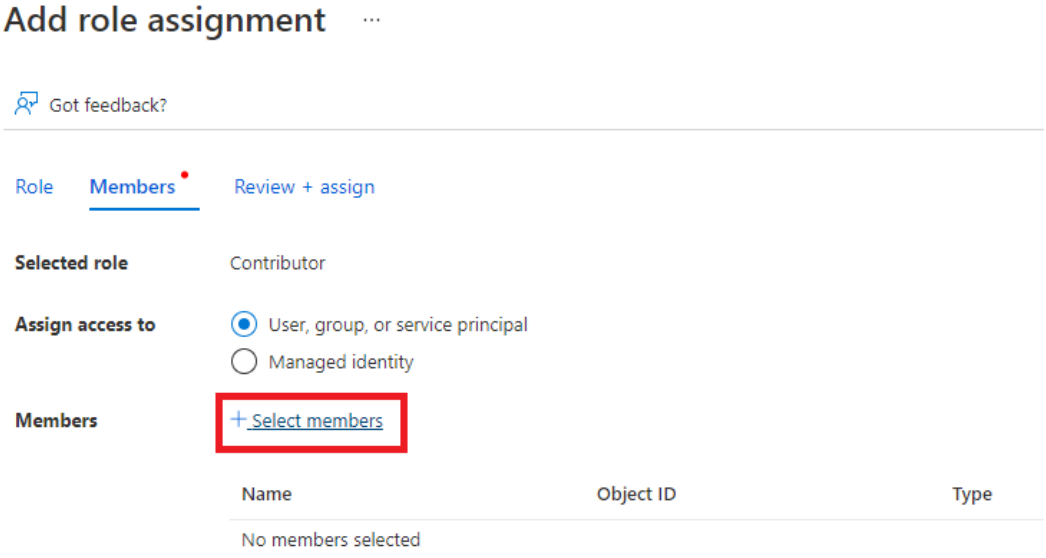
3. Click the + Add button to add access to our new service principle. Select Add role assignment.



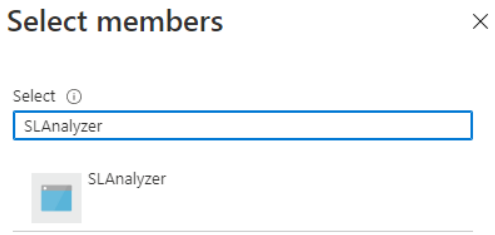
4. Select the role Contributor, then click the Next button.



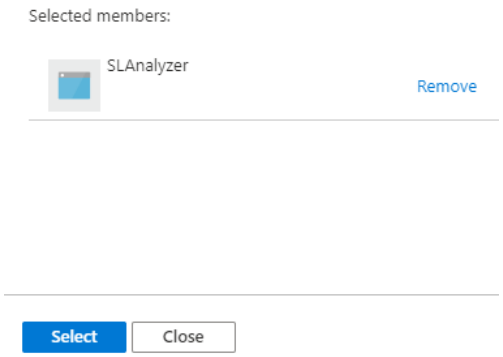
5. Click the + Select members button



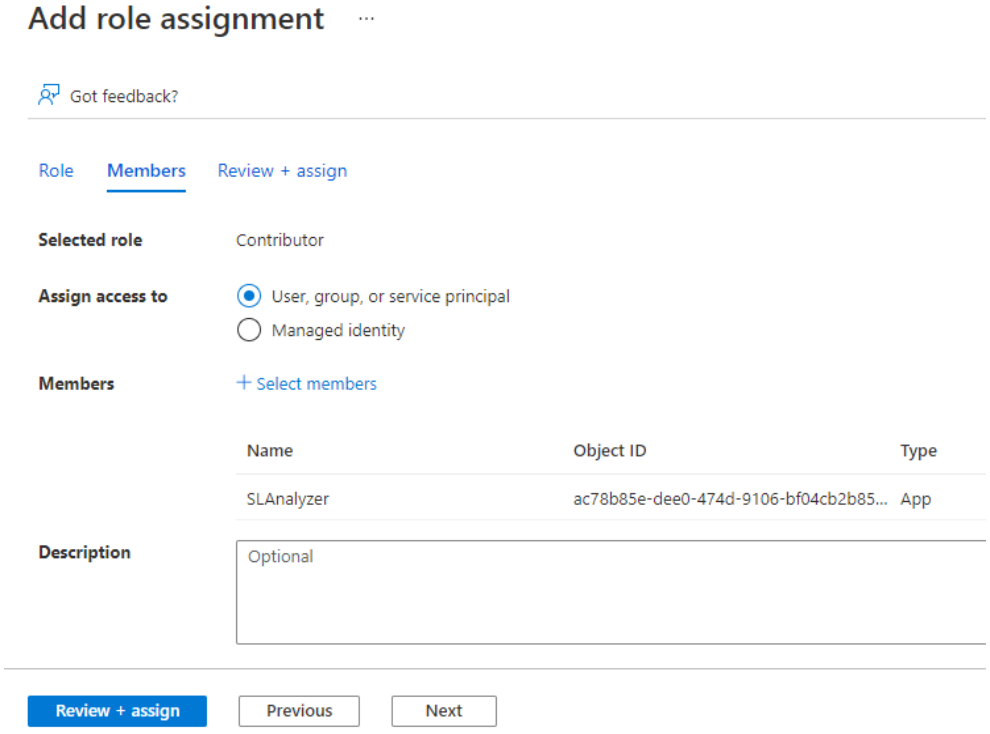
6. In the Select members popup type the name of the service principal.



7. Click on service principal and then click Select.



8. Click the button Review + assign



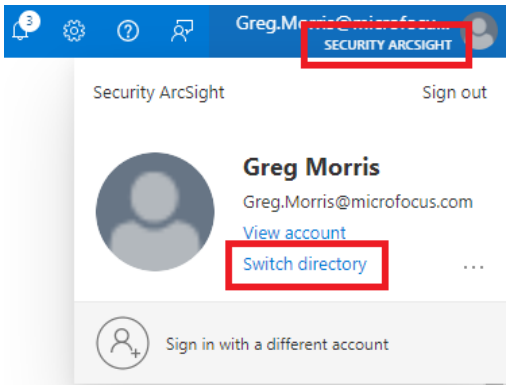
This completes the necessary steps for a new service principal for SLAnalyzer to access Azure.

Prerequisites – Granting access to a service principal for Azure AD access

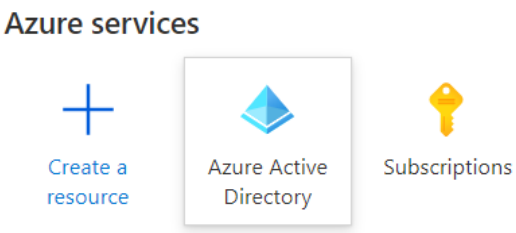
(Optional) After creating a new service principal, access rights need to be granted so that SLAnalyzer can read configuration information from Azure AD. The steps below outline the process necessary for granting access to a service principal.

1. Login to Azure portal (portal.azure.com)

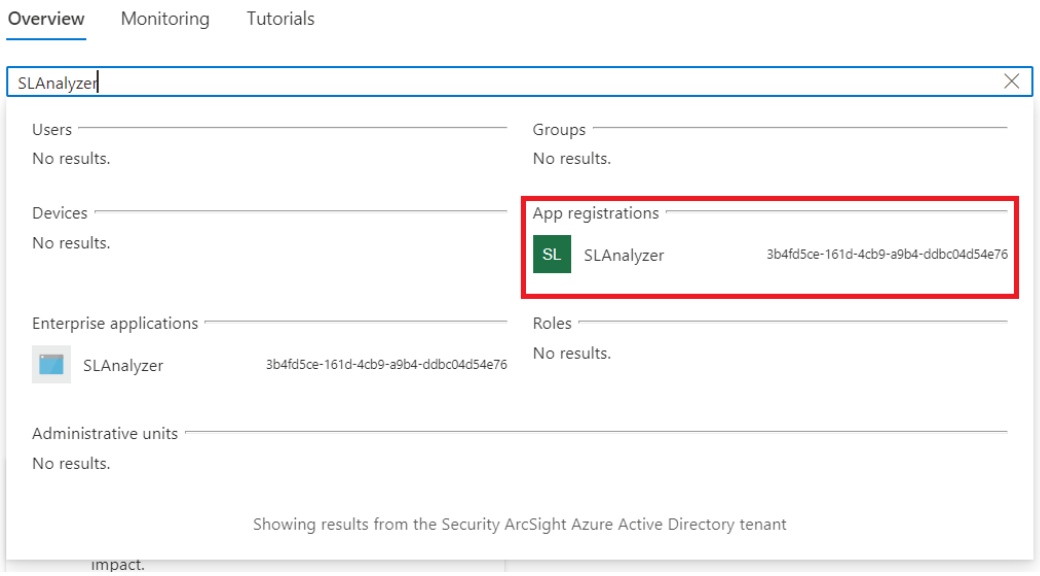
2. Verify and if necessary, switch to the desired directory for the subscription where the Azure information is stored.



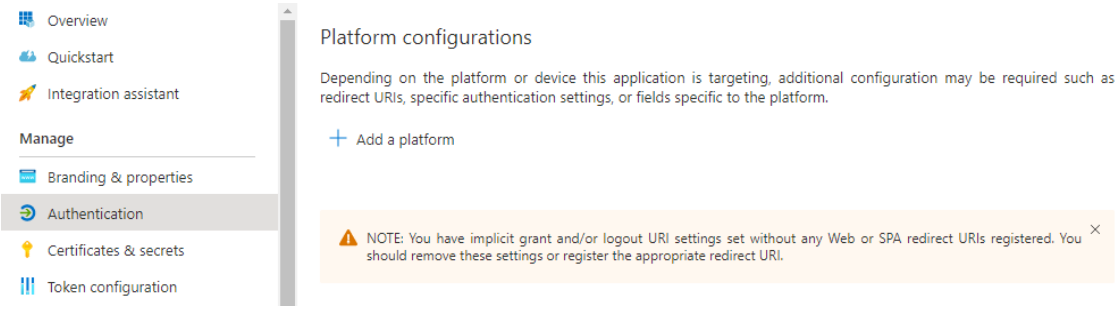
3. Click on Azure Active Directory



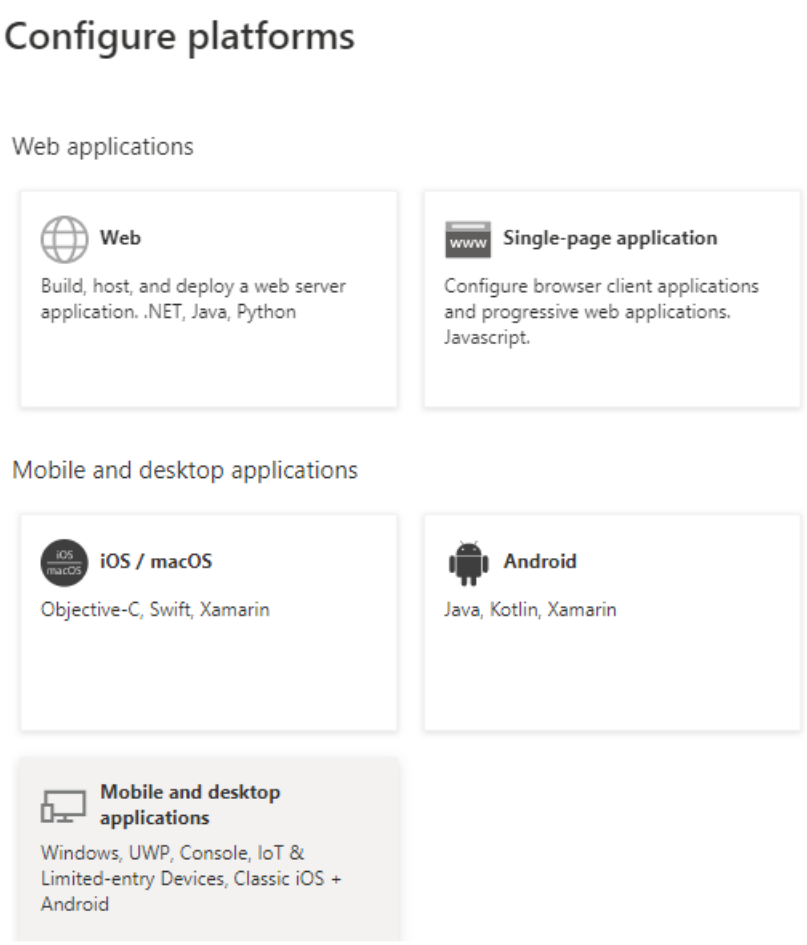
4. Search for service principal name under app registrations. (IE SLAnalyzer)



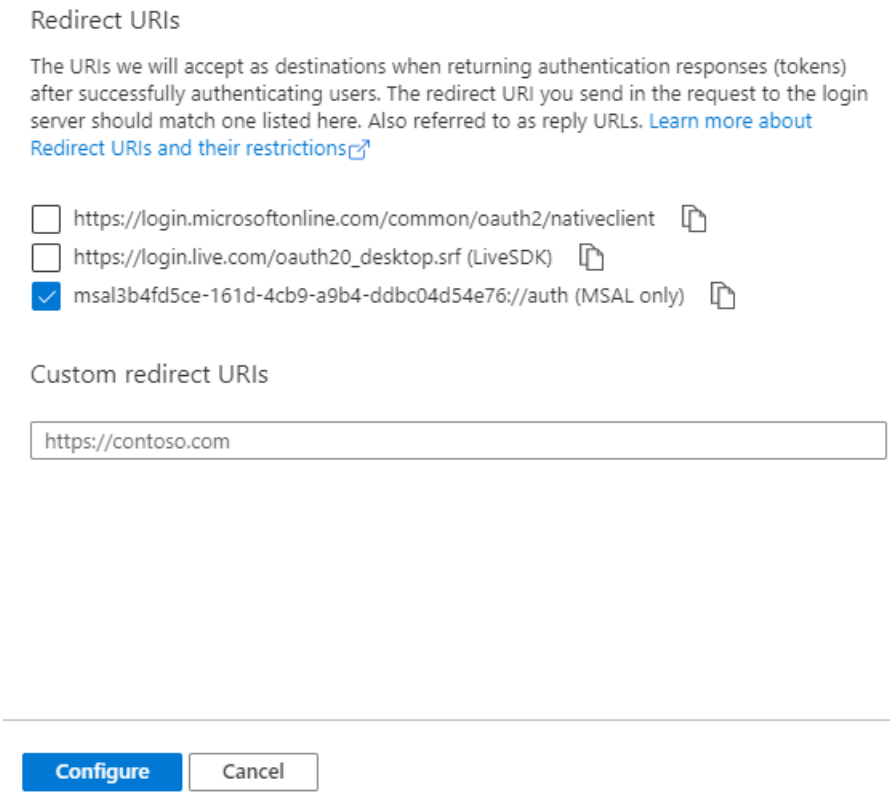
5. Click on Authentication



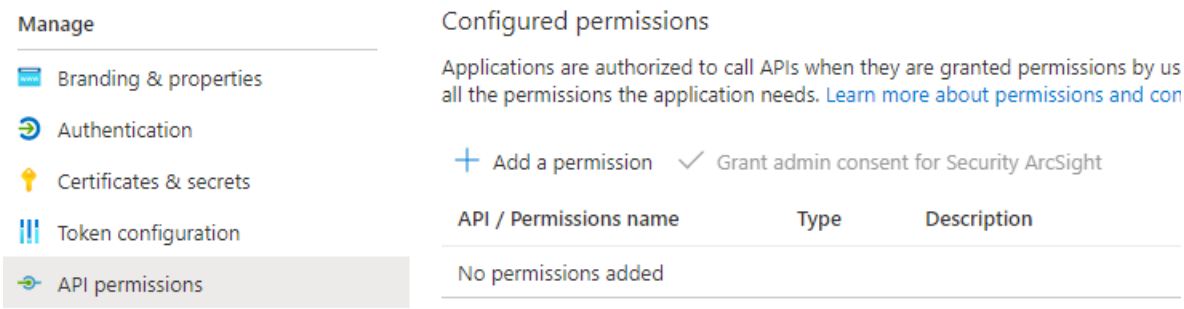
6. Click on + Add a platform, Select Mobile and desktop applications



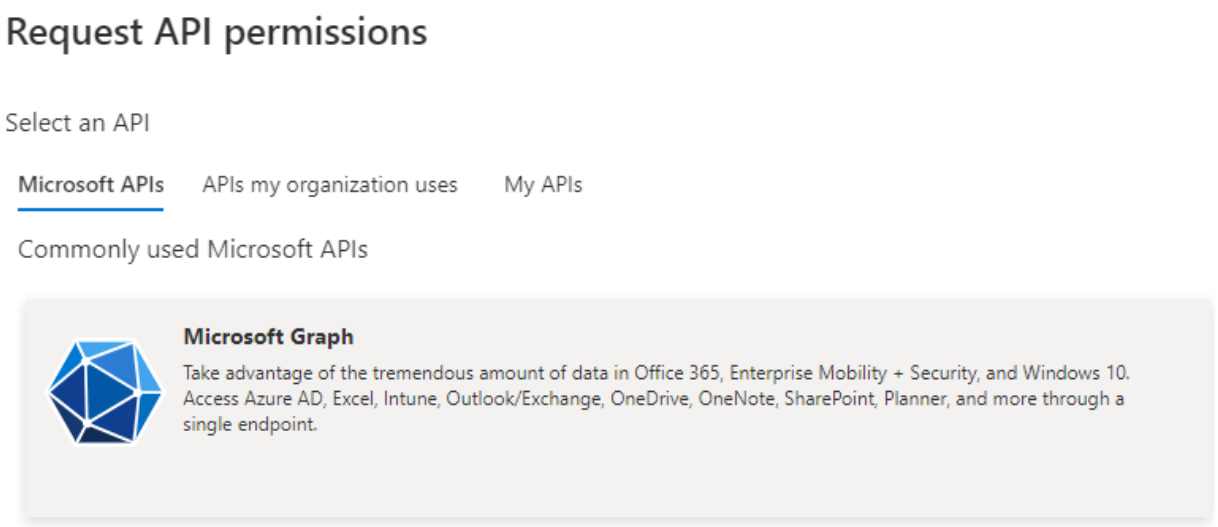
7. Click the box for msal<clientID>://auth and then click Configure



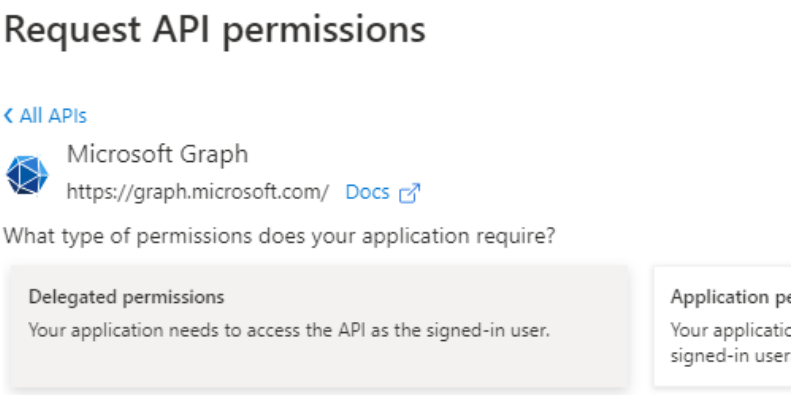
8. Click on API permissions



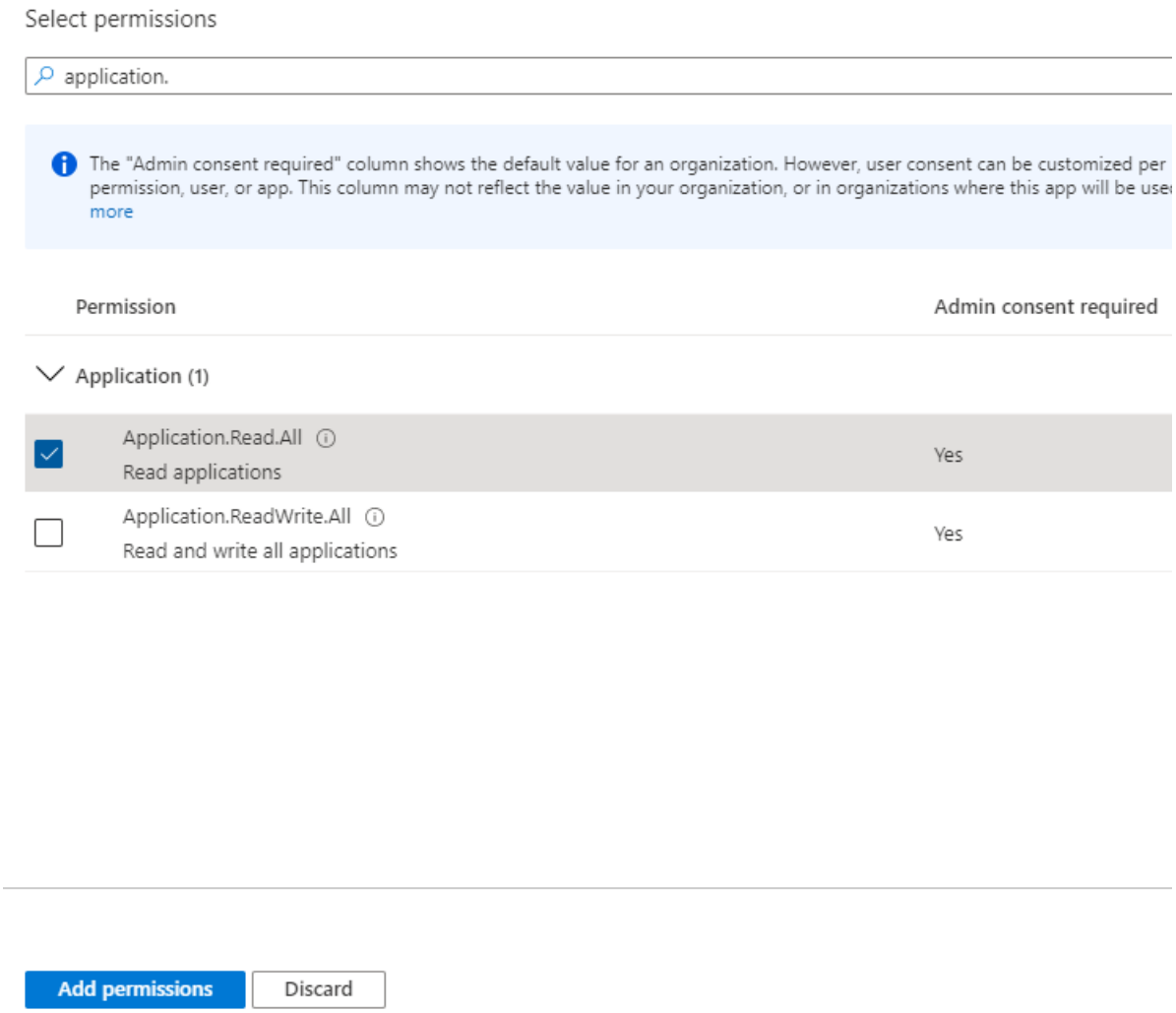
9. Click on + Add a permission and then select Microsoft Graph



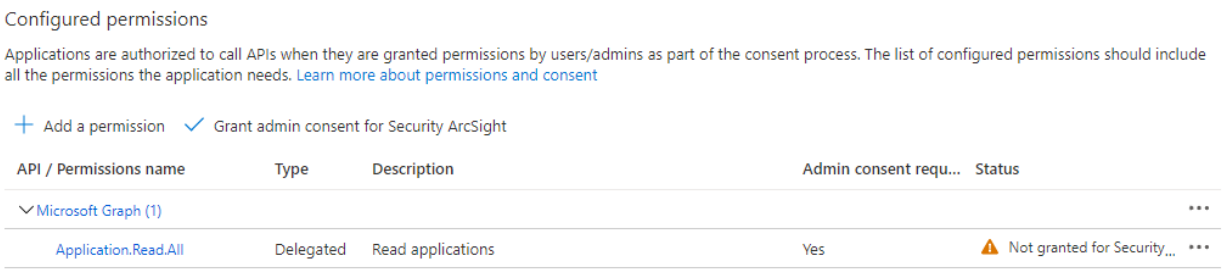
10. Select Delegated permissions



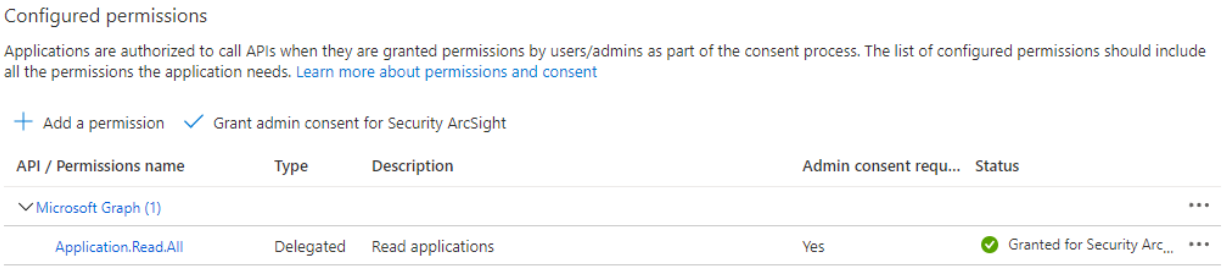
11. In the Select permissions box type application. Then expand Application and select Application.Read.All, then click the Add permissions button.



12. Click the Grant admin consent for ...

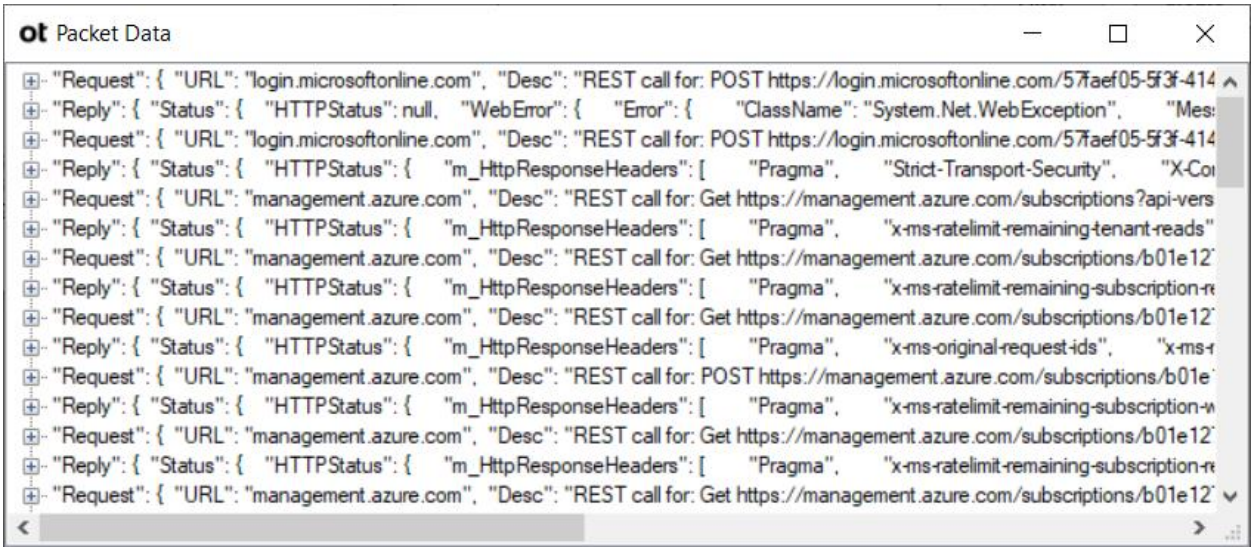


13. The permission should now be displayed.



Packet Data window

When launching any of the Azure menu items, if a REST call is made to Azure, then a packet window will be displayed to show the structure of the request/reply packets. The packet window can be utilized to gather detailed information about each call made to Azure.



The Request items have the following components.

- URL – reflects the host that the packet is destined for
- Desc – description of the REST call being performed
- Headers – header data of the packet
- Data – any parameters sent to host for the specified REST call
- Httpmethod – the HTTP protocol method (IE. GET, PUT, POST, DEL, etc.)
- httpURL – the full URL of the destination host including any URL encoded values

The Reply items have the following components.

- Status – contains error and other status responses from
    - HTTPStatus – the return values for the HTTP protocol
    - WebError – network related return values
    - RESTError – status values returned by the REST call
- Headers – header data of the packet
- Data – response from a successful REST call

Gaining access to Azure

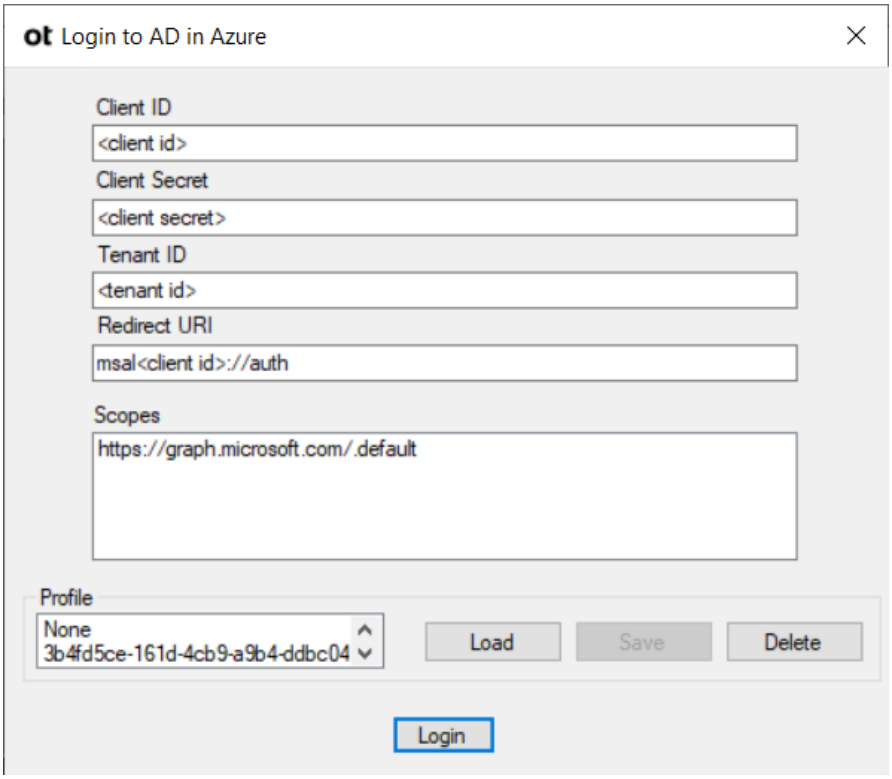
SLAnalyzer implements 3 different methods of logging into the service principle.

- Azure AD Login – AD in Azure via MSAL
- Azure OAuth2 Client Login – Login via OAuth2/OpenID to Azure
- Securlogin Advanced Edition Login – Access Azure via the SLAE server configuration

Azure AD Login

This option allows for accessing Microsoft Active Directory in Azure. It implements the Microsoft Authentication Library to access Active Directory in the Azure cloud.

For information about MSAL see:
Learn about MSAL - Microsoft identity platform | Microsoft Docs



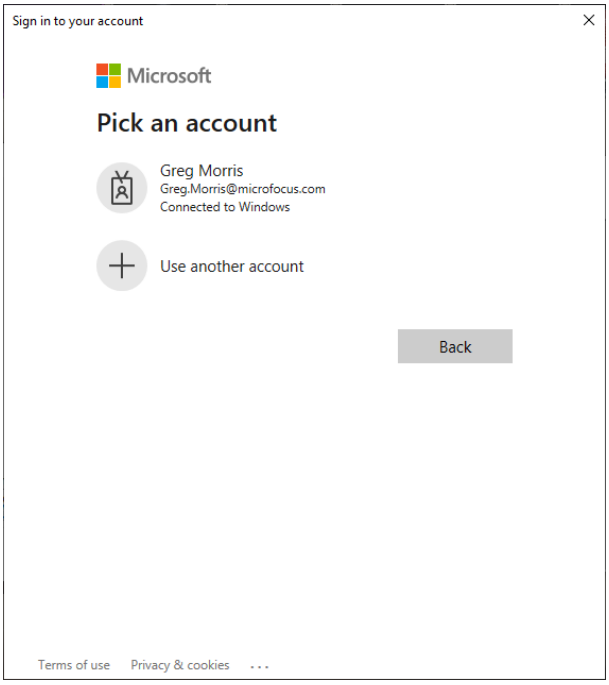
Note that access restrictions are defined in the assigned scopes within the configuration of the AD application.

For more information about scopes and permissions see:
Microsoft identity platform scopes, permissions, & consent | Microsoft Docs

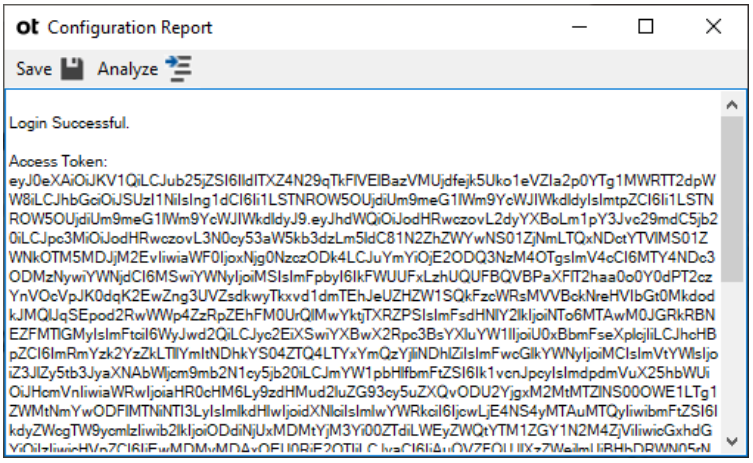
For SLAnalyzer to properly login and read information from Active Directory in Azure `Please login to the Azure portal and make sure the application has the API permission of Microsoft Graph - Application.Read.All`

See the prerequisite for Azure Active Directory for more information.

Azure will now prompt for the account for logon.



If the logon is successful, then the report window will display the results. Also note that the packet data window will sow the exact reply from Azure.

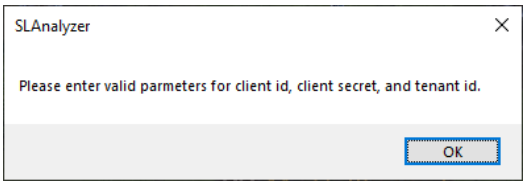


Azure OAuth2 Client Login

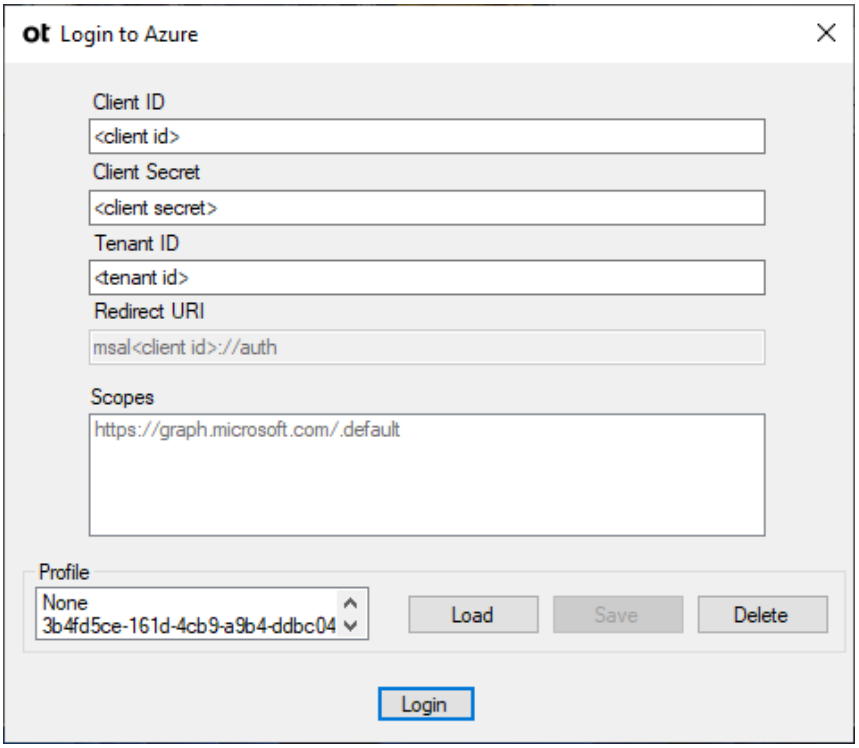
This option utilizes the OAuth2 protocol to obtain an access token to Azure.

For more information about this option see:
[OAuth 2.0 and OpenID Connect protocols on the Microsoft identity platform - Microsoft identity platform | Microsoft Docs]

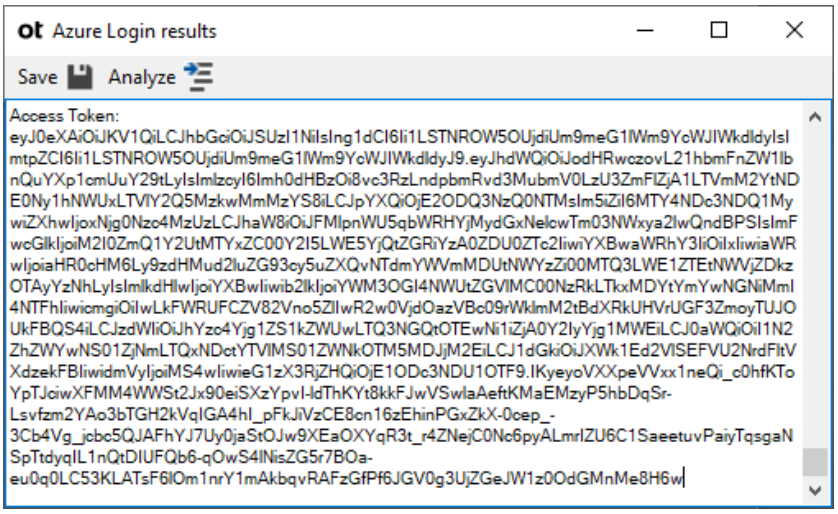
When selecting this option, the user is first prompted that they will need to provide the client ID, client Secret, and tenant ID. These values are found in the Azure portal on the Active Directory application.



Enter the required information and then click Login to obtain an access token.



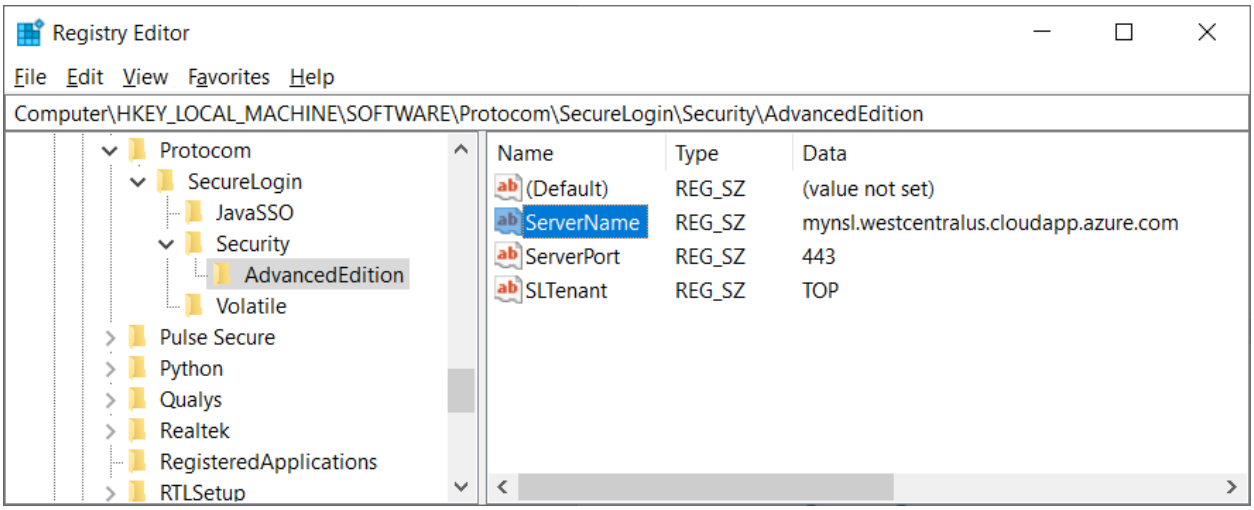
If successful, the report window will display the current access token.


ot Azure Login results
Save
Analyze
Access Token:
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG1lWm9YcWJlWkdldyIsImtpZCI6Ii1LSTNROW5OUjdiUm9meG1lWm9YcWJlWkdldyJ9.eyJhdWQiOiJodHRwczovL21hbmFnZW1lbnQuYXp1cmUuY29tLyIsImlzcyI6Imh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzU3ZmFlZjA1LTVmM2YtNDE0Ny1hNWUxLTVlY2Q5MzkwMmMzYS8iLCJpYXQiOjE2ODQ3NzQ0NTMsIm5iZiI6MTY4NDc3NDQ1MywiZXhwIjoxNjg0Nzc4MzUzLCJhaW8iOiJFMlpnWU5qbWRHYjMydGxNelcwTm03NWxya2lwQndBPSIsImFwcGlkIjoiM2I0ZmQ1Y2UtMTYxZC00Y2I5LWE5YjQtZGRiYzA0ZDU0ZTc2IiwiYXBwaWRhY3IiOiIxIiwiaWRwIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQvNTdmYWVmMDUtNWYzZi00MTQ3LWE1ZTEtNWVjZDkzOTAyYzNhLyIsImlkdHlwIjoiYXBwIiwib2lkIjoiYWM3OGI4NWUtZGVlMC00NzRkLTkxMDYtYmYwNGNiMmI4NTFhIiwicmgiOiIwLkFWRUFCZV82Vno5ZlIwR2w0VjdOazVBc09rWklmM2tBdXRkUHVrUGF3ZmoyTUJOUkFBQS4iLCJzdWIiOiJhYzc4Yjg1ZS1kZWUwLTQ3NGQtOTEwNi1iZjA0Y2IyYjg1MWEiLCJ0aWQiOiI1N2ZhZWYwNS01ZjNmLTQxNDctYTVlMS01ZWNkOTM5MDJjM2EiLCJ1dGkiOiJXWk1Ed2VISEFVU2NrdFltVXdzekFBIiwidmVyIjoiMS4wIiwieG1zX3RjZHQiOjE1ODc3NDU1OTF9.IKyeyoVXXpeVVxx1neQi_c0hfKToYpTJciwXFMM4WWSt2Jx90eiSXzYpvI-ldThKYt8kkFJwVSwlaAeftKMaEMzyP5hbDqSr-Lsvfzm2YAo3bTGH2kVqIGA4hI_pFkJiVzCE8cn16zEhinPGxZkX-0cep_-3Cb4Vg_jcbc5QJAFhYJ7Uy0jaStOJw9XEaOXYqR3t_r4ZNejC0Nc6pyALmrlZU6C1SaeetuvPaiyTqsgaNSpTtdyqIL1nQtDIUFQb6-qOwS4INisZG5r7BOa-eu0q0LC53KLATsF6lOm1nrY1mAkbqvRAFzGfPf6JGV0g3UjZGeJW1z0OdGMnMe8H6w

SecureLogin AE Login

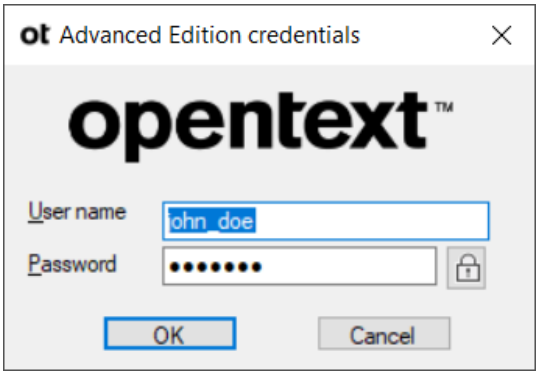
This option instructs SLAnalyzer to connect to an SLAE server and read the application information for access to Azure.

The first thing SLAnalyzer does is read the registry for the configured SLAE server.



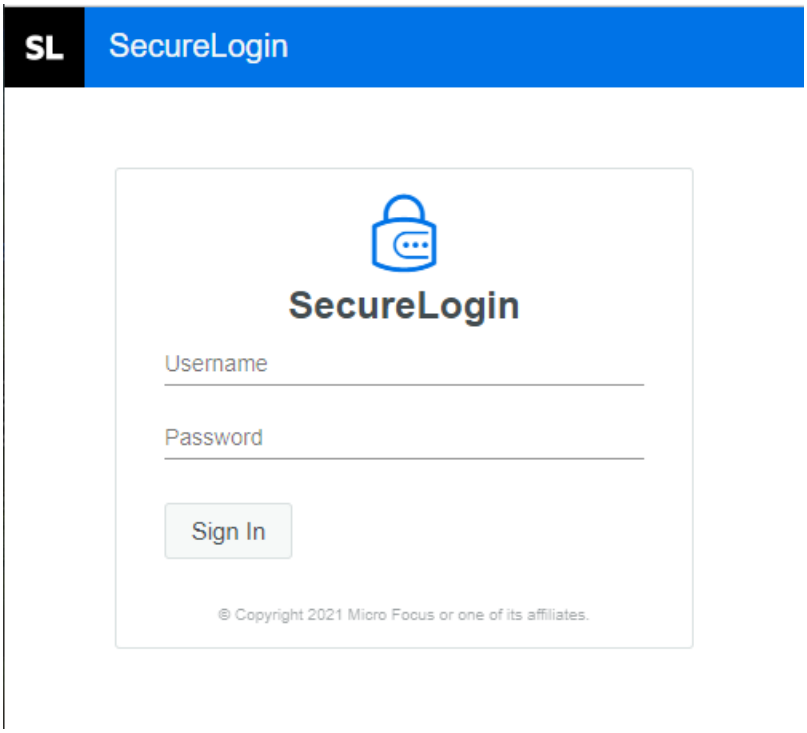
SLAnalyzer then sends REST calls to the SLAE server to obtain the configuration information for Azure.

The SLAE server will first require authentication. SLAnalyzer populates the login dialog with the default values for the SLAE server. Replace these values with appropriate login credentials for the SLAE server.



The user can also open a browser to the same URL to see the same server login page.

https://mynsl.westcentralus.cloudapp.azure.com/



After a successful login has completed, SLAnalyzer will then read the configuration of the SLAE server. This would include the client ID, client Secret, and Tenant ID information.

Note that when running the Analyze->SecureLogin report from SLAnalyzer's Analyze menu, if SecureLogin SLAE is detected then this login will be executed. It will then connect to Azure and read the configuration details for the Kubernetes cluster.

Azure AD functions

After a successful login to Azure AD the following function will gather information about the service principal/Application from Azure AD.

- Get AD Application Info – This function requires Active Directory access API permissions. `API permission of Microsoft Graph - Application.Read.All`
  See the prerequisite for Azure Active Directory for more information

Get AD Application Info

This function sends the following REST call to Azure.

[Get organization - Microsoft Graph v1.0 | Microsoft Docs]

For this function to work successfully the application in Active Directory must have `API permission of Microsoft Graph - Application.Read.All`

If successful, this function will return the information about the application within Azure Active Directory.


```
"value": [
 {
  "id": "2b6cc171-b5e2-4184-bc1a-aff068883b17",
  "deletedDateTime": null,
  "appId": "ddd94951-0266-47cd-b84a-671f90d465ed",
  "applicationTemplateId": null,
  "disabledByMicrosoftStatus": null,
  "createdDateTime": "2021-09-30T15:21:48Z",
  "displayName": "GMorrisApp",
  "description": null,
  "groupMembershipClaims": "None",
  "identifierUris": [
   "api://ddd94951-0266-47cd-b84a-671f90d465ed"
  ],
  "isDeviceOnlyAuthSupported": null,
  "isFallbackPublicClient": true,
  "notes": null,
  "publisherDomain": "nsl-test.xyz",
  "signInAudience": "AzureADMyOrg",
  "tags": [],
  "tokenEncryptionKeyId": null,
  "defaultRedirectUri": null,
  "certification": null,
  "addIns": [],
  "api": {
   "acceptMappedClaims": null,
   "knownClientApplications": [],
   "requestedAccessTokenVersion": 2,
   "oauth2PermissionScopes": [
    {
     "adminConsentDescription": "Allow all",
     "adminConsentDisplayName": "All",
     "id": "bf3c091e-1070-450d-b4e8-48f85a0541da",
     "isEnabled": true,
     "type": "User",
     "userConsentDescription": null,
     "userConsentDisplayName": null,
     "value": "All"
    },
    {
     "adminConsentDescription": "Allow the application to access GMorrisApp on behalf of the signed-in user.",
     "adminConsentDisplayName": "Access GMorrisApp",
     "id": "c4508ebc-4269-48e5-8f9f-2d420cb34625",
     "isEnabled": true,
     "type": "User",
     "userConsentDescription": "Allow the application to access GMorrisApp on your behalf.",
     "userConsentDisplayName": "Access GMorrisApp",
     "value": "user_impersonation"
    }
   ],
   "preAuthorizedApplications": []
  },
  "appRoles": [
   {
    "allowedMemberTypes": [
```

```
      "User",
      "Application"
    ],
    "description": "User access",
    "displayName": "User",
    "id": "46f12ec6-cc9b-4ccf-8eee-a5894a767bd4",
    "isEnabled": true,
    "origin": "Application",
    "value": "user"
  },
  {
    "allowedMemberTypes": [
      "User",
      "Application"
    ],
    "description": "Admin access",
    "displayName": "Admin",
    "id": "b02fa612-42aa-4b47-bac0-79febcab0490",
    "isEnabled": true,
    "origin": "Application",
    "value": "admin"
  }
],
"info": {
  "logoUrl": null,
  "marketingUrl": null,
  "privacyStatementUrl": null,
  "supportUrl": null,
  "termsOfServiceUrl": null
},
"keyCredentials": [],
"optionalClaims": {
  "accessToken": [
    {
      "additionalProperties": [],
      "essential": false,
      "name": "upn",
      "source": null
    },
    {
      "additionalProperties": [
        "use_guid"
      ],
      "essential": false,
      "name": "aud",
      "source": null
    }
  ],
  "idToken": [],
  "saml2Token": []
},
"parentalControlSettings": {
  "countriesBlockedForMinors": [],
  "legalAgeGroupRule": "Allow"
},
"passwordCredentials": [
  {
    "customKeyIdentifier": "//5yAGIAYQBjAA==",
    "displayName": null,
    "endDateTime": "2022-09-30T15:21:48.235986Z",
    "hint": null,
    "keyId": "baf39b0d-00d9-4806-aee6-0ab777cc17a2",
    "secretText": null,
    "startDateTime": "2021-09-30T15:21:48.235986Z"
  }
],
"publicClient": {
  "redirectUris": [
    "msalddd94951-0266-47cd-b84a-671f90d465ed://auth",
    "https://login.live.com/oauth20_desktop.srf",
```

```
        "https://login.microsoftonline.com/common/oauth2/nativeclient"
      ]
    },
    "requiredResourceAccess": [
      {
        "resourceAppId": "00000003-0000-0000-c000-000000000000",
        "resourceAccess": [
          {
            "id": "a154be20-db9c-4678-8ab7-66f6cc099a59",
            "type": "Scope"
          },
          {
            "id": "5f8c59db-677d-491f-a6b8-5f174b11ec1d",
            "type": "Scope"
          },
          {
            "id": "14dad69e-099b-42c9-810b-d002981feec1",
            "type": "Scope"
          },
          {
            "id": "9a5d68dd-52b0-4cc2-bd40-abcf44ac3a30",
            "type": "Role"
          }
        ]
      },
      {
        "resourceAppId": "ddd94951-0266-47cd-b84a-671f90d465ed",
        "resourceAccess": [
          {
            "id": "bf3c091e-1070-450d-b4e8-48f85a0541da",
            "type": "Scope"
          }
        ]
      }
    ],
    "verifiedPublisher": {
      "displayName": null,
      "verifiedPublisherId": null,
      "addedDateTime": null
    },
    "web": {
      "homePageUrl": null,
      "logoutUrl": null,
      "redirectUris": [],
      "implicitGrantSettings": {
        "enableAccessTokenIssuance": false,
        "enableIdTokenIssuance": true
      }
    },
    "spa": {
      "redirectUris": []
    }
  }
]
```

Azure functions

After a successful login to Azure, a number of other functions are available for diagnostics. These functions are implemented to gather the Azure configuration information for Kubernetes configurations in Azure (AKS).

- Get Subscriptions – This function reads the subscription information for the provided client ID.
- Get Resources – This function reads the resource definition for the provided client ID.
- Get Kubernetes Info – This function reads the Kubernetes configuration information for the provided client ID.
- Get Kubernetes Name Space – This function reads the Kubernetes name spaces for the provided client ID.
- Get Kubernetes Pods – This function reads the pods running in the configured Kubernetes name space.
- Get Kubernetes Logs – This function will download the logs from one of the pods returned from the Get Kubernetes Pods function.
- Initialize for Kubernetes – Connects to Azure and reads the required information from Azure for the terminal and node explorer features noted below.
  This option automates the options of:
  1. Service principal login
  2. Get Subscriptions
  3. Get Kubernetes Info
  4. Get Kubernetes Name Space
  5. Get Kubernetes Pods

After acquiring the necessary Kubernetes information, then the following features will be available.

- KubeCtl terminal – Terminal emulation via the KubeCtl command.
- Kubernetes Node Explorer – Similar to Windows explorer providing a graphical interface to the selected Kubernetes node.

Get Subscriptions

This function sends the following REST call to Azure.

Subscriptions - List - REST API (Azure Resource Management) | Microsoft Docs

If successful, this function returns the subscriptions for the authenticated Client ID.


```
{
  "id": "/subscriptions/b01e1276-bbbd-49df-b177-1f8592512abb",
  "subscriptionId": "b01e1276-bbbd-49df-b177-1f8592512abb",
  "displayName": "SWServices-NTSNAMSupport-NonProd",
  "state": "Enabled",
  "subscriptionPolicies": {
    "locationPlacementId": "Public_2014-09-01",
    "quotaId": "MSDNDevTest_2014-09-01",
    "spendingLimit": "Off"
  }
}
```

Get Resources

This function sends the following REST call to Azure.

[Resource Groups - List - REST API (Azure Resource Management) | Microsoft Docs]

If successful, this function returns the resources for the authenticated Client ID.


```
[
  {
    "id": "/subscriptions/b01e1276-bbbd-49df-b177-1f8592512abb/resourceGroups/gregsnsl-
rg/providers/Microsoft.ContainerRegistry/registries/gregsnslacr",
    "name": "gregsnslacr",
    "type": "Microsoft.ContainerRegistry/registries",
    "sku": {
      "name": "Basic",
      "tier": "Basic"
    },
    "location": "westcentralus",
    "tags": {},
    "systemData": {
      "createdBy": "greg.morris@microfocus.com",
      "createdByType": "User",
      "createdAt": "2021-10-01T15:21:33.1591427Z",
      "lastModifiedBy": "greg.morris@microfocus.com",
      "lastModifiedByType": "User",
      "lastModifiedAt": "2021-10-01T15:21:33.1591427Z"
    }
  },
  {
    "id": "/subscriptions/b01e1276-bbbd-49df-b177-1f8592512abb/resourceGroups/gregsnsl-
rg/providers/Microsoft.ContainerService/managedClusters/gregsnsl-cluster",
    "name": "gregsnsl-cluster",
    "type": "Microsoft.ContainerService/managedClusters",
    "location": "westcentralus",
    "tags": {
      "Environment": "gregsnsl-cluster"
    }
  },
  {
    "id": "/subscriptions/b01e1276-bbbd-49df-b177-1f8592512abb/resourceGroups/mc_gregsnsl-rg_gregsnsl-
cluster_westcentralus/providers/Microsoft.Compute/virtualMachineScaleSets/aks-nslpool-28468538-vmss",
    "name": "aks-nslpool-28468538-vmss",
    "type": "Microsoft.Compute/virtualMachineScaleSets",
    "sku": {
      "name": "Standard_D2_v2",
      "tier": "Standard",
      "capacity": 1
    },
    "location": "westcentralus",
    "tags": {
      "Environment": "gregsnsl-cluster",
      "creationSource": "vmssclient-aks-nslpool-28468538-vmss",
      "orchestrator": "Kubernetes:1.20.9",
      "poolName": "nslpool",
      "resourceNameSuffix": "28468538"
    }
  },
  {
    "id": "/subscriptions/b01e1276-bbbd-49df-b177-1f8592512abb/resourceGroups/mc_gregsnsl-rg_gregsnsl-
cluster_westcentralus/providers/Microsoft.Network/loadBalancers/kubernetes",
    "name": "kubernetes",
    "type": "Microsoft.Network/loadBalancers",
    "sku": {
      "name": "Standard"
    },
    "location": "westcentralus",
    "tags": {
      "Environment": "gregsnsl-cluster"
```

```
    }
  },
  {
    "id": "/subscriptions/b01e1276-bbbd-49df-b177-1f8592512abb/resourceGroups/mc_gregsnsl-rg_gregsnsl-
cluster_westcentralus/providers/Microsoft.Network/networkSecurityGroups/aks-agentpool-28468538-nsg",
    "name": "aks-agentpool-28468538-nsg",
    "type": "Microsoft.Network/networkSecurityGroups",
    "location": "westcentralus",
    "tags": {
      "Environment": "gregsnsl-cluster"
    }
  },
  {
    "id": "/subscriptions/b01e1276-bbbd-49df-b177-1f8592512abb/resourceGroups/MC_gregsnsl-rg_gregsnsl-
cluster_westcentralus/providers/Microsoft.Network/publicIPAddresses/40d8626e-6a6a-41a4-8e0d-11741da213f4",
    "name": "40d8626e-6a6a-41a4-8e0d-11741da213f4",
    "type": "Microsoft.Network/publicIPAddresses",
    "sku": {
      "name": "Standard"
    },
    "location": "westcentralus",
    "tags": {
      "type": "aks-slb-managed-outbound-ip"
    }
  },
  {
    "id": "/subscriptions/b01e1276-bbbd-49df-b177-1f8592512abb/resourceGroups/mc_gregsnsl-rg_gregsnsl-
cluster_westcentralus/providers/Microsoft.Network/publicIPAddresses/kubernetes-aeae725b8823e4e65a3a239fabe086a2",
    "name": "kubernetes-aeae725b8823e4e65a3a239fabe086a2",
    "type": "Microsoft.Network/publicIPAddresses",
    "sku": {
      "name": "Standard"
    },
    "location": "westcentralus",
    "tags": {
      "Environment": "gregsnsl-cluster",
      "kubernetes-cluster-name": "kubernetes",
      "service": "gregsnsl-ingress/nginx-ingress-ingress-nginx-controller"
    }
  },
  {
    "id": "/subscriptions/b01e1276-bbbd-49df-b177-1f8592512abb/resourceGroups/mc_gregsnsl-rg_gregsnsl-
cluster_westcentralus/providers/Microsoft.Network/routeTables/aks-agentpool-28468538-routetable",
    "name": "aks-agentpool-28468538-routetable",
    "type": "Microsoft.Network/routeTables",
    "location": "westcentralus",
    "tags": {
      "Environment": "gregsnsl-cluster"
    }
  },
  {
    "id": "/subscriptions/b01e1276-bbbd-49df-b177-1f8592512abb/resourceGroups/MC_gregsnsl-rg_gregsnsl-
cluster_westcentralus/providers/Microsoft.Network/virtualNetworks/aks-vnet-28468538",
    "name": "aks-vnet-28468538",
    "type": "Microsoft.Network/virtualNetworks",
    "location": "westcentralus"
  }
]
```

Get Kubernetes Info

This function sends the following REST call to Azure.

[Managed Clusters - List - REST API (Azure AKS) | Microsoft Docs]

If successful, this function returns the Kubernetes information for the authenticated Client ID.

Note that all resources are returned by Azure. SLAnalyzer will then query information about each resource to gather additional information about Kubernetes.

1 entry example from response.


```
{
  "id": "/subscriptions/b01e1276-bbbd-49df-b177-1f8592512abb/resourcegroups/gregsnsl-
rg/providers/Microsoft.ContainerService/managedClusters/gregsnsl-cluster",
  "location": "westcentralus",
  "name": "gregsnsl-cluster",
  "tags": {
    "Environment": "gregsnsl-cluster"
  },
  "type": "Microsoft.ContainerService/ManagedClusters",
  "properties": {
    "provisioningState": "Succeeded",
    "powerState": {
      "code": "Running"
    },
    "kubernetesVersion": "1.20.9",
    "dnsPrefix": "gregsnsl",
    "fqdn": "gregsnsl-39ae6ba0.hcp.westcentralus.azmk8s.io",
    "azurePortalFQDN": "gregsnsl-39ae6ba0.portal.hcp.westcentralus.azmk8s.io",
    "agentPoolProfiles": [
      {
        "name": "nslpool",
        "count": 1,
        "vmSize": "Standard_D2_v2",
        "osDiskSizeGB": 128,
        "osDiskType": "Managed",
        "maxPods": 110,
        "type": "VirtualMachineScaleSets",
        "enableAutoScaling": false,
        "provisioningState": "Succeeded",
        "powerState": {
          "code": "Running"
        },
        "orchestratorVersion": "1.20.9",
        "enableNodePublicIP": false,
        "mode": "System",
        "osType": "Linux",
        "osSKU": "Ubuntu",
        "nodeImageVersion": "AKSUbuntu-1804containerd-2021.09.22",
        "enableFIPS": false
      }
    ],
    "servicePrincipalProfile": {
      "clientId": "ddd94951-0266-47cd-b84a-671f90d465ed"
    },
    "addonProfiles": {
      "aciConnectorLinux": {
        "enabled": false,
        "config": null
      },
      "azurepolicy": {
        "enabled": false,
        "config": null
      },
      "httpApplicationRouting": {
```

```
        "enabled": false,
        "config": null
      },
      "kubeDashboard": {
        "enabled": false,
        "config": null
      },
      "omsagent": {
        "enabled": false,
        "config": null
      }
    },
    "nodeResourceGroup": "MC_gregsnsl-rg_gregsnsl-cluster_westcentralus",
    "enableRBAC": false,
    "networkProfile": {
      "networkPlugin": "kubenet",
      "loadBalancerSku": "Standard",
      "loadBalancerProfile": {
        "managedOutboundIPs": {
          "count": 1
        },
        "effectiveOutboundIPs": [
          {
            "id": "/subscriptions/b01e1276-bbbd-49df-b177-1f8592512abb/resourceGroups/MC_gregsnsl-rg_gregsnsl-
cluster_westcentralus/providers/Microsoft.Network/publicIPAddresses/40d8626e-6a6a-41a4-8e0d-11741da213f4"
          }
        ]
      },
      "podCidr": "10.244.0.0/16",
      "serviceCidr": "10.0.0.0/16",
      "dnsServiceIP": "10.0.0.10",
      "dockerBridgeCidr": "172.17.0.1/16",
      "outboundType": "loadBalancer"
    },
    "maxAgentPools": 100,
    "apiServerAccessProfile": {
      "enablePrivateCluster": false
    }
  },
  "sku": {
    "name": "Basic",
    "tier": "Free"
  }
}
```


SLAnalyzer will process each of the responses to determine which resources match the application. It will then query each of the subsequent node definitions for additional data via the following REST call. [Managed Clusters - Get - REST API (Azure AKS) | Microsoft Docs]

If successful Azure will return information about each node in the AKS cluster


```
{
  "id": "/subscriptions/b01e1276-bbbd-49df-b177-1f8592512abb/resourceGroups/gregsnsl-
rg/providers/Microsoft.ContainerRegistry/registries/gregsnslacr",
  "name": "gregsnslacr",
  "type": "Microsoft.ContainerRegistry/registries",
  "sku": {
    "name": "Basic",
    "tier": "Basic"
  },
  "location": "westcentralus",
  "tags": {},
  "systemData": {
    "createdBy": "greg.morris@microfocus.com",
    "createdByType": "User",
```

```
    "createdAt": "2021-10-01T15:21:33.1591427Z",
    "lastModifiedBy": "greg.morris@microfocus.com",
    "lastModifiedByType": "User",
    "lastModifiedAt": "2021-10-01T15:21:33.1591427Z"
  }
}
```


Get Kubernetes Name Space

This function communicates with the Kubernetes node and runs a bash command to return the configured name space.

The command is sent to the node via this REST call.
[Managed Clusters - Run Command - REST API (Azure AKS) | Microsoft Docs]

"{\"command\":\"kubectl get namespaces\",\"context\":\"\",\"clusterToken\":\"\"}"

If successful, the node will return a list of name spaces

NAME STATUS AGE

aks-command Active 42d

default Active 61d

gregsnsl-ingress Active 61d

kube-node-lease Active 61d

kube-public Active 61d

kube-system Active 61d

SLAnalyzer will process the name spaces to determine which name space matches the application definition name. in this case gregsnsl-ingress.

Get Kubernetes Pods

This function communicates with the Kubernetes node and runs a bash command to return the information for each pod.

The command is sent to the node via this REST call.
[Managed Clusters - Run Command - REST API (Azure AKS) | Microsoft Docs]

"{\"command\":\"kubectl get services -n gregsnsl-ingress\",\"context\":\"\",\"clusterToken\":\"\"}"

If successful, the node will return:

NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE

cert-manager ClusterIP 10.0.173.81 <none> 9402/TCP 61d

cert-manager-webhook ClusterIP 10.0.229.178 <none> 443/TCP 61d

nginx-ingress-ingress-nginx-controller LoadBalancer 10.0.15.152 13.78.183.47 80:30408/TCP,443:32763/TCP 61d

nginx-ingress-ingress-nginx-controller-admission ClusterIP 10.0.37.151 <none> 443/TCP 61d

postgres ClusterIP 10.0.1.25 <none> 5432/TCP 49d

slserver ClusterIP 10.0.188.236 <none> 8081/TCP 28d

Get Kubernetes Logs

This function communicates with the Kubernetes node and runs a bash command to return the information for each pod/container within the last hour.

The command is sent to the node via this REST call.
[Managed Clusters - Run Command - REST API (Azure AKS) | Microsoft Docs]

"{\"command\":\"kubectl logs pod/nginx-ingress-ingress-nginx-controller-5d6cdb5c85-g9w9m -n gregsnsl-ingress\",\"context\":\"\",\"clusterToken\":\"\"}"

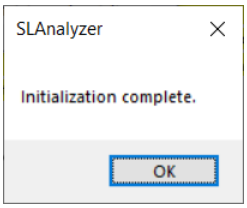
If successful, the node will return:

```
10.244.0.1 - - [27/Nov/2021:23:57:06 +0000] "\x05\x01\x00" 400 150 "-" "-" 0 0.128 [] [] - - - - 53ba41cfce56458d36285f6dbc2203ae
10.244.0.1 - - [28/Nov/2021:00:22:35 +0000] "OPTIONS / RTSP/1.0" 400 150 "-" "-" 0 0.038 [] [] - - - -
1059eb03ed600211e5552e74cdbe117a
10.244.0.1 - - [28/Nov/2021:00:22:36 +0000] "HELP" 400 150 "-" "-" 0 0.040 [] [] - - - - 92e3f515ba3eb8d1630d8ec442fd6c0c
2021/11/28 01:08:16 [crit] 33#33: *8014237 SSL_do_handshake() failed (SSL: error:141CF06C:SSL
routines:tls_parse_ctos_key_share:bad key share) while SSL handshaking, client: 10.244.0.1, server: 0.0.0.0:443
10.244.0.1 - - [28/Nov/2021:02:43:33 +0000] "GET / HTTP/1.1" 400 248 "-" "-" 37 0.000 [] [] - - - -
fd62b62845a974b4c3f9d15ba17cf716
10.244.0.1 - - [28/Nov/2021:03:30:22 +0000] "GET / HTTP/1.1" 400 248 "-" "-" 37 0.000 [] [] - - - -
cf18a0703dba07c3fe218e94f081c64b
10.244.0.1 - - [28/Nov/2021:03:34:33 +0000] "SSTP_DUPLEX_POST /sra_{BA195980-CD49-458b-9E23-C84EE0ADCD75}/
HTTP/1.1" 400 150 "-" "-" 191 0.000 [] [] - - - - ff921c06c4ed85755f4e62a8cd763d24
10.244.0.1 - - [28/Nov/2021:03:37:52 +0000] "CONNECT 85.206.160.115:80 HTTP/1.1" 400 150 "-" "-" 0 0.128 [] [] - - - -
8232a627bf88933503e64256633ddd2a
10.244.0.1 - - [28/Nov/2021:03:43:51 +0000] "GET / HTTP/1.0" 400 248 "-" "-" 18 0.000 [] [] - - - -
9067105a419f244072e45177378d9c45
…
…
```

Initalize for Kubernetes

Note the option "Initialize for Kubernetes" is a quick method of getting logged in and gathering the required information necessary for using the Kubernetes terminal and node explorer. These features require the information from the Azure functions Subscription, Resource, Kubernetes info, Kubernetes name space, and Kubernetes pods. Users will need to either use the Initalize for Kubernetes function or manually select each of the individual functions (in order) to gather the necessary information for use with the Kubernetes terminal and node explorer.

After successful initialization SLAnalyzer will inform the user that the process completed.



Initialize for Kubernetes automates the following in order:

1. Azure Client Login or SecureLogin AE Login
2. Get Subscriptions
3. Get Resources
4. Get Kubernetes Info
5. Get Kubernetes Name Space
6. Get Kubernetes Pods

KubeCtl terminal

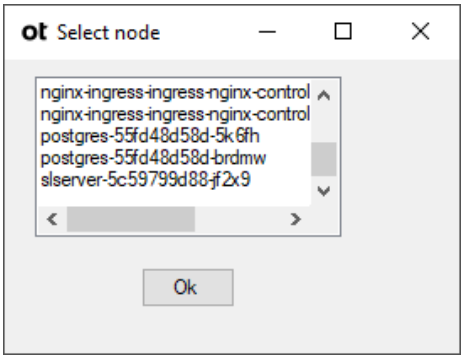
This function allows the execution of commands on a specific node. This allows standard Linux commands to be sent to the node/container.

Note that this option requires the steps be completed as noted under Initialize for Kubernetes

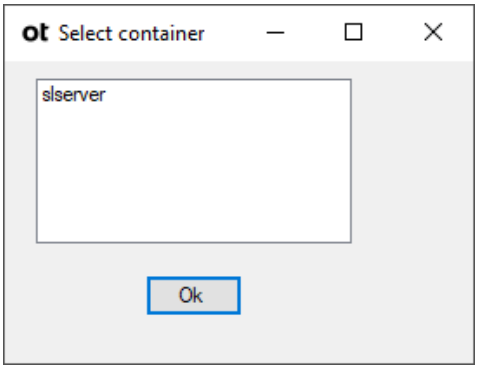
Commands to the node are sent via the Azure REST call:

The command is sent to the node via this REST call.
Managed Clusters - Run Command - REST API (Azure AKS) | Microsoft Docs

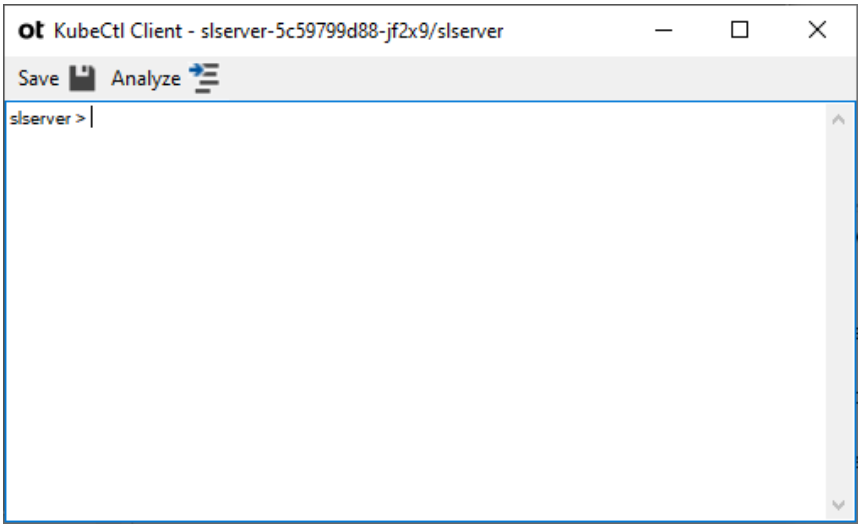
After selecting this feature SLAnalyzer will prompt for selection of the desired node. Click on the desired node and then click Ok.



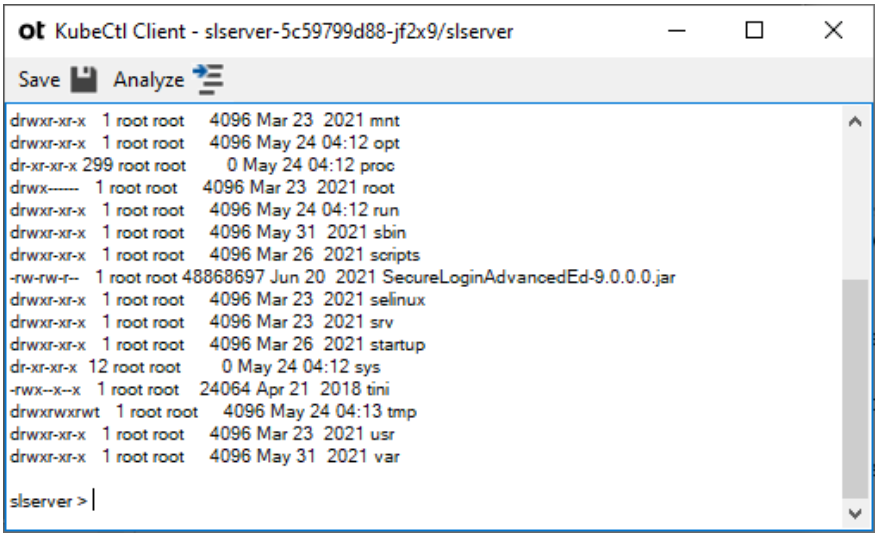
After selecting the desired node, SLAnalyzer will prompt the user to select the desired container.



After selecting the desired container, the terminal window will be displayed.



The terminal is a BASH terminal and the user can then enter normal Linux commands. For example, ls -l will return a listing of the files/directories in the root container of the selected node.



The terminal window will remember the commands entered. Pressing the up arrow will repeat the commands used during the terminal session.

Typing cls will clear the terminal screen

Typing exit will close the terminal

One limitation of the terminal is that it is based off of the root folder. You cannot CD into another folder but instead reference the folder in your command. For example, to list the contents of the etc folder you would type something like “ls -l /etc”

The base image used by Azure for a Linux host is Ubuntu. This version contains a base configuration and many standard Linux packages are not installed by default. To install a missing package (IE sudo) then use the zypper command to install the necessary package and its dependent modules.

For example,

zypper -n install sudo

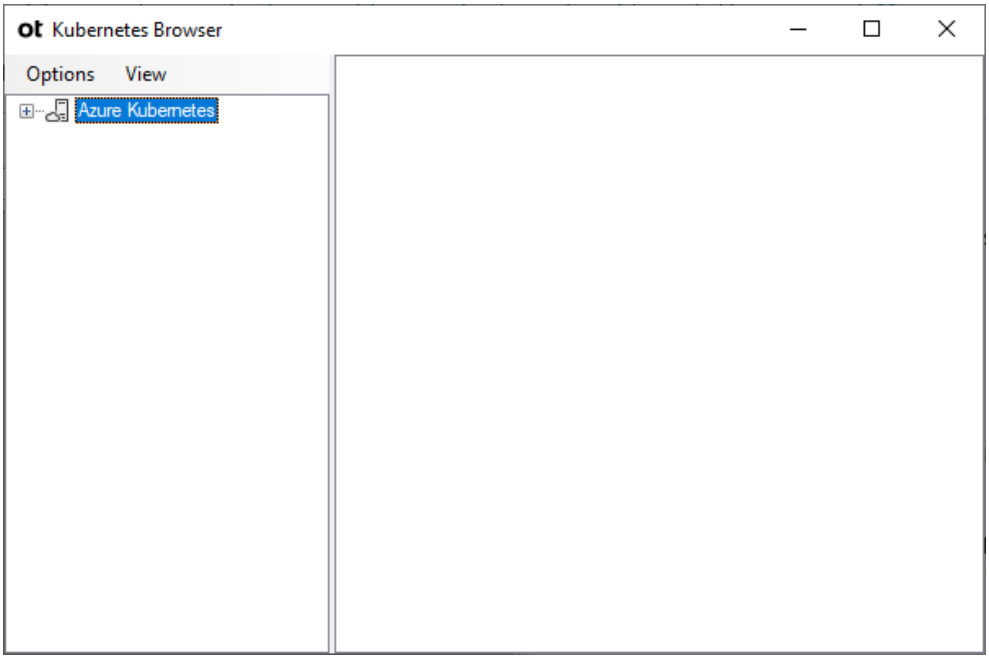
This will install sudo within the selected node/container. This same process can be used to install other required packages.

For more information about Kubernetes components see this link.

Kubernetes Node Explorer

The node explorer is much easier to use then the terminal because you can perform many functions from within the explorer and obtain a view of the file system without having to type Linux commands. These commands are all automated to make the user experience much better.

Note that this option requires the steps be completed as noted under Initialize for Kubernetes

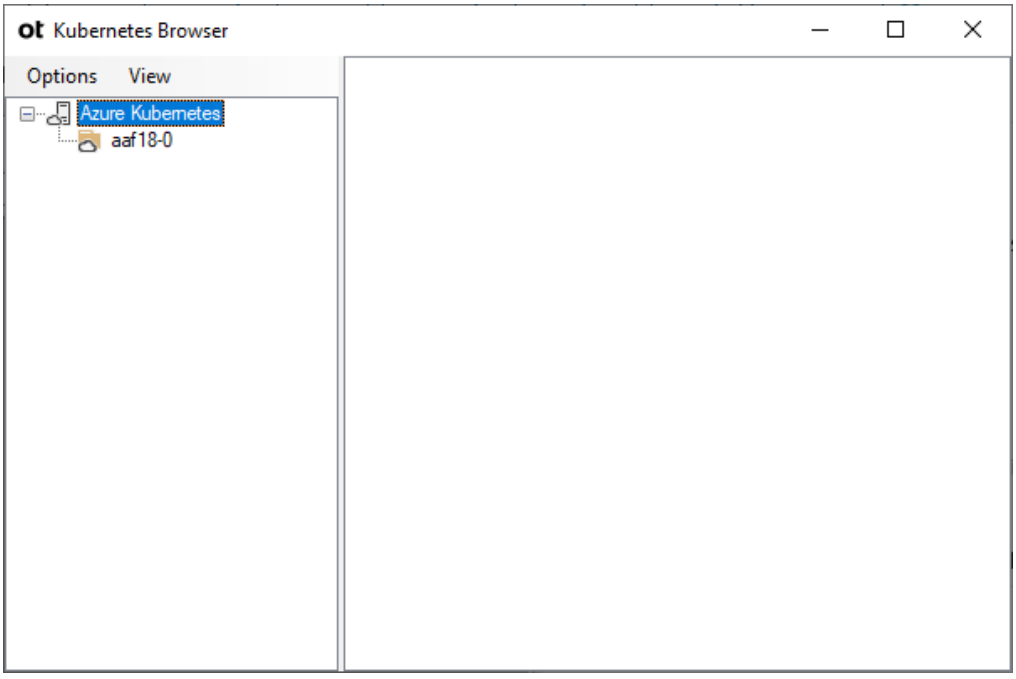


Click the plus symbol or double click the item in the left part of the window to expand the item.

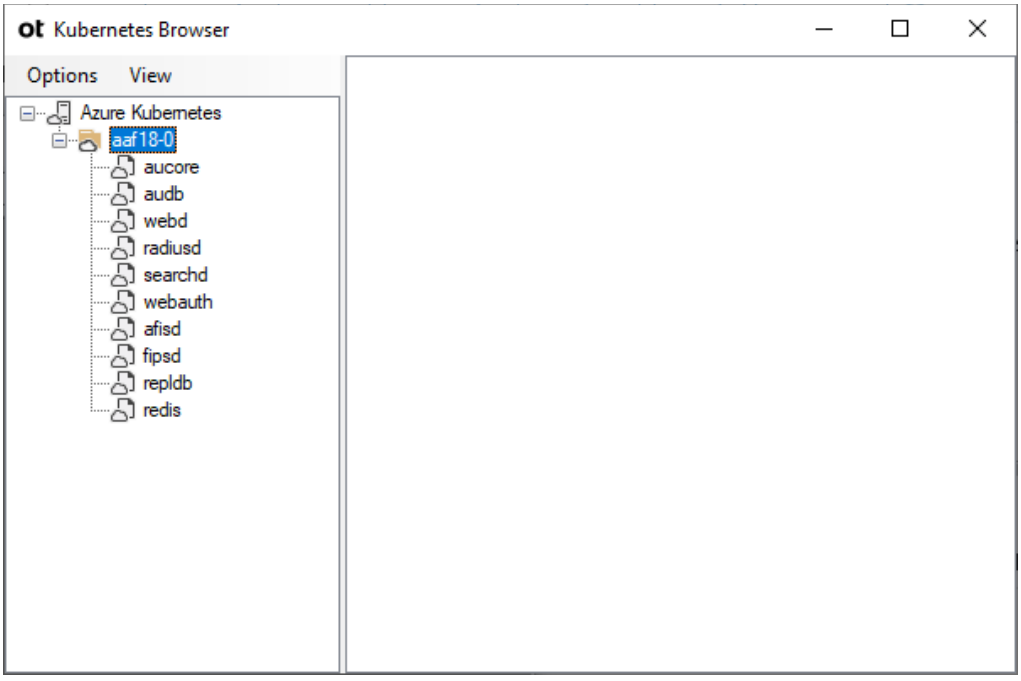
An Azure Kubernetes cluster has the following components viewable in the Node explorer.

1. Cluster Nodes – The node is the parent for one or more containers.
2. Containers – The container is the file system or other Kubernetes objects.

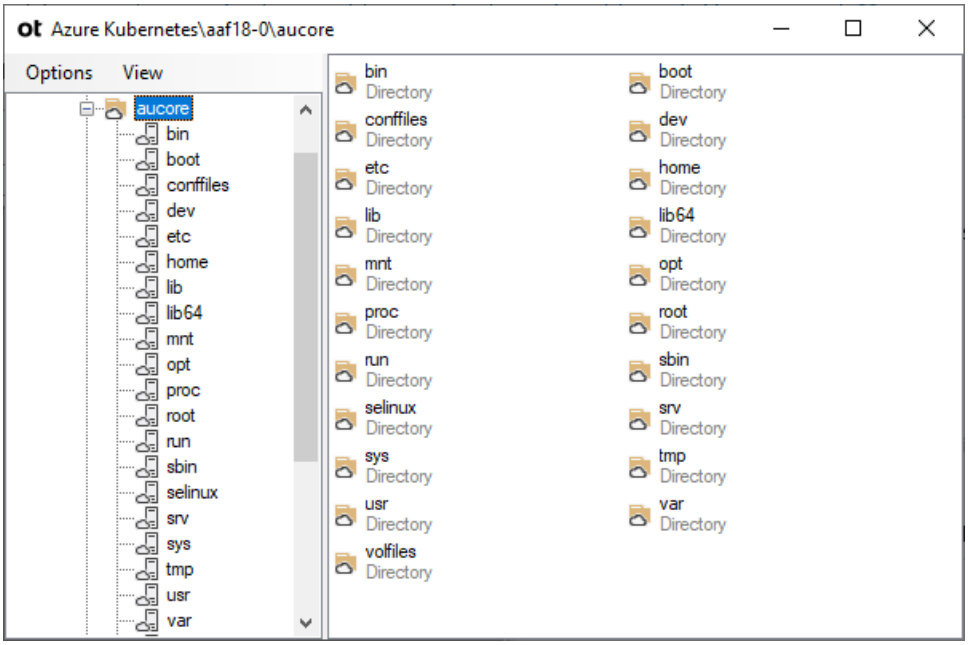
For more information about Kubernetes components see this link.



Selecting a node will display the containers for that selected node.



Selecting a container will display the file system (if applicable)

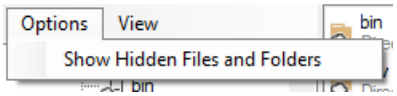


The node explorer contains a number of functions.

Options menu

The main menu provides Options and View

Options allows the inclusion of hidden files and folders.

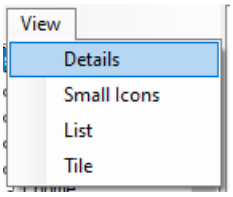


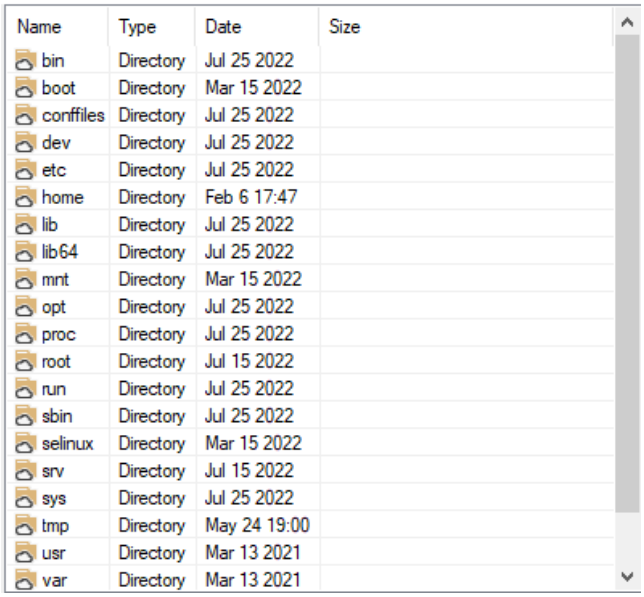
By default hidden files and folders are not displayed. Note that changing this value will be remembered between instances of SLAnalyzer.

View menu

The View menu option allows the user to change the view of the files and folders displayed in the explorer window (right side). As with Options the user selected view will be remembered between instances of SLAnalyzer.

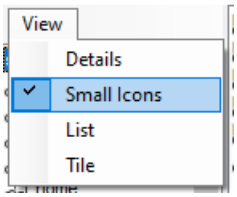
Details view

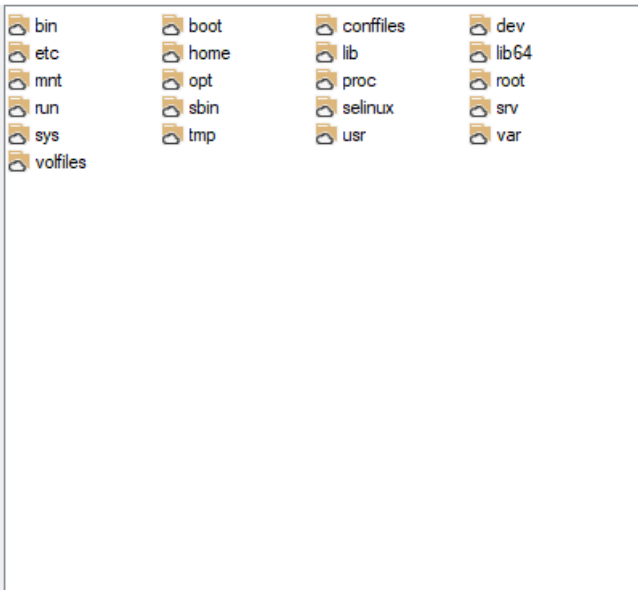




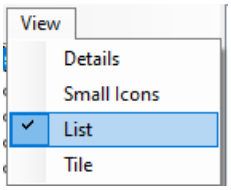
Name	Type	Date	Size
bin	Directory	Jul 25 2022	
boot	Directory	Mar 15 2022	
conffiles	Directory	Jul 25 2022	
dev	Directory	Jul 25 2022	
etc	Directory	Jul 25 2022	
home	Directory	Feb 6 17:47	
lib	Directory	Jul 25 2022	
lib64	Directory	Jul 25 2022	
mnt	Directory	Mar 15 2022	
opt	Directory	Jul 25 2022	
proc	Directory	Jul 25 2022	
root	Directory	Jul 15 2022	
run	Directory	Jul 25 2022	
sbin	Directory	Jul 25 2022	
selinux	Directory	Mar 15 2022	
srv	Directory	Jul 15 2022	
sys	Directory	Jul 25 2022	
tmp	Directory	May 24 19:00	
usr	Directory	Mar 13 2021	
var	Directory	Mar 13 2021	

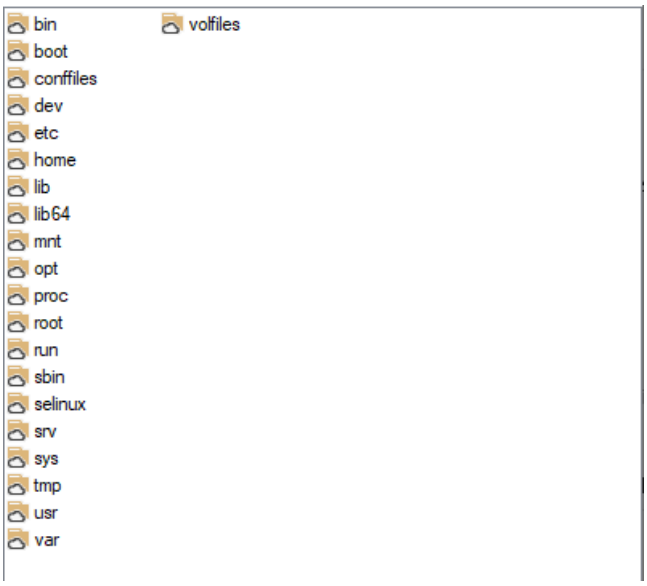
Small Icons view



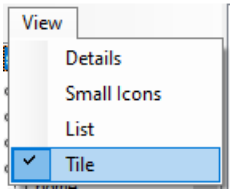


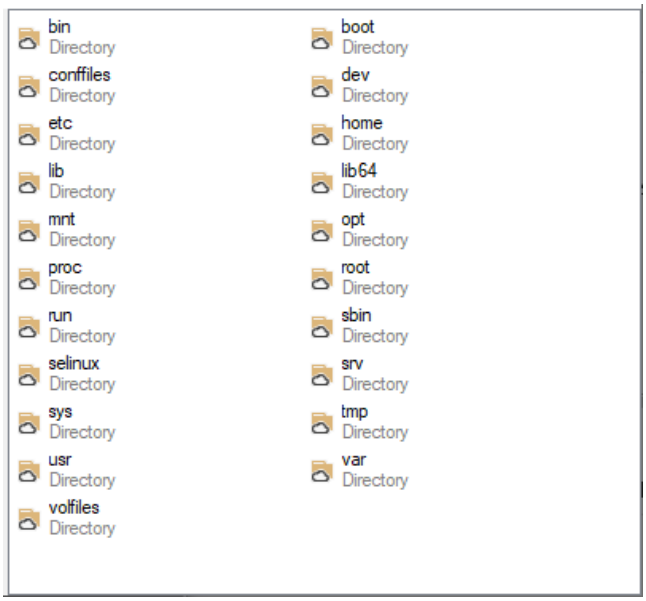
List view





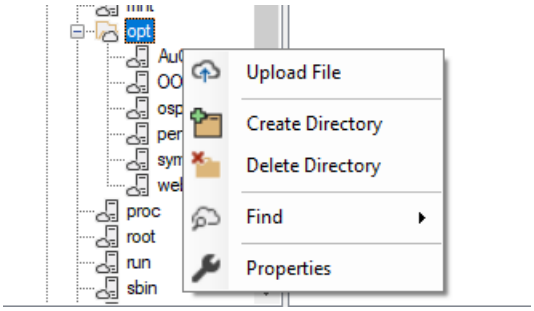
Tile view (default view)



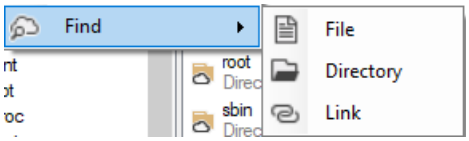


Node/Container/Directory functions

The left side of the explorer window provides several functions. Right click on an entry to see the options available.



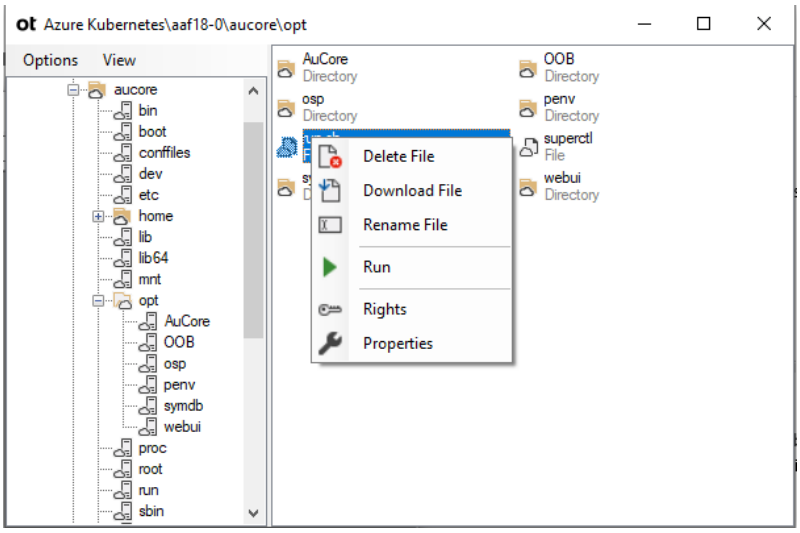
- Upload File – will attempt to upload a file to the selected directory
- Create Directory – will attempt to create a directory in the selected directory location
- Delete Directory – will attempt to delete the currently selected directory
- Find – will attempt to search for information starting at the selected directory
    - File – will attempt to find a file starting at the selected directory
    - Directory – will attempt to find a directory starting at the selected directory
    - Link – will attempt to find a link starting at the selected directory



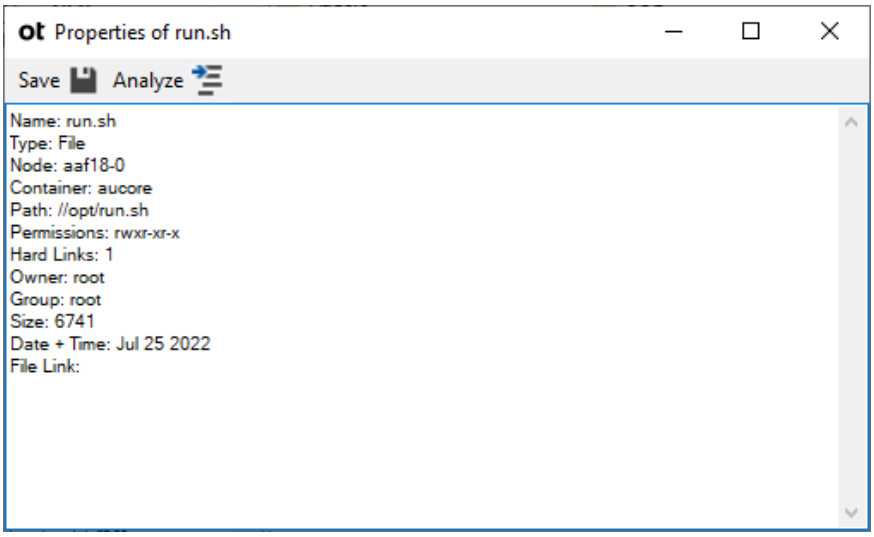
- Properties – will display information about the currently selected object

File functions

The right side of the explorer window also has several different functions. Right click within the right side of the window to display the possible options.



- Delete File – will attempt to delete the selected file
- Download File – will attempt to download the selected file
- Rename File – will attempt to rename the selected file
- Run – will attempt to run the selected file
- Rights – will attempt to modify the permissions of the selected file
- Properties – will display the properties of the selected item



In addition to the context menu, double clicking on a file will display the first part of the file for viewing. Double clicking on a folder will open the folder and display Its contents.

Get File

This function is the same as download file in the node explorer window. When selecting this option, the user is prompted to provide the full path and filename to download.

Send File

This function is the same as upload file in the node explorer window. When selecting this option, the user is prompted for the source file from the local workstation and then the destination folder.

Send a Command

This function is like the KubeCtl terminal but is for a single command. It also is not invoked via BASH so the native command functionality for piping and wildcards will act differently.

To invoke bash with the command type: /bin/bash -c “<command>”
For example: /bin/bash -c "date && whoami"

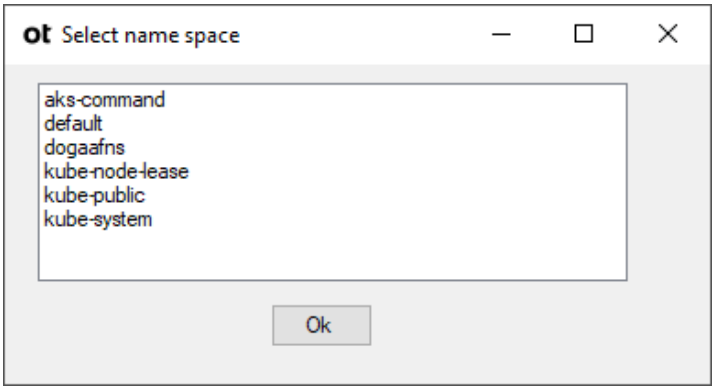
Send REST Get Request

This function allows the user to send any Azure REST command to Azure. Note that this function only supports the GET REST calls. It is used for gathering information where current functions are not currently supported by SLAnalyzer.

The Azure REST calls are documented here.
Azure REST API reference documentation | Microsoft Docs

Viewing Kubernetes Name Space Nodes

An AKS cluster in Azure will have several different name spaces.



aks-command – commands that have been issued to the cluster

dogaafns – name space created for our Kubernetes cluster. Could be any name

kube-system – name space showing default system nodes

To display information about the nodes within a name space then perform the steps outlined in Initialize for Kubernetes.

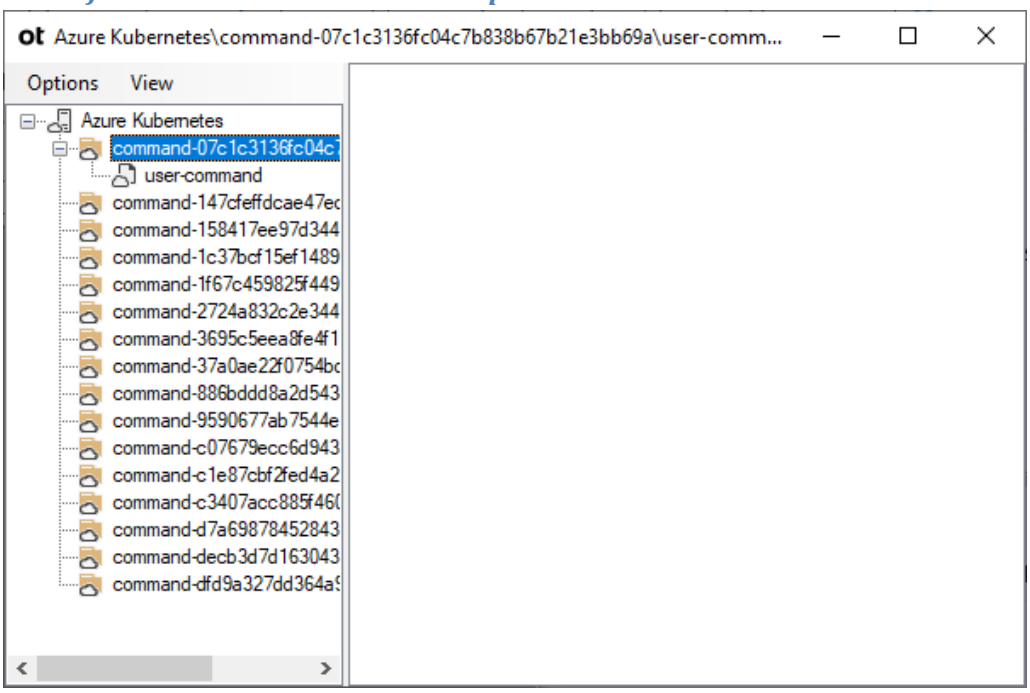
When running Get Kubernetes Name Space, select the desired name space. Then run the command Get Kubernetes Pods. Finally run either the KubeCtl terminal or Kubernetes Node Explorer to view information about the nodes found within the selected name space.

For more information about Kubernetes Name Spaces see this: Namespaces | Kubernetes

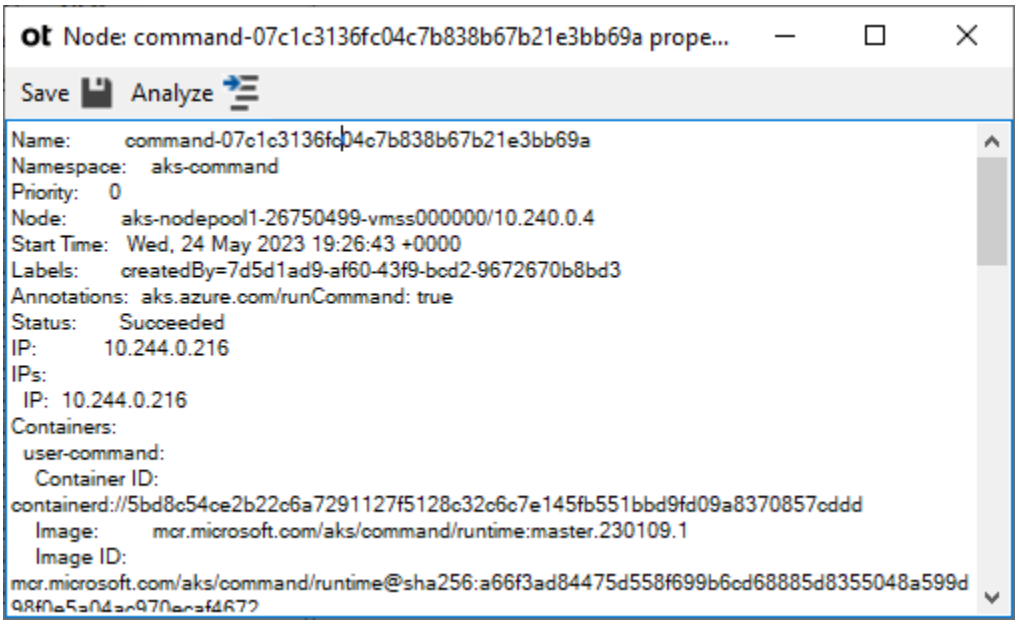
To switch between different name spaces, select:

- Tools->Azure->Get Kubernetes Name Space
- Tools->Azure->Get Kubernetes Pods
- Tools->Azure->Kubernetes Node Explorer or Tools->Azure->KubeCtl Terminal

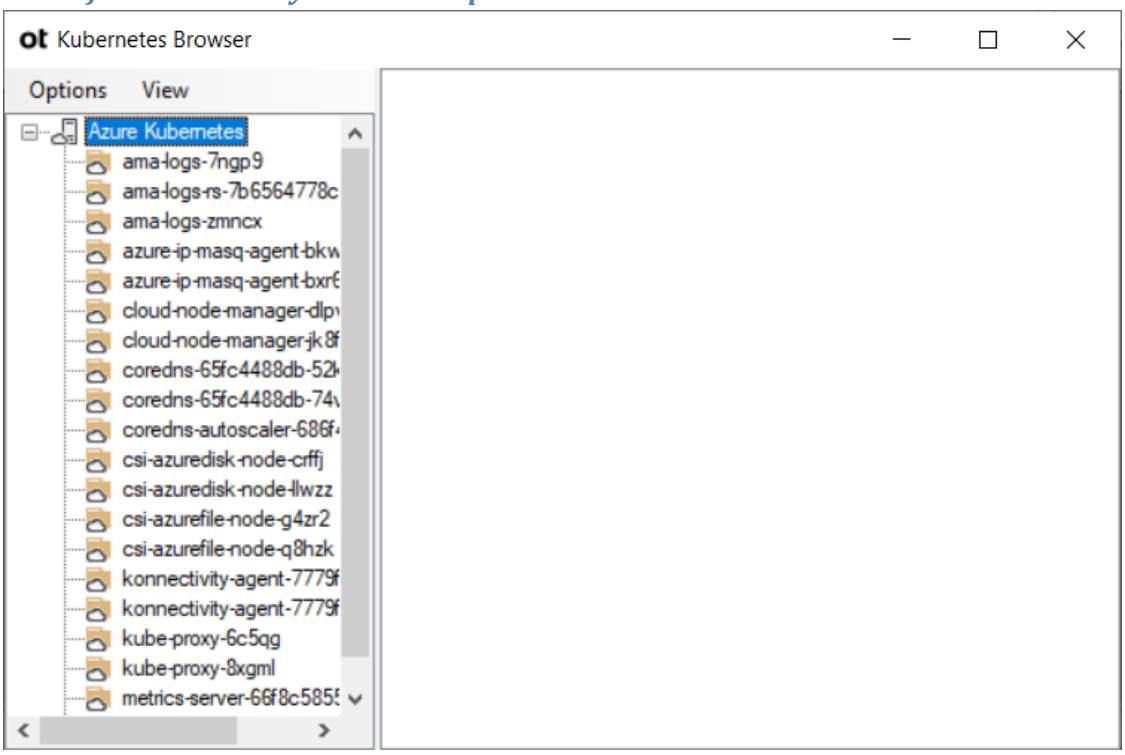
Nodes found in aks-command name space



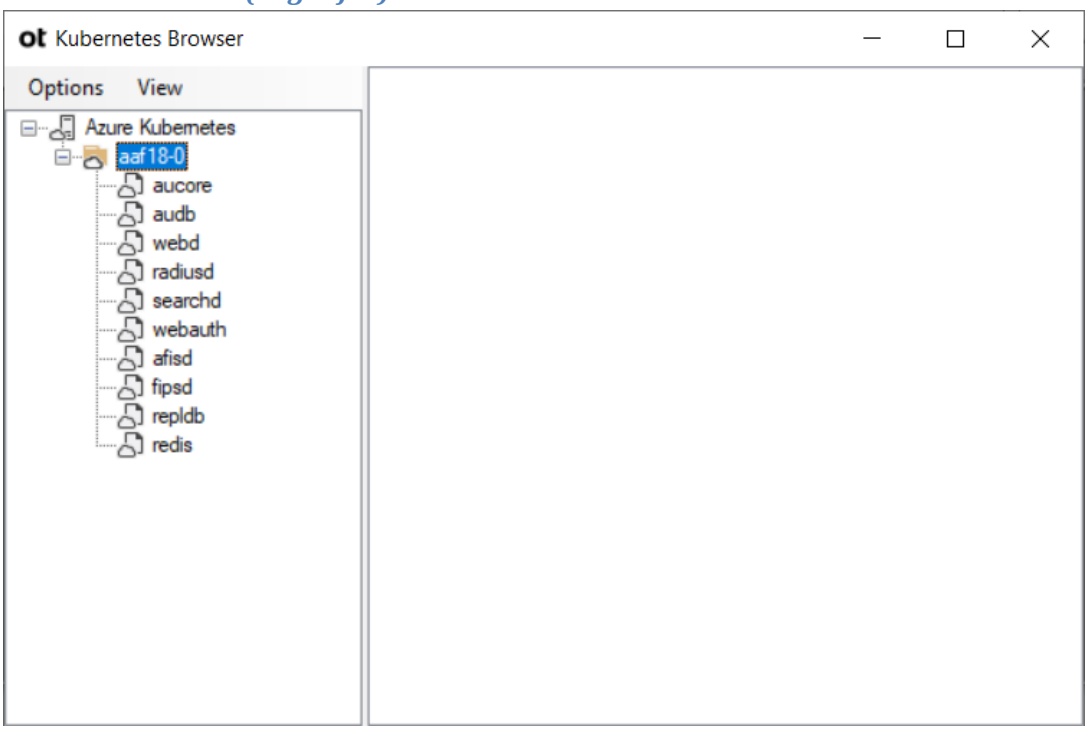
Right click in the left side pane and select Properties.



Nodes found in kube-system name space

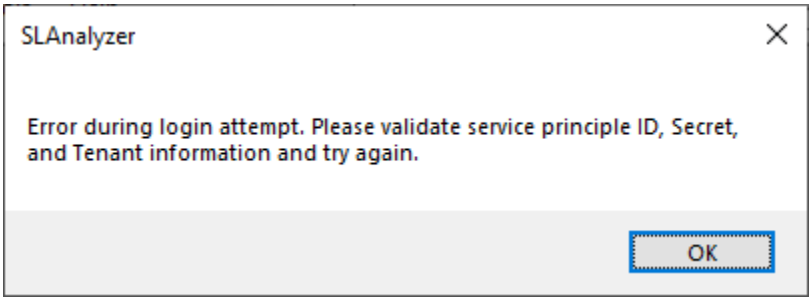


Product AKS Node (dogaafns)



Troubleshooting Azure connectivity

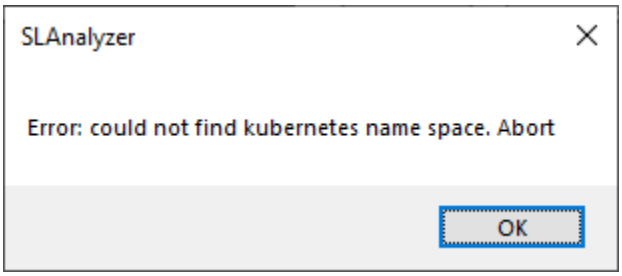
Login failure due to wrong client ID, secret, or tenant information.



Enter the correct information into the login page and try again. This applies to the following items under tools->Azure.

1. Azure AD Login
2. Azure Client Login
3. SecureLogin AE Login
4. Initialize for Kubernetes

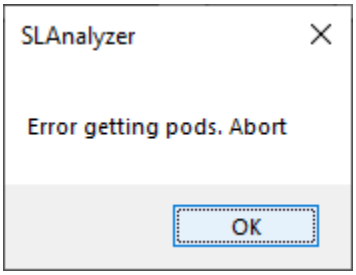
Selecting a resource group and then selecting a cluster object not in that resource group



After login and gathering the subscription and resource group, if the wrong cluster object is selected then SLAnalyzer will display this message. Retry the operation and select the correct cluster resource. See the steps listed for Initialize for Kubernetes.

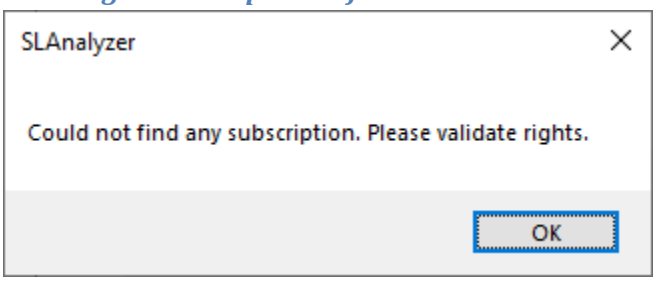
It is important to understand that Azure creates two cluster objects.

Selecting the resource group, cluster, but not the correct name space



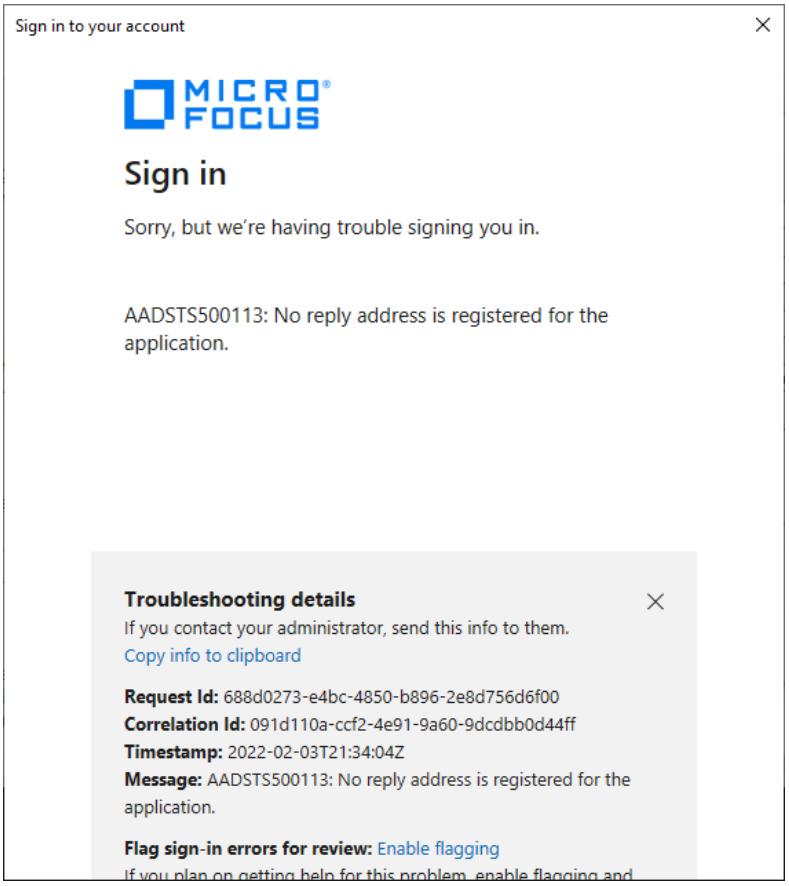
After login and gathering the subscription, resource group and cluster object, if the incorrect name space is specified then this error will be displayed. Retry the operation and select the correct name space. See the steps listed for Initialize for Kubernetes.

Cannot get subscription information



After login when trying to gather subscription information this error appears. This is the result of the service principle not having access rights to subscription information. See the section Prerequisites – Granting access to a service principal for Azure access.

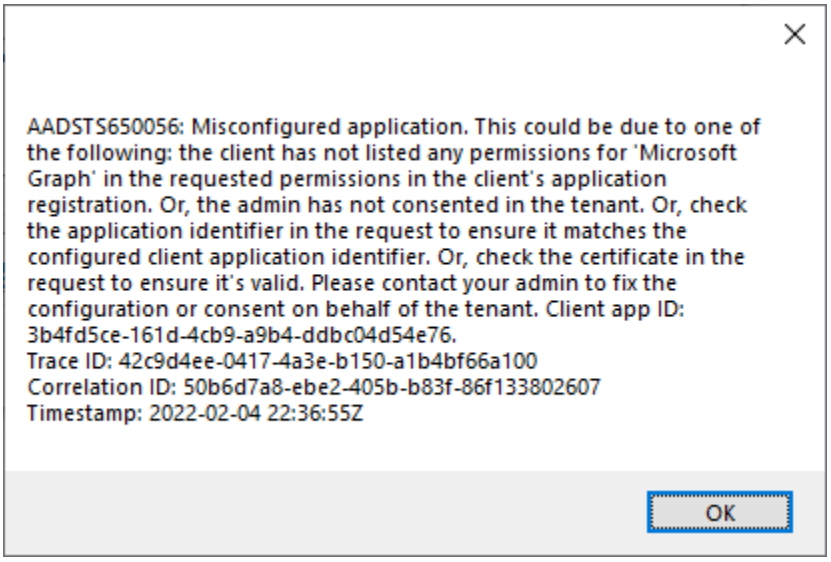
Azure error during login to AD in Azure – No reply address



The service principle does not have the necessary authentication configuration.

See step 5 in the section Prerequisites – Granting access to a service principal for Azure AD access

Azure error during login to AD in Azure – Misconfigured application



The service principle does not have the necessary API permissions

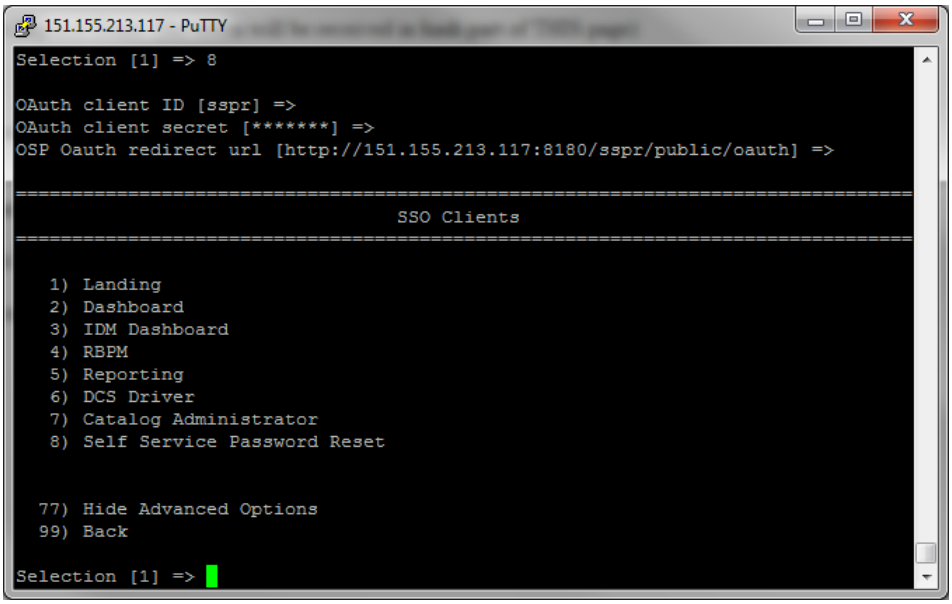
See step 8 in the section Prerequisites – Granting access to a service principal for Azure AD access

Identity Manager

Getting IDM information

Prior to running the IDM REST Client tool, we need to know the endpoint information from the IDM configuration. Follow the steps below to gather the appropriate information.

1. SSH to the IDM server and login
2. Change to the location - /opt/netiq/idm/apps/UserApplication
3. Run configupdate.sh - ./configupdate.sh
4. Select option 3 Authentication
5. Select option 1 Authentication Server
6. Validate ip address and port (Write down for use in SLAnalyzer)
7. Select option 99 Back
8. Select option 4 SSO Clients



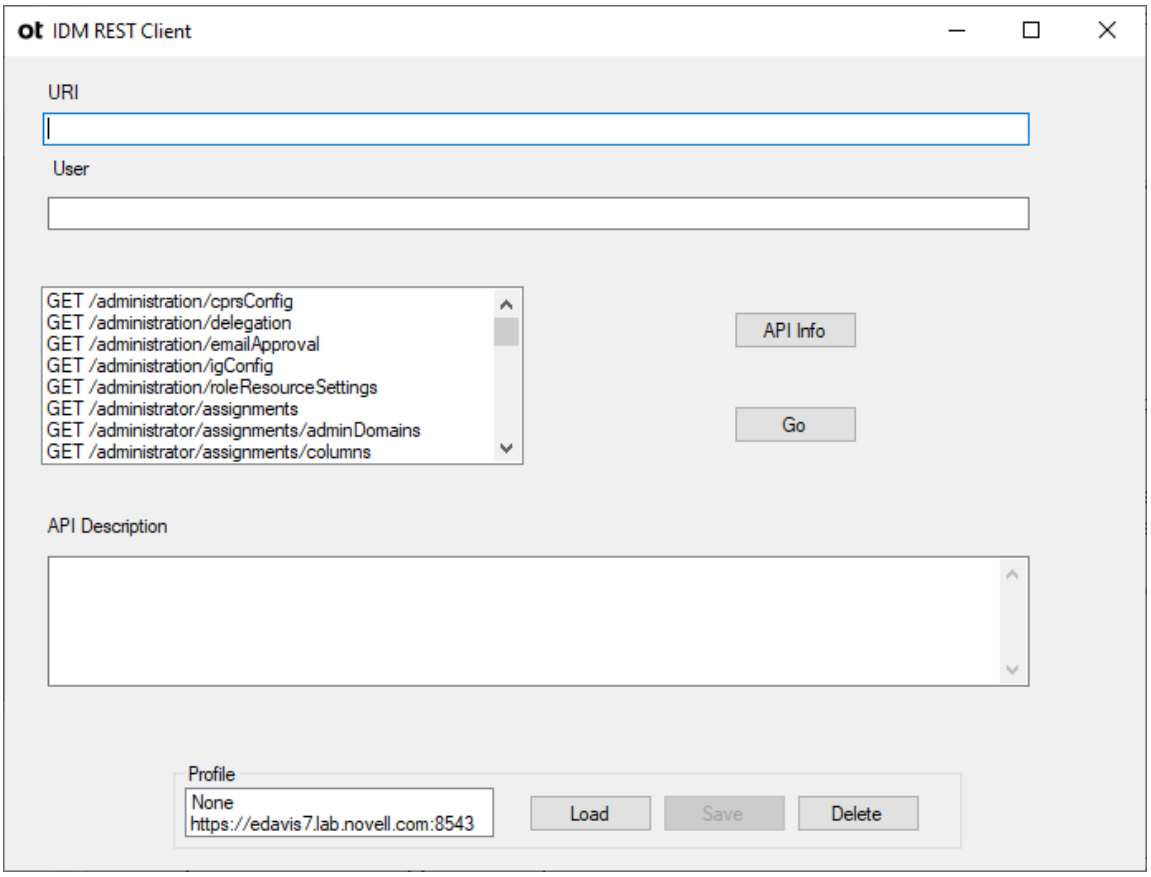
9. Select option 5 Reporting
10. Validate OAuth client ID (Write down for use in SLAnalyzer)
11. Validate/update OAuth client secret (Write down for use in SLAnalyzer)
12. Select 99 Back
13. Select either option 88 Cancel if password wasn't changed, or option 99 Save.

Rest Client

This option provides the ability to submit REST calls to an IDM server. Before using this tool follow the steps outlined in the section "Getting IDM information"

The IDM REST Client window contains the following controls:

- URI – Specifies the location resource (IDM server)
- User – User credentials for performing the API/REST call
- API List – This box lists all of the available API/REST calls that can be performed
- API Info button – Forces the read of API data from the specified IDM server
- Go button – Performs the selected API/REST call
- API Description – Provides information about the selected API/REST call



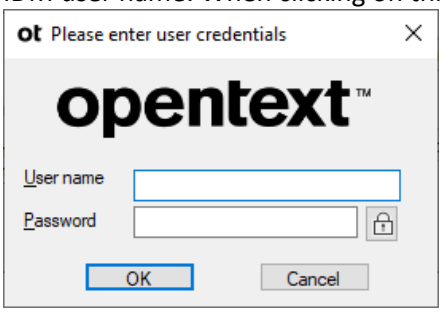
Window components:

URI

Enter server protocol + DNS/IP Address + Port. For example: http://myidmserver.example.com:8180
This information should have been obtained when gathering the IDM information.
See section Getting IDM Information.

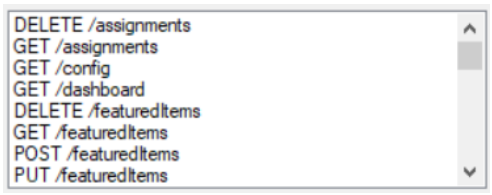
User

IDM user name. When clicking on this box, SLAnalyzer will prompt for the user credentials.



API List

List of available REST/API calls. Select the desired REST/API call by clicking the item in the list.

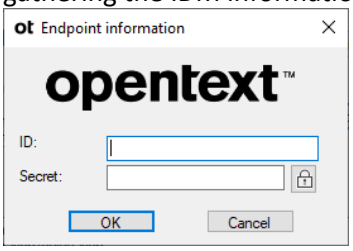


API Info button

Forces the read of API information from the specified URI.

Go button

Submits the selected API to the server. If the REST call requires additional parmaters then the user will be prompted. If an endpoint is not yet been defined then the user will be prompted for the endpoint for SLAnalyzer to use when submitting the API call. This information should have been obtained when gathering the IDM information. See section Getting IDM Information.



API Description

Text based field that describes the selected API.

Gather Support Bundle

This option requires an SSH connection to the Identity Manager server. When selected SLAnalyzer will first prompt for the SSH connection information. After successful login diagnostic information will be gathered from the server and downloaded to the local workstation.

LDAP Browser

This option will open a new window designed to allow the testing of LDAP communications between the workstation and the server. You will have the option of connecting to the LDAP server with an anonymous bind or with specified user credentials. This feature has been tested against AD and eDirectory server platforms but should work with any LDAP v3 compliant server.

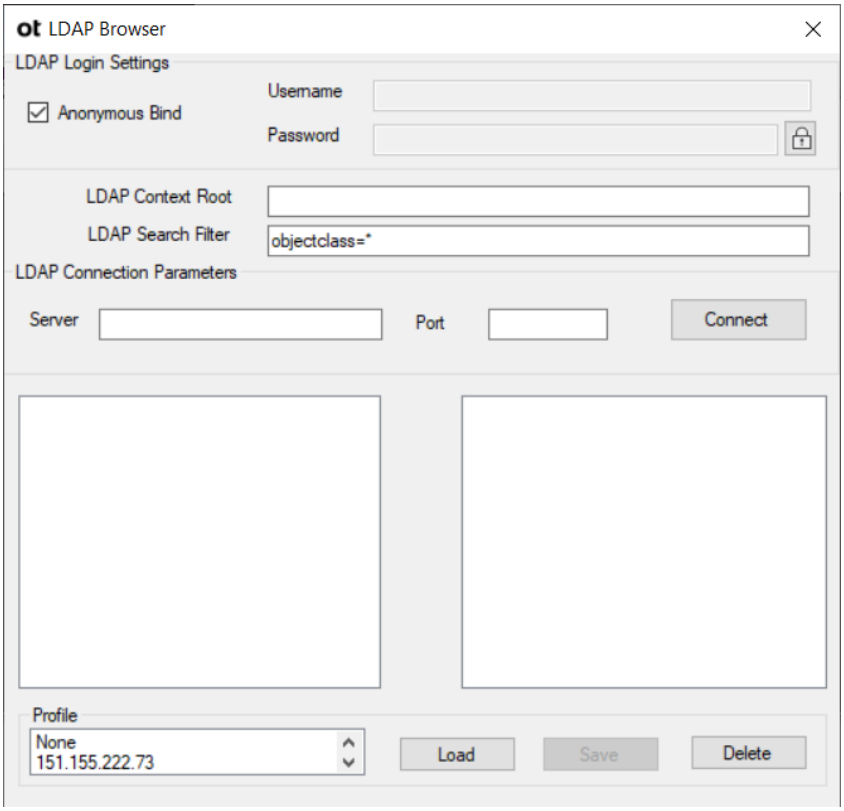


Figure 186 - LDAP browser

The LDAP Browser window has the following components

- LDAP Login Settings
- LDAP Search Criteria
- LDAP Connection Parameters
- LDAP object window
- LDAP attribute window
- Profile data

LDAP Login Settings

The Anonymous Bind checkbox indicates if user credentials will be used or if the anonymous user will be utilized when binding to the LDAP server. Note that in some environments anonymous binds are disabled in the directory and only LDAP binds with real user credentials will be successful. This tool has been designed to allow for testing in both types of environments. To enter a username and password for the LDAP bind process, uncheck the box Anonymous Bind.

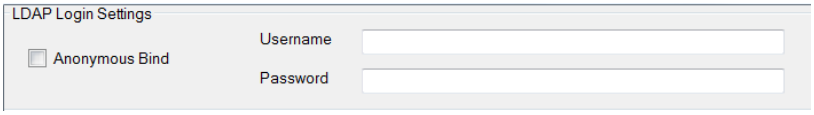


Figure 187 - LDAP Login Settings

The Username box is used to define the username and context to be used when making an LDAP connection to the server. This option is only available when the Anonymous Bind checkbox is unchecked. The full LDAP syntax needs to be supplied here.

For example:
In an AD environment
cn=administrator,cn=users,dc=gmadr2,dc=novell,dc=com

If you are having a problem identifying the correct username and context on an AD server, you can use a tool called BeaverTail ADSI Browser to look at the DN of the object.
(http://adsi.mvps.org/adsi/CSharp/beavertail.html)

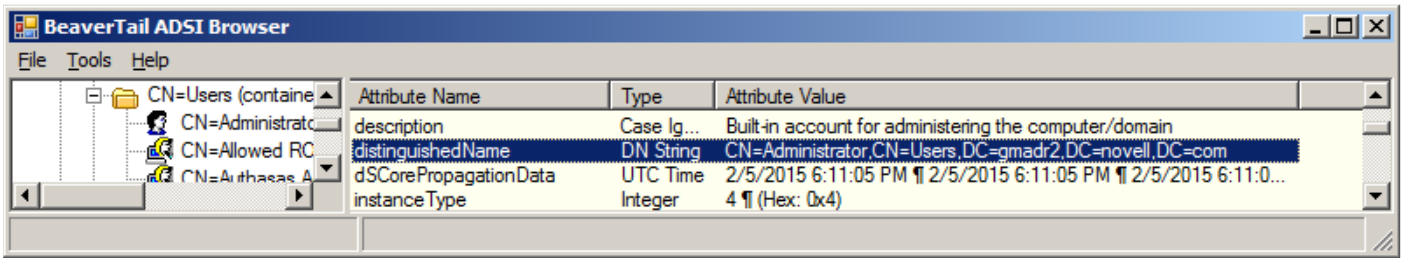


Figure 188 - Beavertail

In an eDirectory environment

cn=admin,o=novell

The password field is for the password of the LDAP user specified in the username field.

LDAP Search Criteria

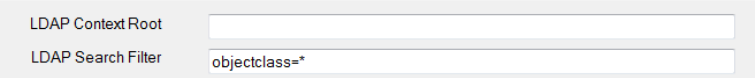


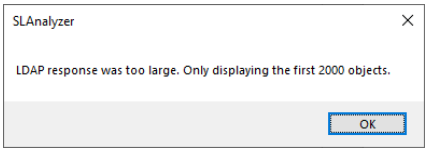
Figure 189 - LDAP Search criteria

LDAP Context Root: This box allows you to enter the root context you want to begin the search from. You can start the search on a container or a single object. Only the subordinate objects of the subject root will be returned in the search. For example, entering cn=users,dc=gmadr2,dc=novell,dc=com will begin the LDAP search at the users container on my AD server. All objects that match my search filter that exist in this container or any subcontainer will be returned. But entering cn=administrator,cn=users,dc=gmadr2,dc=novell,dc=com will only return the LDAP record for the administrator user since there are no subordinate objects.

LDAP Search Filter: This box defines the types of objects you want to return in the LDAP search request. For example return all objects? Or maybe just return all valid user objects? This filter can be complex or simple depending on the type of information you want the LDAP server to return. The following are a few examples:

Description	**Syntax**
Return all records	objectclass=*
Return just groups	objectclass=group
Return just users	objectclass=person
Any object with attribute mobile set too	mobile=18015552222
Any group with a member of test admin	member=cn=test admin,cn=users,dc=gmadr2,dc=novell,dc=com
Return groups or users	(|(objectclass=group)(objectclass=person)
Return groups and users	(&(objectclass=group)(objectclass=person)

Note: LDAP searches can result in a large number of records returned. SLAnalyzer will receive an error message from the LDAP server if the results are too large. When this error is encountered, SLAnalyzer will report the error and then display the data that was returned.



If this error is encountered, modify the search filter to return a smaller set of records.

For example, when searching for all users with the search filter of “objectclass=person”, this error is returned.
The search filter could be changed to “cn<G”. This would return all users whose name starts with the letter A-F.
To continue the search for the next set of users the search filter could be set to “cn>=G”. This would return all users whose name starts with the letter G through Z.
Searches can also be combined to return a smaller group of records. For example to search for users whose names start with G through K then a search filter of “(&(cn>=G)(cn<=K))” could be used.

LDAP Connection Parameters

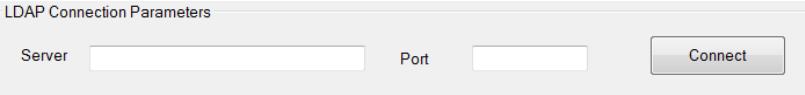


Figure 190 - LDAP connection parameters

Server – The DNS name or IP address of the LDAP server

Port – The TCP port that the LDAP service is listening on (typically ports 636 or 389)

Clicking the Connect button will send the request to the LDAP server.

LDAP Object window

When connecting successfully to an LDAP server then the objects found in the LDAP context root will be displayed.

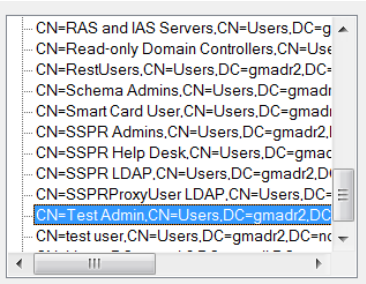


Figure 191 - LDAP Object window

LDAP Attribute window

When selecting an LDAP object in the LDAP Object window, the LDAP attribute window will show the attributes that were found on that object.

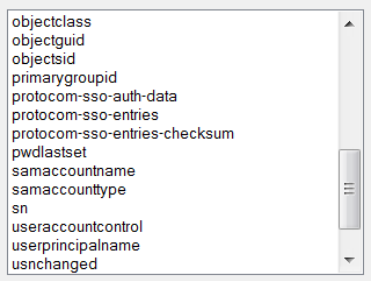


Figure 192 - LDAP Attribute window

Profile data

Allows the storing and retrieving of configuration information of the SSPR Rights Validator window. For general information regarding the use of the profile options refer to the profile data section of the SSPR REST client section of this document. Data stored with this option will be saved to: HKEY_CURRENT_USER\Software\MicroFocus\SLAnalyzer\LDAP.

Viewing LDAP attribute data

Clicking on an attribute name in the attribute window will display the LDAP values.

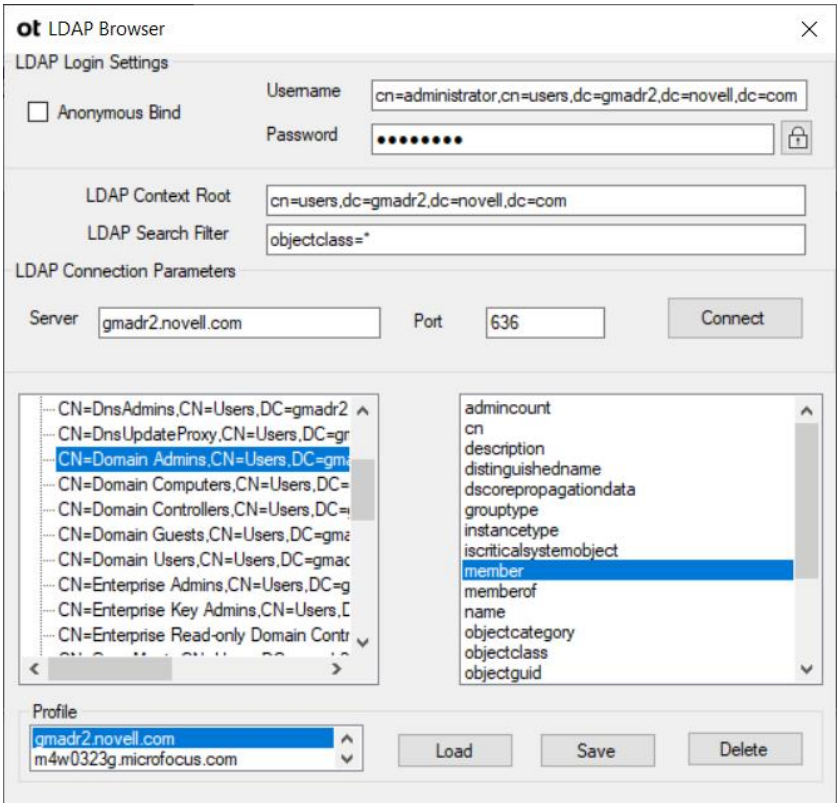
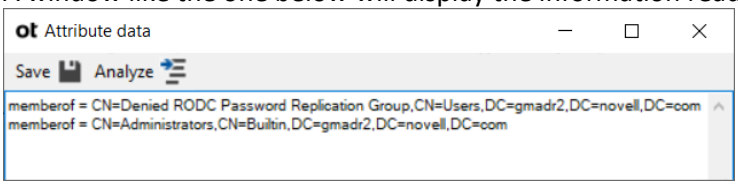


Figure 193 - Viewing LDAP attribute data

A window like the one below will display the information read from the attribute.



Building a list of LDAP users

Login to the LDAP server and set the search filter for objectclass=person. This will generate a list of all users in the specified LDAP context Root. Once the list of users is displayed then right click on any user object and select Export List. SLAnalyzer will then prompt to create a file in the log path directory (default of c:\nslfiles) with the name of LDAPExport.log.

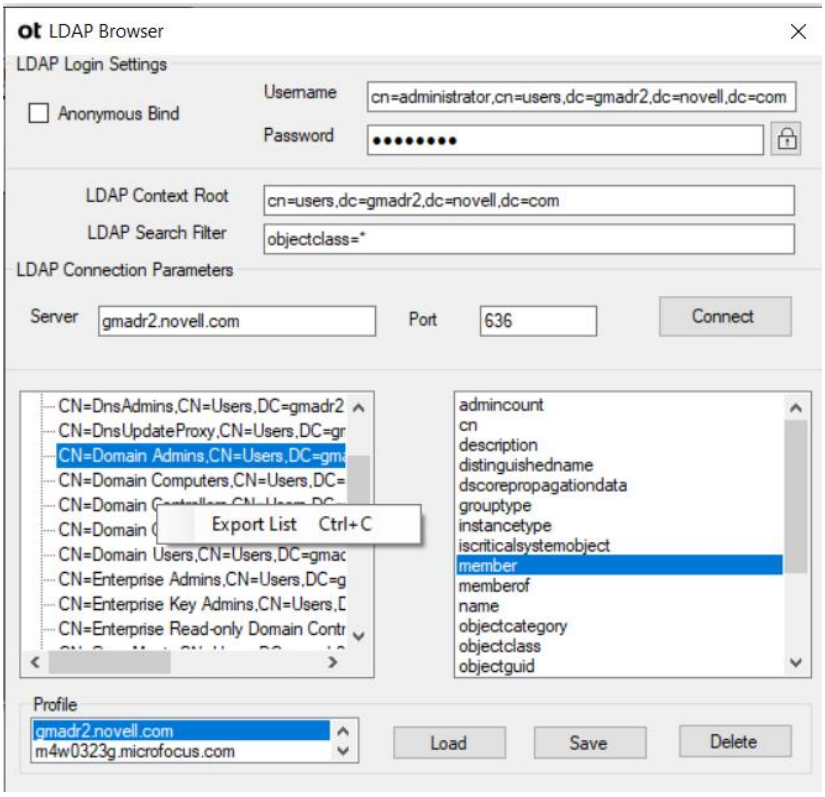


Figure 194 - LDAP users

(Sample content of c:\NSLFiles\LDAPExport.log)
cn=admin,o=novell
cn=clinical,o=novell
cn=dswain,o=novell
cn=gmorris,o=novell
cn=Greg,o=novell

LDAP Browser examples

Example 1:

The LDAP browser provides a view of the attributes that can be accessed with the currently defined user object that was used for the LDAP bind process.

In this example we first bind to eDirectory as a test user and view the attributes of the organization container object.

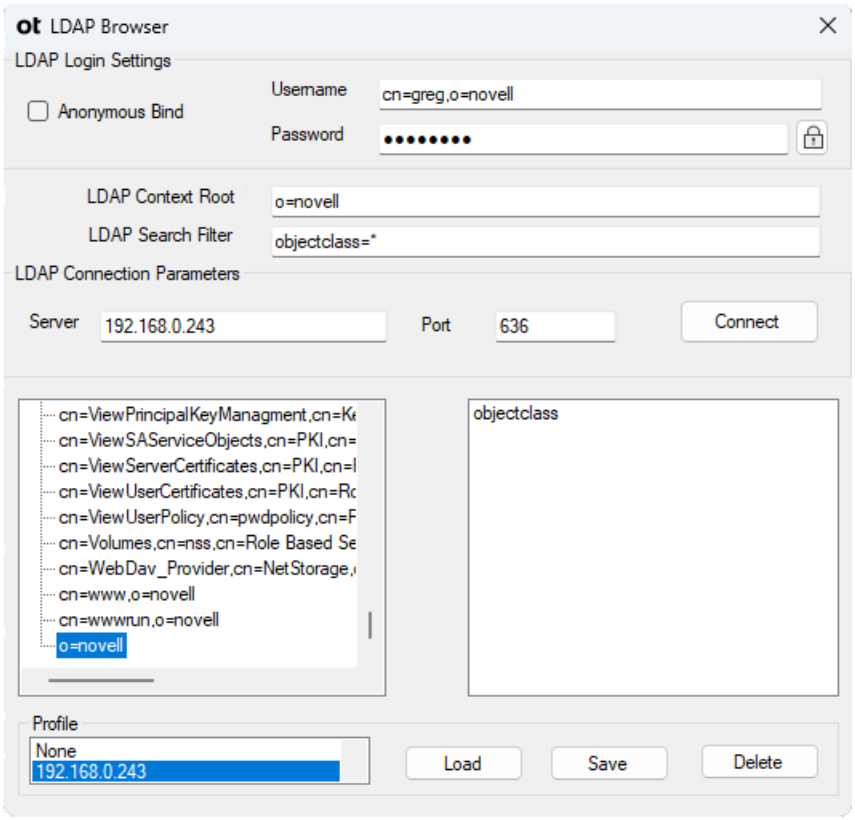


Figure 195 - LDAP browser login as test

We can see that the test user only has read access to 1 attribute

- objectclass

Now we bind to the LDAP server as the admin user.

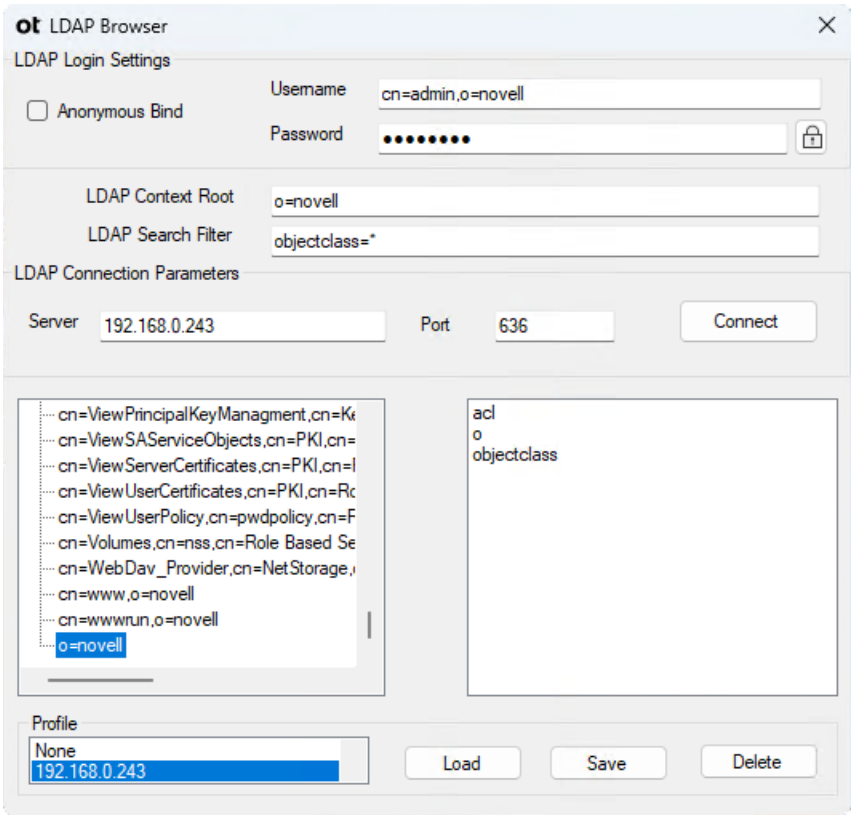


Figure 196 - LDAP browser logged in as admin

We now have read access to 3 different attributes.

- acl
- o
- objectclass

Example 2:

In this example we take one of the SSPR settings to validate the information that might be returned.

For the username we enter the SSPR proxy account
For the LDAP context we enter the root search
In the LDAP Search filter we copy in the search string being used by SSPR (activateUser.queryMatch).
(&(objectclass=person)(!(loginDisabled=TRUE))(!(loginTime=*)))

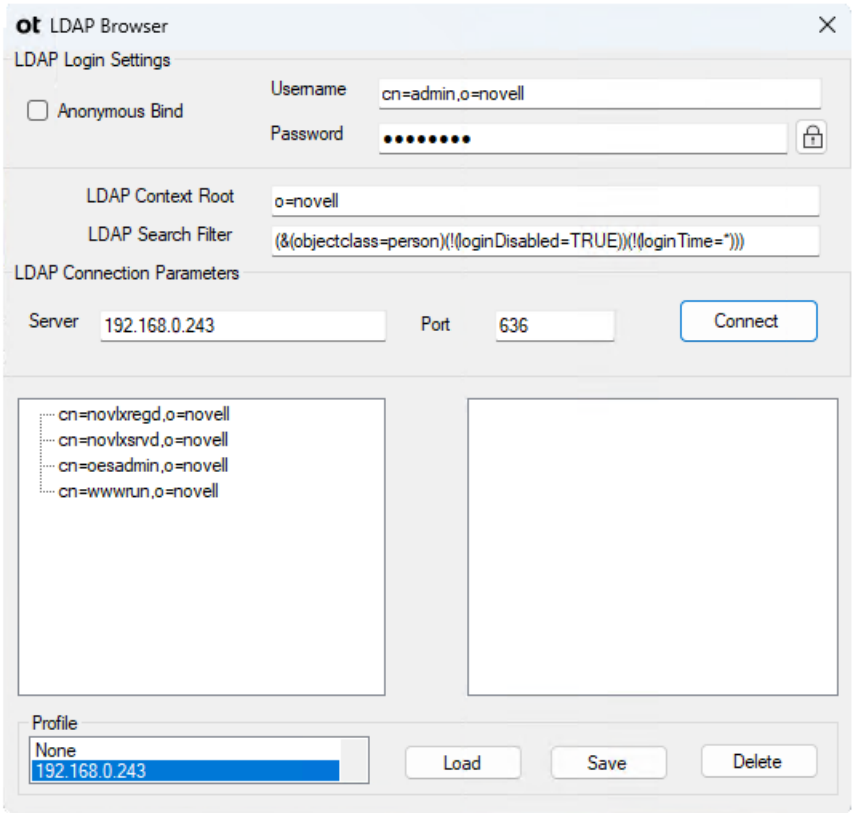


Figure 197 - LDAP Browser validate SSPR setting

JSON Console

The JSON console provides an interface where the user can paste in JSON formatted data and then view the content in a more readable fashion. Paste the JSON formatted data by pressing Ctrl-V on the keyboard in the top window or right click and select Paste. Then right click and select Process to display the JSON data in tree format or Clear to clear the data.

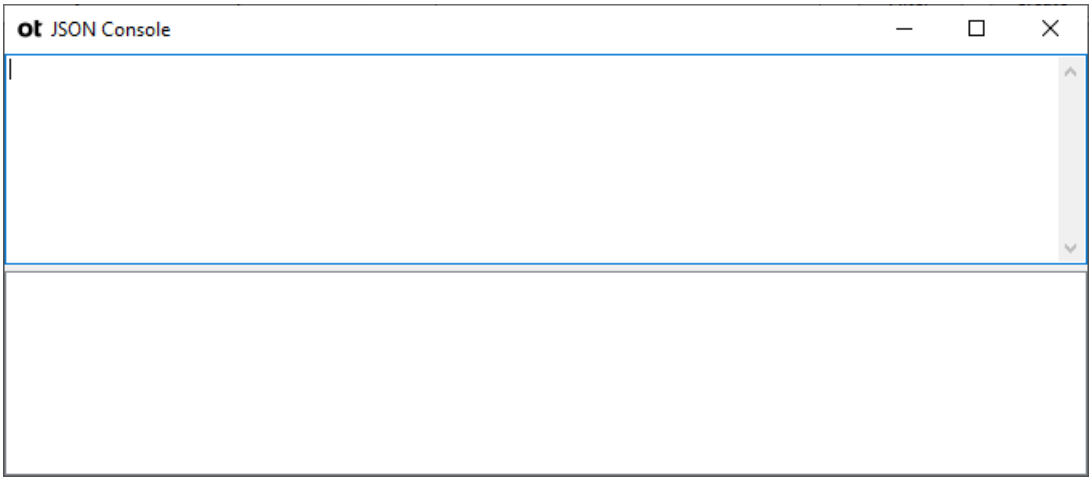


Figure 198 - JSON console window

The following example copies an item in an existing json file to the system copy/paste buffer. We can see that the item is not expandable. So we can copy this data to view more easily.

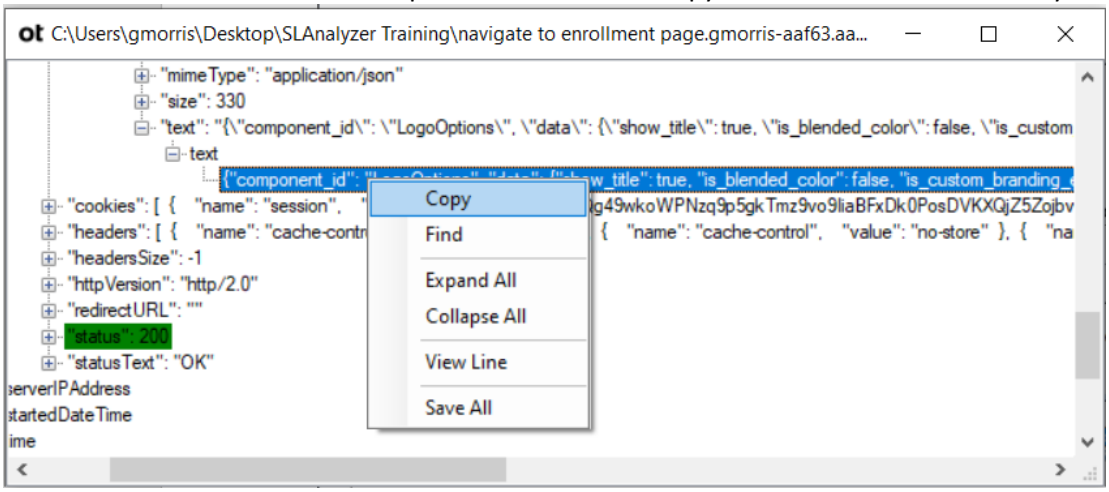


Figure 199 - Copy JSON data

Paste in the JSON data into the top window of the JSON Console by pressing Ctrl-V on the keyboard or right click and select paste. After the paste, right click and select Process to display the JSON data in a tree view.



Figure 200 - Process JSON data

SLAnalyzer will examine the JSON data and build a tree view of the information. The tree view will be displayed in the lower window.

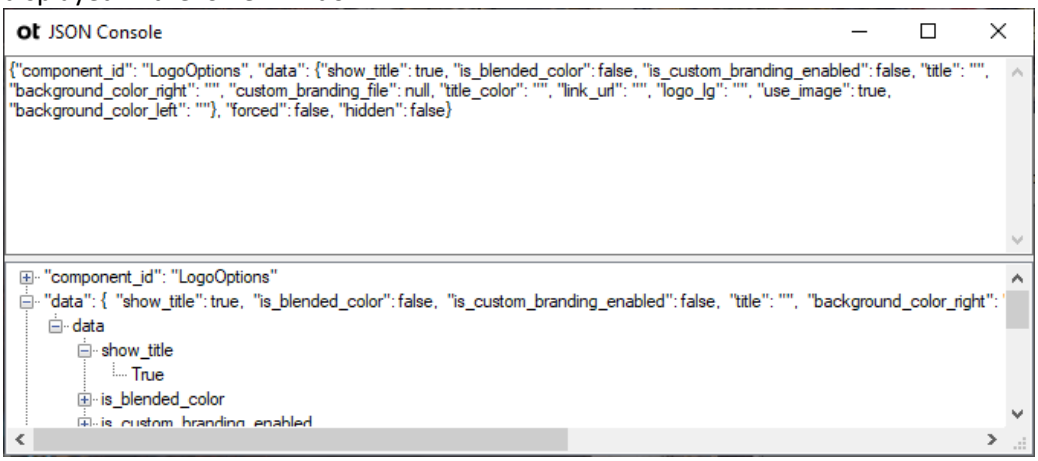


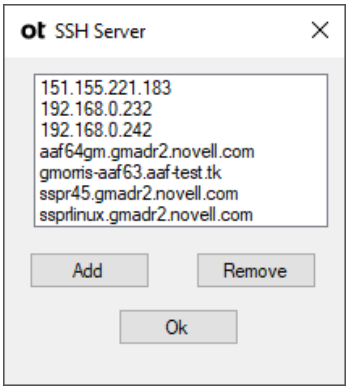
Figure 201 - JSON console window with data

The JSON console can be helpful when looking at the request and responses from the REST clients built into SLAnalyzer tools. You can copy any JSON data and paste it into the window to provide an easy view of the data. Note that you can also create a new text file with the content. Give the file the extension .json and then open with SLAnalyzer… See opening JSON files.

SSH/SCP

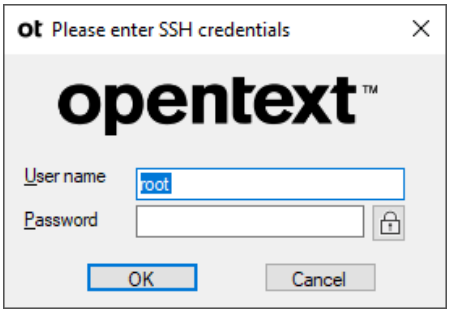
This option has 5 options

- Explorer – Similar to Windows explorer.
- Terminal – Basic SSH terminal. This is provided for quick access to the server via SSH.
- Download file – Uses SCP to download a file from the server to the local workstation.
- Upload file – Uses SCP to upload a file from the local workstation to the server
- Restart host – Will send a reboot command to the selected host.



When selecting an SSH/SCP function the user is first prompted for the destination host. Click Add to add a server not listed. Click remove to remove a saved server entry.

After selecting the server then SLAnalyzer will prompt the user for the login credentials for the session.



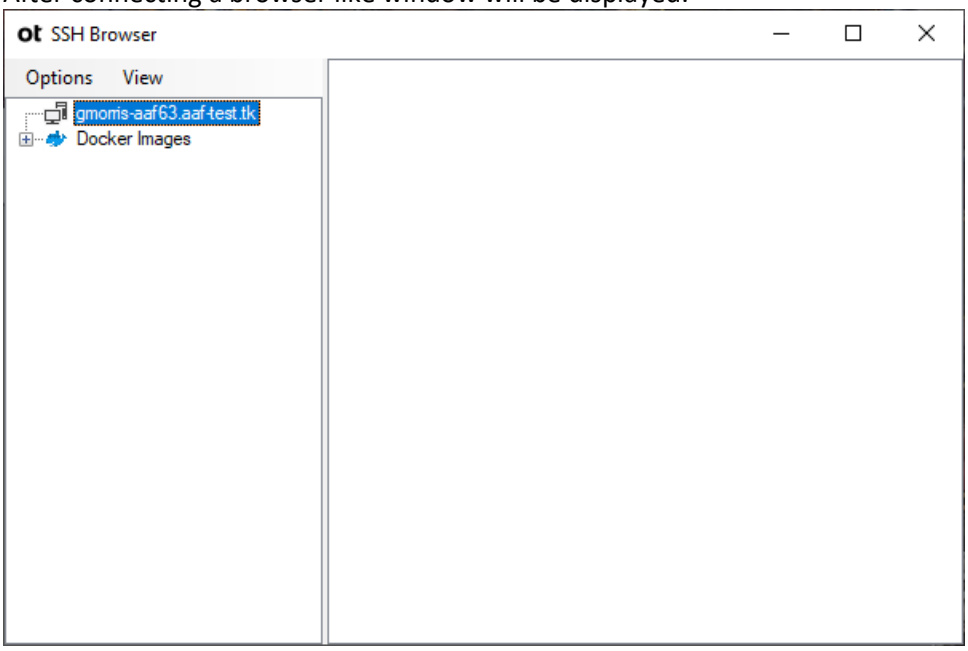
Once connected the appropriate menu item will be displayed.

Explorer

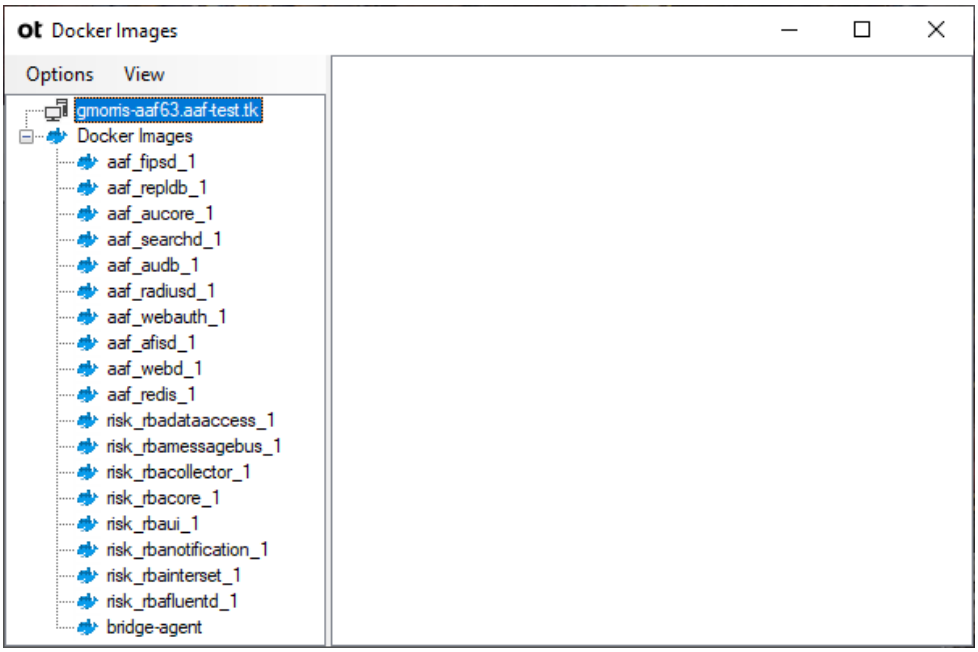
This browser is like the [Kubernetes Node explorer].

After selecting this option the user is prompted for the SSH information

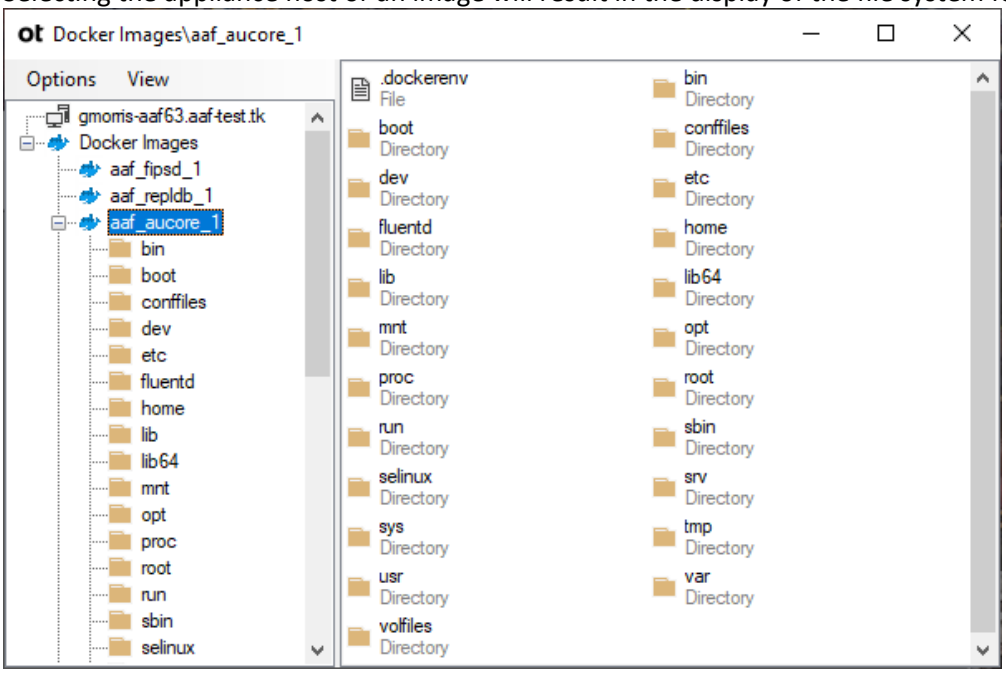
After connecting a browser like window will be displayed.



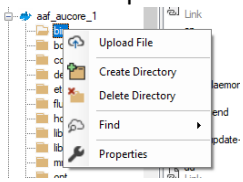
The left pane allows for navigation of the appliance file system and the docker images running on the host.



Selecting the appliance host or an image will result in the display of the file system for that object.



The left pane includes a number of features. Right clicking the mouse will display a menu with the available options.



Properties of the Linux host will display information about the server.

- DNS name
- OS information
- CPU information
- Block devices
- PCI information
- Network information
- Port information

Properties of Docker Images will display information about the docker service

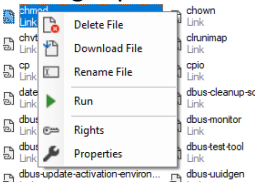
- Images found
- Image resource properties

Properties of a selected Docker image will display

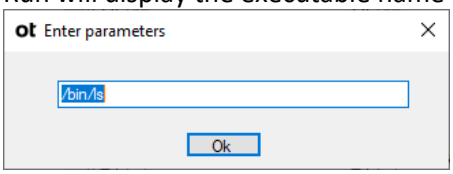
- Image details
- Container details
- Container statistics
- Container CPU usage

Properties of a directory will display information about the directory:

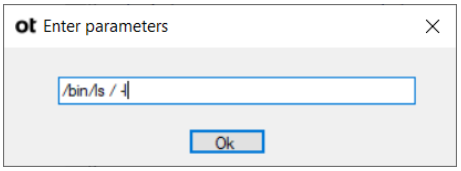
The right pane also has a number of features. Right click the mouse to display the context menu.



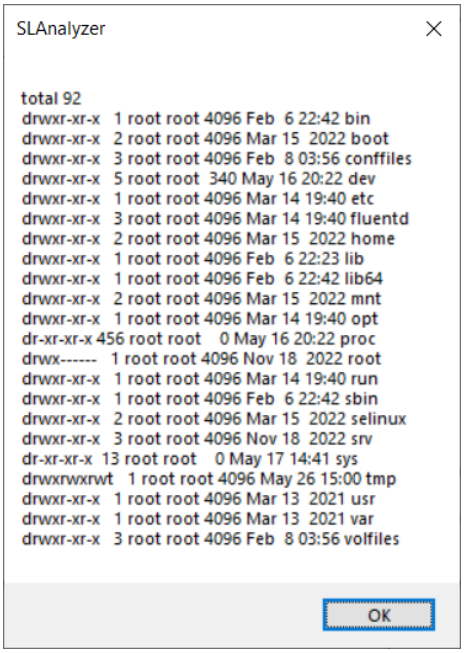
Run will display the executable name in a window where you can add additional parameters



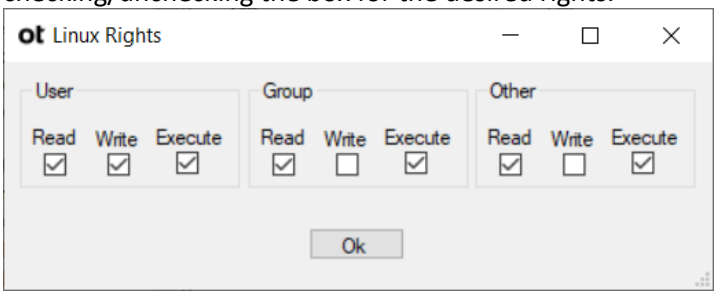
/bin/ls / -l



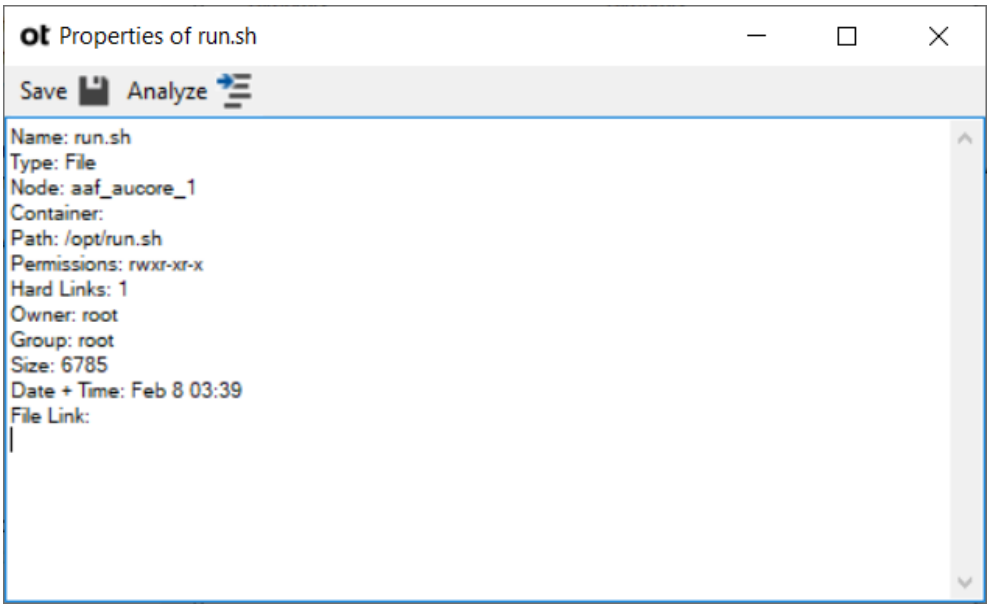
After the command is executed SLAnalyzer will display the results.



The rights option will display the current rights for the selected file and allow for modification by checking/unchecking the box for the desired rights.

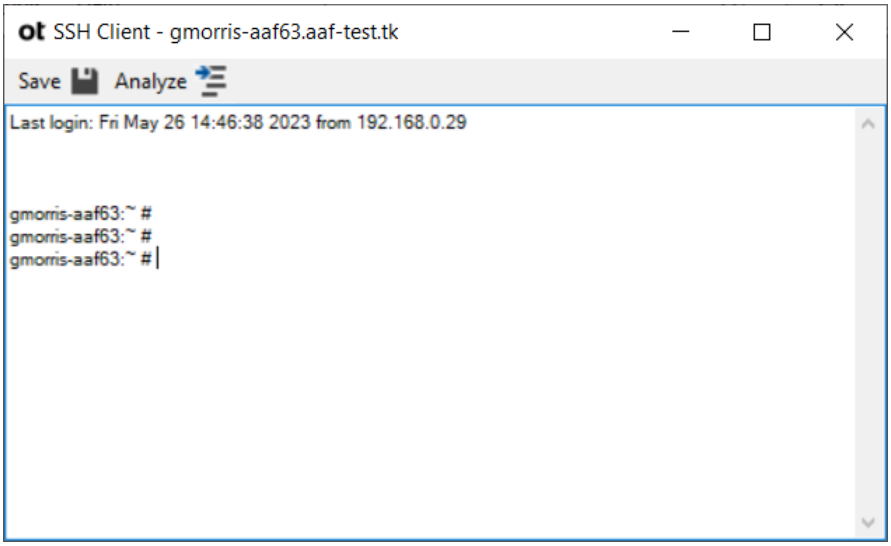


Properties will show the details on the selected file/folder.



SSH Terminal

The SSH terminal is a basic terminal used to access the host.



Type clear to clear the screen

Type exit to exit the terminal window

Download File

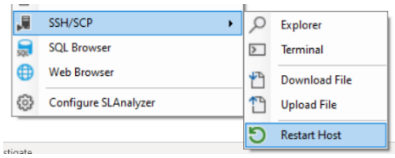
When selected SLAnalyzer will prompt the user for the full path of the file to download.

Upload File

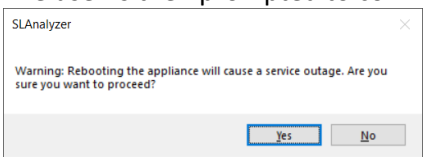
When selected SLAnlayzer will prompt the user to select the file to upload. It will then prompt the user to enter the full path for the destination.

Restart Host

This option will send a request to the SSH host to restart.



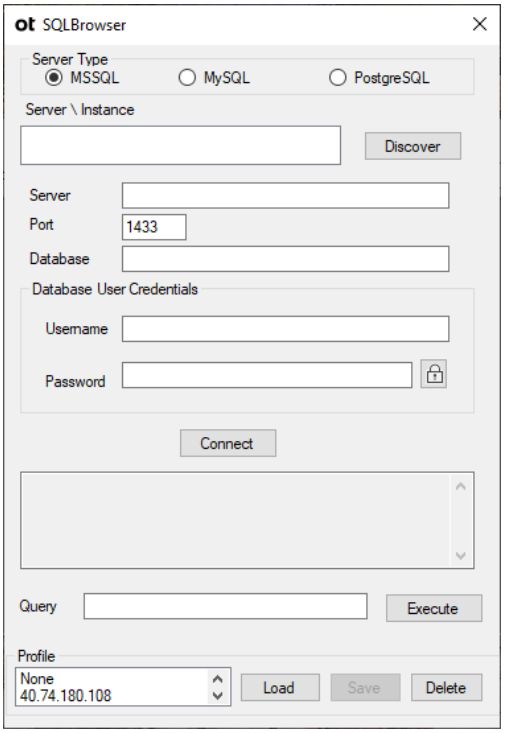
Like the other SSH options this process will prompt for the SSH connection information. The user is then prompted to confirm reboot.



After connection then /sbin/reboot is executed to restart the server.

SQL Browser

The SQL browser allows the testing of an SQL server connection. It also provides the ability to submit a query to an SQL database and display the query results.



The SQL Browser window has the following components:

- Server Type – MSSQL, MySQL, or PostgreSQL
- SQL server list
- Discover button
- Server
- Port
- Database
- Database User Credentials – Username
- Database User Credentials – Password
- Connect button
- Status box
- Query
- Execute button
- Profile data

Server Type

SLAnalyzer supports the following SQL server types:

- MSSQL – Microsoft SQL server
- MySQL
- PostgreSQL

SQL server list

This list is a listing of SQL servers found on the local network. The list is populated by clicking on the discover button. The server will be listed with the NETBIOS name of the server followed by the instance name. The instance name may or may not be displayed depending on the installation options and configuration of the SQL server.

Note that the order and number of servers listed here may vary depending on network traffic and server availability. This is only supported with MSSQL server type.

Discover button

The discover button attempts to find all SQL servers advertising on the local network. Servers existing beyond the local network will not be found.

Server

This field is populated by selecting one of the servers listed in the SQL server list. The user can also manually enter a server entry for an SQL server not listed in the server list.

Note that the server name must be resolvable via DNS to a valid IP address. If a connection problem is reported then open a cmd window and try to ping the server host name. For example if the name listed in the server list is “MySQLServer\MySQLInstance” then attempt to ping “MySQLServer” if this is not successful then change this to the IP address of the SQL server.
For example: 192.168.1.200\MySQLInstance

Port

By default the port for SQL is 1433. If the SQL server is listening on a different port then specify that here. You can verify the port by going to the SQL server and using the command netstat to see the ports that the SQL server is listening on.

Database

Specify the SQL database to connect/query against. Note that the database name and the instance name are not necessarily the same.

For example my server might be MySQLServer\MySQLInstance and my database name is SELFSERVICEDB.

Database User Credentials

Enter the credentials of the database user to connect with. By default SQL provides a user named sa that can be used for administration. This account might be disabled so verify with the appropriate SQL manager tools.

Username

Enter the SQL user name. This user must have read access to the specified database.

Password

Enter the password to the SQL user.

Connect button

Attempt to connect to the SQL server with the parameters specified. If the connection is successful then the status box will display the connection information.
See SQL connection example

Status box

The status box displays the information about the connection and the database tables found.

Query

The query box allows the database to be queried for information. Any valid SQL query is supported.
See SQL query examples

Execute button

The execute button submits the defined SQL query to the SQL server. A results window will display the information returned for the query. If the results window contains no entries then the query did not find any matches.

Profile data

Allows the storing and retrieving of configuration information of the SSPR Rights Validator window. For general information regarding the use of the profile options refer to the profile data section of the SSPR REST client section of this document. Data stored with this option will be saved to: HKEY_CURRENT_USER\Software\MicroFocus\SLAnalyzer\SQL.

MSSQL

This option supports the connection and queries to a Microsoft SQL server.

Connecting to an MSSQL database

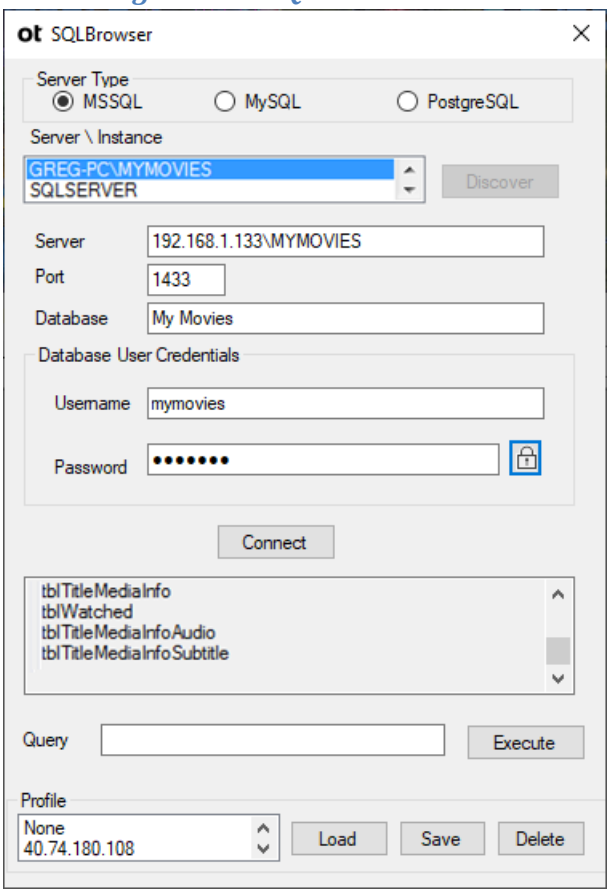


Figure 202 - Connect to SQL server with IP address

Server name of GREG-PC did not resolve to a valid IP address. So in the server field we had to change the name of the server to the actual IP address.

This SQL server is listening on the default port of 1433.
After clicking connect the status box shows:

Successfully connected to SQL server.
Connection string was: server=192.168.1.133\MYMOVIES;database=my movies; User Id=mymovies;
Server version: 09.00.5000
Connection state: Open

Tables:
tblCollectionChanges
tblTitles
tblEpisodeCountrySpecific
etc…

Connecting to an SSPR database on a non-standard port

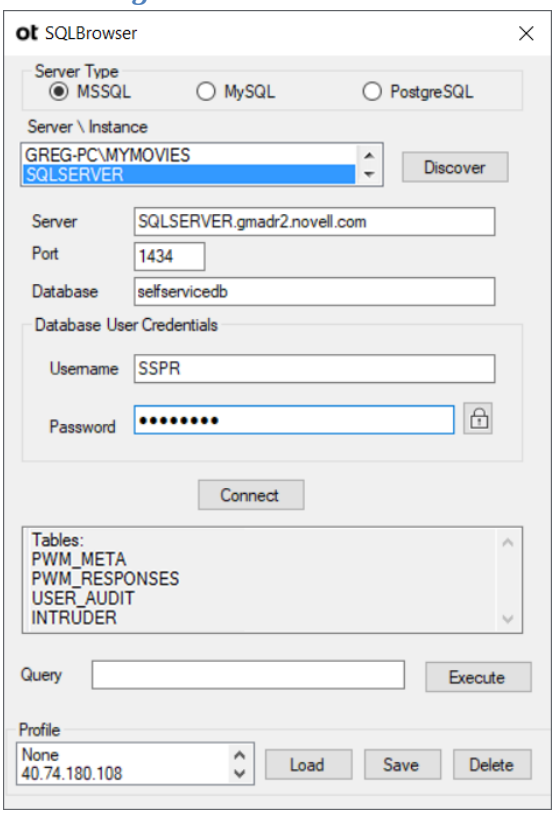


Figure 203 - Connect to SQL server with DNS name

The server name of SQLSERVER did not resolve to a valid IP address so the server field was edited to include the full DNS name of the object.

In this case the SQL server is configured to listen on port 1434

After clicking the connect button the following data is seen in the status box.

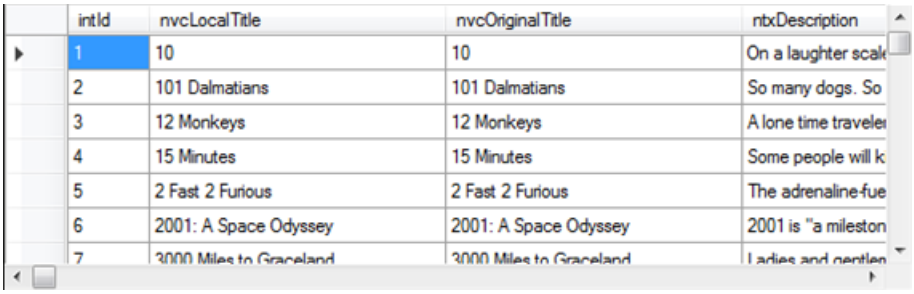
Successfully connected to SQL server.
Connection string was: server=SQLSERVER.gmadr2.novell.com,1434;database=selfservicedb; User Id=SSPR;
Server version: 11.00.5058
Connection state: Open

Tables:
PWM_META
PWM_RESPONSES
USER_AUDIT
INTRUDER
TOKENS
OTP

MSSQL query examples

Locate the table to query from the status box. Enter the desired query into the Query box and then click the Execute button to submit the query. The following are examples of different queries:

To return all columns and data.
Select * from tbltitles

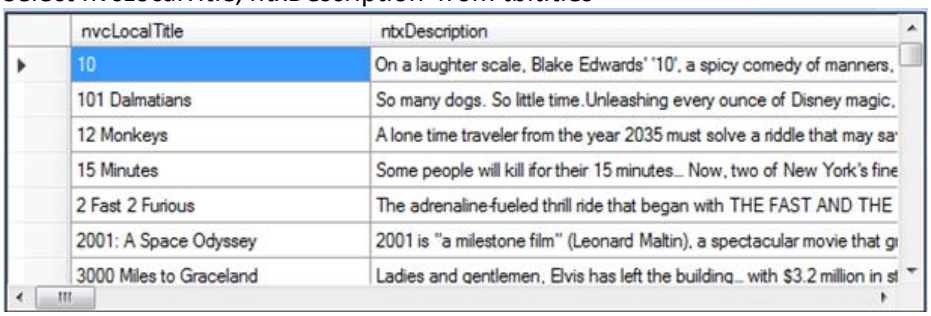


intId	nvcLocalTitle	nvcOriginalTitle	ntxDescription
1	10	10	On a laughter scal
2	101 Dalmatians	101 Dalmatians	So many dogs. So
3	12 Monkeys	12 Monkeys	A lone time travele
4	15 Minutes	15 Minutes	Some people will k
5	2 Fast 2 Furious	2 Fast 2 Furious	The adrenaline-fue
6	2001: A Space Odyssey	2001: A Space Odyssey	2001 is "a mileston
7	3000 Miles to Graceland	3000 Miles to Graceland	Ladies and gentlen

Figure 204 - Return all columns and records

To return only specific columns from the table. Then identify the column names with the previous search and then specify in your query.

Select nvcLocalTitle, ntxDescription from tbltitles



nvcLocalTitle	ntxDescription
10	On a laughter scale, Blake Edwards' '10', a spicy comedy of manners,
101 Dalmatians	So many dogs. So little time.Unleashing every ounce of Disney magic,
12 Monkeys	A lone time traveler from the year 2035 must solve a riddle that may sa
15 Minutes	Some people will kill for their 15 minutes... Now, two of New York's fine
2 Fast 2 Furious	The adrenaline-fueled thrill ride that began with THE FAST AND THE
2001: A Space Odyssey	2001 is "a milestone film" (Leonard Maltin), a spectacular movie that g
3000 Miles to Graceland	Ladies and gentlemen, Elvis has left the building... with $3.2 million in st

Figure 205 - Return specific columns for all records

To return all columns but only for records matching a specific value:
Select * from tblTitles where nvclocaltitle = 'Against the ropes'

intId	nvcLocalTitle	nvcOriginalTitle	ntxDescription
18	Against the Ropes	Against the Ropes	Jackie Kallen isn't fighting for glory. She's fighting for respec

Figure 206 - Return all columns when record equals value

To return all columns matching only the records containing a specific value:
Select * from tblTitles where nvclocaltitle like '%the%'

intId	nvcLocalTitle	nvcOriginalTitle	ntxDescription
17	The Adventures of Rocky & Bullwinkle	The Adventures of Rocky & Bullwinkle	Everyone's favorite r
18	Against the Ropes	Against the Ropes	Jackie Kallen isn't fig
28	America's Sweethearts	America's Sweethearts	A comedy about cele
32	The Aviator	The Aviator	One of the 20th cent
35	The Banger Sisters	The Banger Sisters	Goldie Hawn and Su
38	Saturday Night Live - The Best of Mike Myers	Saturday Night Live - The Best of Mike Myers	Mike is a genius a

Figure 207 - Return all columns when record contains specified data

More SLQ query examples can be found at:
https://technet.microsoft.com/en-us/library/bb264565(v=sql.90).aspx

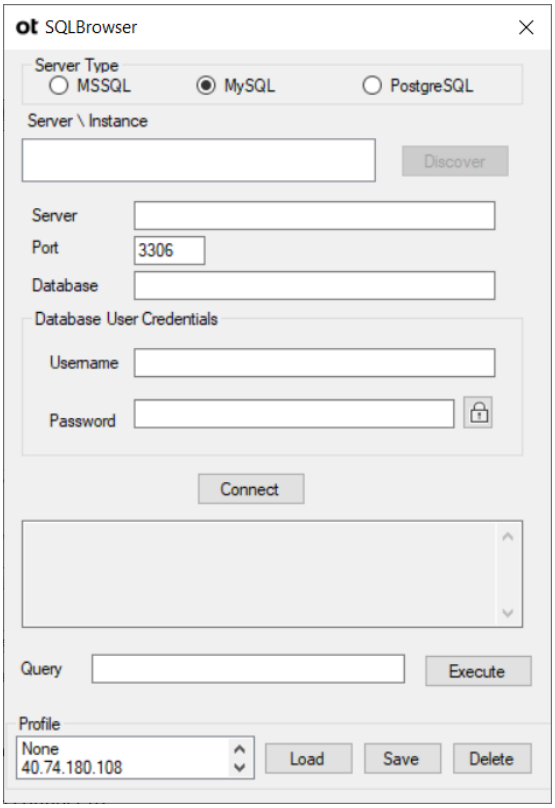
MySQL

This option supports the connection and queries to a MySQL server.

Connecting to a MySQL server

Within SLAnalyzer click on Tools -> SQL Browser

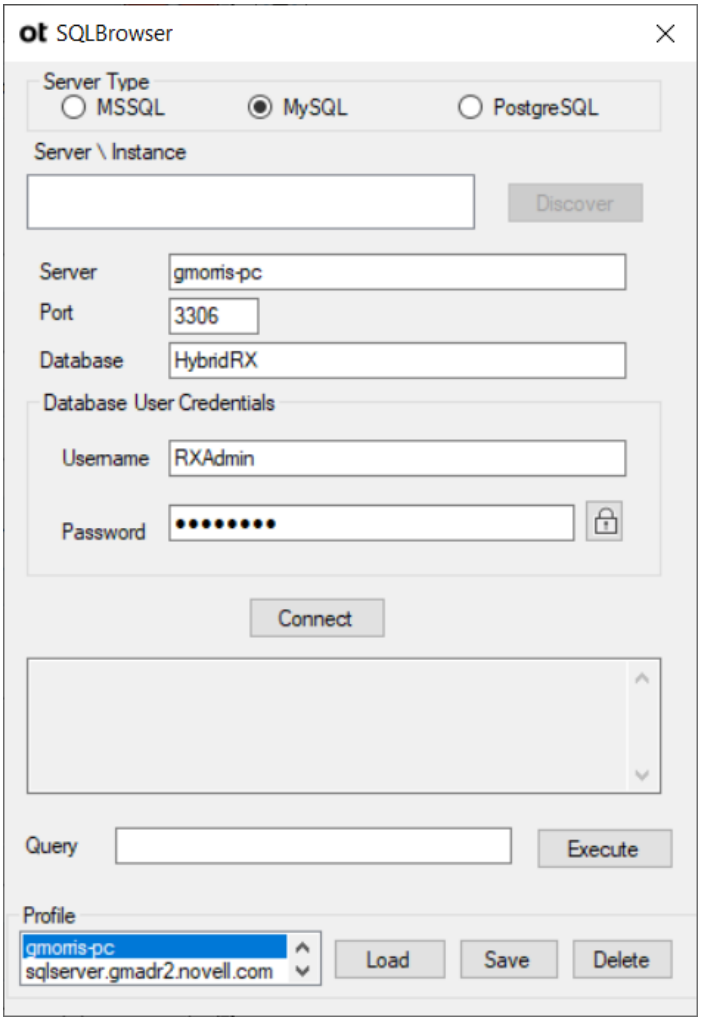
Click on MySQL radio button



Enter the following:

- MySQL server name. This can be the DNS name or IP address of the MySQL server.
- Modify the port if necessary. The default port of 3306 is prepopulated.
- Database. Name of the database to connect to.
- Database User Credentials
    - Username – Database User name
    - Password – Password of the Database User

Click the Connect button to perform a connection attempt to the MySQL server.



Successfully connected to SQL server.

Connection string was: server=gmorris-pc;port=3306;database=HybridRX;user id=RXAdmin;pooling=False

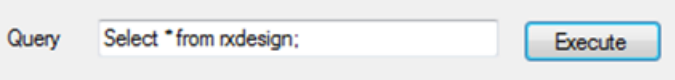
Server version: 8.0.12
Connection state: Open

Tables:
rxcat
rxcustomer
rxdesign
etc.

MySQL Query example

You can display information or even edit the database by sending MySQL statements to the SQL server. Enter the command into the Query field and then click the Execute button to send the statement to the server. If data is returned then SLAnalyzer will display the information. See https://dev.mysql.com/doc/refman/8.0/en/sql-syntax.html

Example of Select * from rxdesign command:



Data returned by command:

	Name	location	rows	columns	type
▶	Debbie	19, 33	50	50	0
	Greg	9, 149	50	50	1
	Scott	8, 271	50	50	2

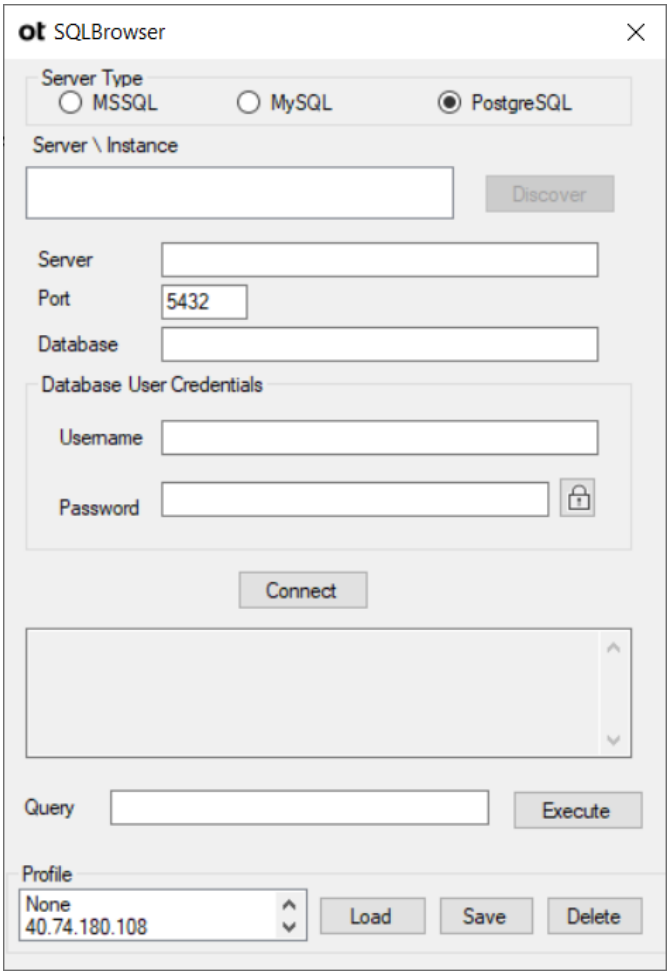
PostgreSQL

This option supports the connection and commands to a PostgreSQL server.

Connecting to a PostgreSQL server

Within SLAnalyzer click on Tools -> SQL Browser

Click on PostgreSQL radio button



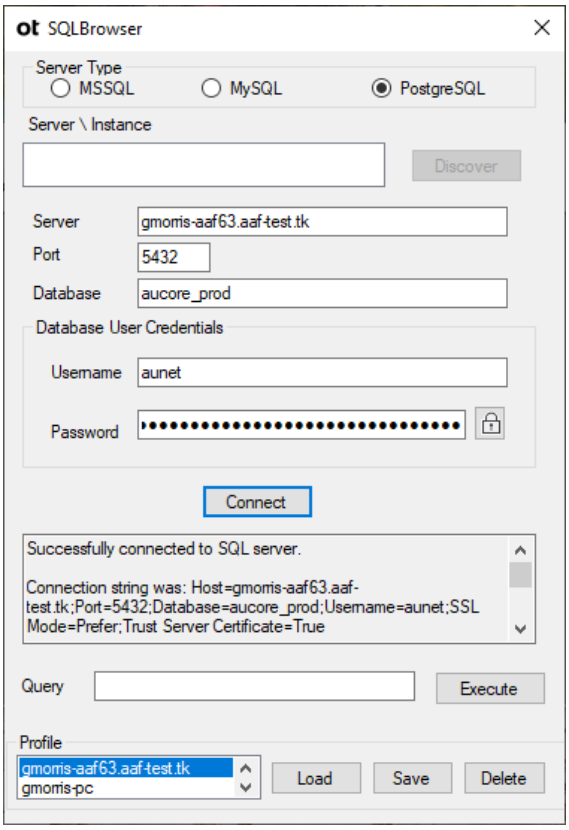
Note that the Port field is automatically set to a value of 5432. In this example we will be connecting to an Advanced Authentication Framework server. The AAF server uses the default PostgreSQL database port of 5432. For other server types you may need to validate the proper port if 5432 doesn't seem to respond properly.

In the Server field type in the IP address or the DNS name of the AAF server.

In the Database field type in the name of the PostgreSQL database to connect to. For an AAF server, the PostgreSQL database name is aucore_prod.

In the Database User Credentials type in the Username of the database user and their password. For an AAF server, the user aunet is defined for remote access.

If connecting to an AAF (Advanced Authentication Framework) server, then you can obtain the aunet user password by performing the steps outlined in this section (Steps to obtain PostgreSQL database user on AAF server).



Click the connect button

Immediately below the connect button is a status window. In this box you will see the connection details.

///

Successfully connected to SQL server.
Connection string was: Host=naaf60.gmadr2.novell.com;Port=5432;Database=aucore_prod;Username=aunet;SSL Mode=Prefer;Trust Server Certificate=True
Server version: 10.3
Connection state: Open
SQL Server Database(s):

Postgres
aucore_prod

aucore_prod Table(s):

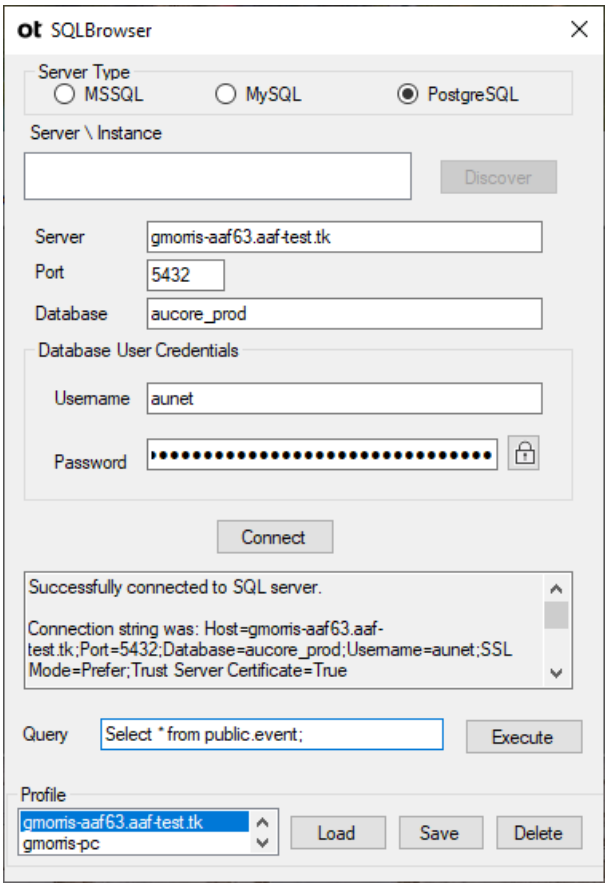
public	**alembic_version**
public	**user__auth_template**
public	**role__role**
public	**user__role**
public	**logon_chain__role**
public	**role**
public	**group__role**
public	**logon_chain__group**
public	**event_logon_chain**
public	**endpoint_session**
public	**grp**
public	**chain_image**
public	**event_endpoint**
public	**adfs_state**
public	**last_logon**
public	**server_pulse**
public	**spatial_ref_sys**
public	**geo_event_zone_links**
public	**geo_polygon**
public	**geo_zone_polygon_links**
public	**session_cookie**
public	**logon_process**
public	**enroll_process**
public	**smartphone_state**
public	**auth_t_smartphone_push_id**
public	**license**
public	**otp_token**
public	**adfs_partner**
public	**u2f_attestation_cert**
public	**geo_zone**
public	**local_user**
public	**pki_trusted_cert**
public	**category**
public	**repository**
public	**repo_site_cfg**
public	**server**
public	**logon_session**
public	**device**
public	**dashboard**
public	**policy**
public	**event**
public	**auth_template**
public	**custom_messages**
public	**endpoint**
public	**logon_chain**
public	**tenant**
public	**oob_logon_process**
public	**oob_secret**
public	**report**
public	**user**
public	**report_export**

///

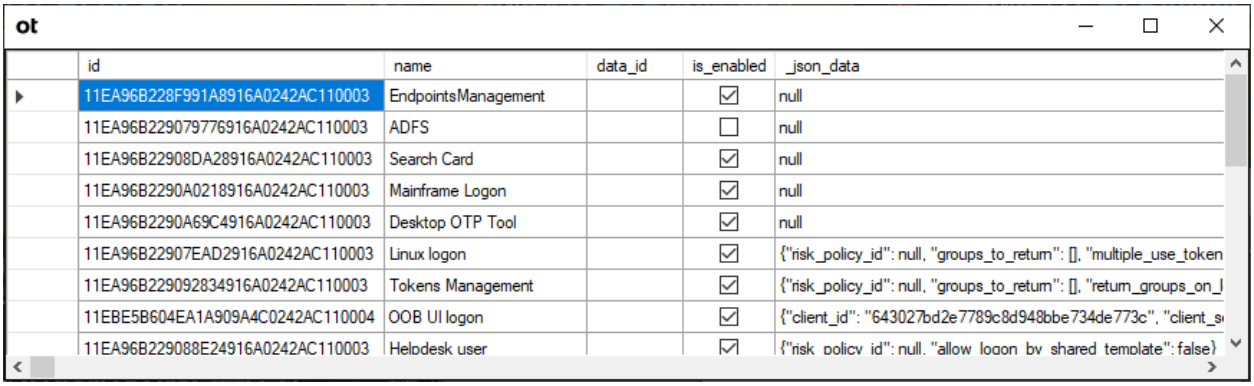
PostgreSQL command examples

Once a connection can be made to the server, you can submit any valid PostgreSQL command via the Query field.

Type “Select * from public.event;“ without the quotes into the Query box.



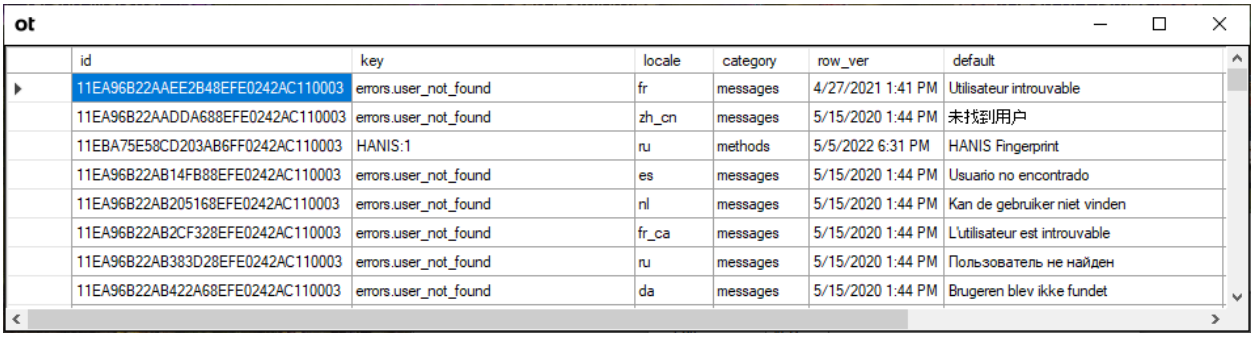
SLAnalyzer will now display a window with the query results.



	id	name	data_id	is_enabled	_json_data
▶	11EA96B228F991A8916A0242AC110003	EndpointsManagement		☑	null
	11EA96B229079776916A0242AC110003	ADFS		☐	null
	11EA96B22908DA28916A0242AC110003	Search Card		☑	null
	11EA96B2290A0218916A0242AC110003	Mainframe Logon		☑	null
	11EA96B2290A69C4916A0242AC110003	Desktop OTP Tool		☑	null
	11EA96B22907EAD2916A0242AC110003	Linux logon		☑	{"risk_policy_id": null, "groups_to_return": [], "multiple_use_token
	11EA96B229092834916A0242AC110003	Tokens Management		☑	{"risk_policy_id": null, "groups_to_return": [], "return_groups_on_l
	11EBE5B604EA1A909A4C0242AC110004	OOB UI logon		☑	{"client_id": "643027bd2e7789c8d948bbe734de773c", "client_s
	11EA96B229088E24916A0242AC110003	Helpdesk user		☑	{"risk_policy_id": null, "allow_logon_by_shared_template": false}

In this example we can view the custom messages returned by the AAF server.

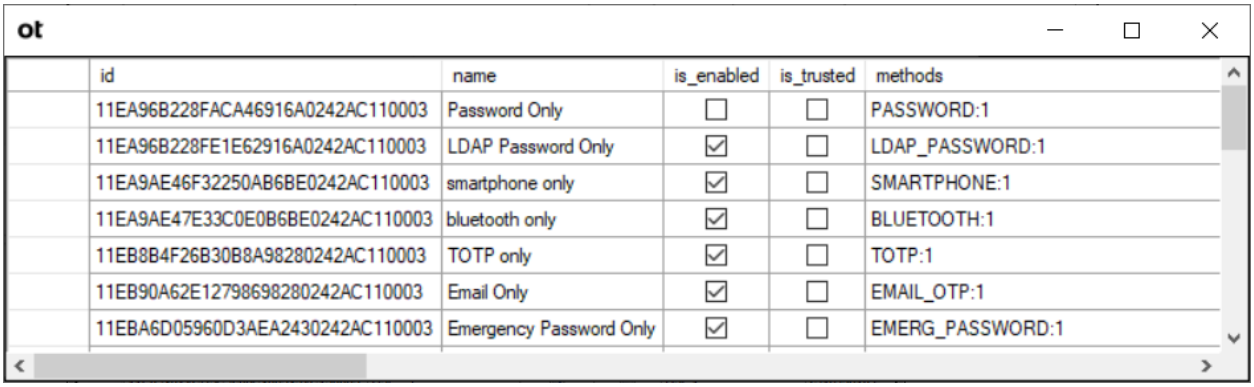
Select * from public.custom_messages;



id	key	locale	category	row_ver	default
11EA96B22AAEE2B48EFE0242AC110003	errors.user_not_found	fr	messages	4/27/2021 1:41 PM	Utilisateur introuvable
11EA96B22AADDA688EFE0242AC110003	errors.user_not_found	zh_cn	messages	5/15/2020 1:44 PM	未找到用户
11EBA75E58CD203AB6FF0242AC110003	HANIS:1	ru	methods	5/5/2022 6:31 PM	HANIS Fingerprint
11EA96B22AB14FB88EFE0242AC110003	errors.user_not_found	es	messages	5/15/2020 1:44 PM	Usuario no encontrado
11EA96B22AB205168EFE0242AC110003	errors.user_not_found	nl	messages	5/15/2020 1:44 PM	Kan de gebruiker niet vinden
11EA96B22AB2CF328EFE0242AC110003	errors.user_not_found	fr_ca	messages	5/15/2020 1:44 PM	L'utilisateur est introuvable
11EA96B22AB383D28EFE0242AC110003	errors.user_not_found	ru	messages	5/15/2020 1:44 PM	Пользователь не найден
11EA96B22AB422A68EFE0242AC110003	errors.user_not_found	da	messages	5/15/2020 1:44 PM	Brugeren blev ikke fundet

Updating a record in the PostgreSQL table. (See warning at the end of this section)

Select * from public.logon_chain;

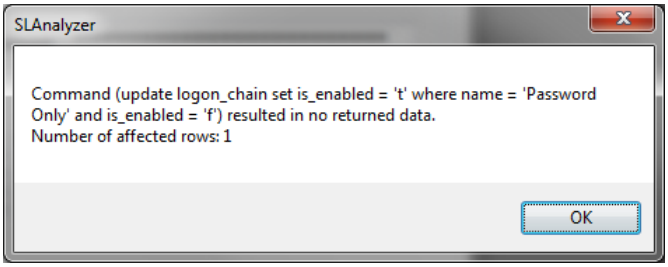


id	name	is_enabled	is_trusted	methods
11EA96B228FACA46916A0242AC110003	Password Only	☐	☐	PASSWORD:1
11EA96B228FE1E62916A0242AC110003	LDAP Password Only	☑	☐	LDAP_PASSWORD:1
11EA9AE46F32250AB6BE0242AC110003	smartphone only	☑	☐	SMARTPHONE:1
11EA9AE47E33C0E0B6BE0242AC110003	bluetooth only	☑	☐	BLUETOOTH:1
11EB8B4F26B30B8A98280242AC110003	TOTP only	☑	☐	TOTP:1
11EB90A62E12798698280242AC110003	Email Only	☑	☐	EMAIL_OTP:1
11EBA6D05960D3AEA2430242AC110003	Emergency Password Only	☑	☐	EMERG_PASSWORD:1

Find the Password Only logon chain and set it to enabled if it is disabled.

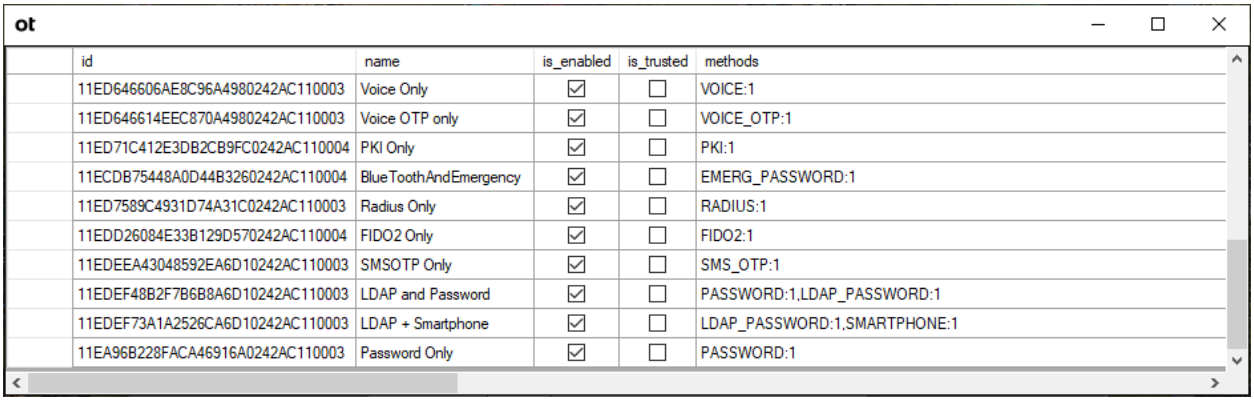
update public.logon_chain set is_enabled = 't' where name = 'Password Only' and is_enabled = 'f';

After clicking the Execute button SLAnalyzer will report the number of affected rows. If this value is 0 then nothing was changed in the database.



Now to see the changed record we need to perform our Select query again.

Select * from public.logon_chain;


ot

id	name	is_enabled	is_trusted	methods
11ED646606AE8C96A4980242AC110003	Voice Only	☑	☐	VOICE:1
11ED646614EEC870A4980242AC110003	Voice OTP only	☑	☐	VOICE_OTP:1
11ED71C412E3DB2CB9FC0242AC110004	PKI Only	☑	☐	PKI:1
11ECDB75448A0D44B3260242AC110004	BlueToothAndEmergency	☑	☐	EMERG_PASSWORD:1
11ED7589C4931D74A31C0242AC110003	Radius Only	☑	☐	RADIUS:1
11EDD26084E33B129D570242AC110004	FIDO2 Only	☑	☐	FIDO2:1
11EDEEA43048592EA6D10242AC110003	SMSOTP Only	☑	☐	SMS_OTP:1
11EDEF48B2F7B6B8A6D10242AC110003	LDAP and Password	☑	☐	PASSWORD:1,LDAP_PASSWORD:1
11EDEF73A1A2526CA6D10242AC110003	LDAP + Smartphone	☑	☐	LDAP_PASSWORD:1,SMARTPHONE:1
11EA96B228FACA46916A0242AC110003	Password Only	☑	☐	PASSWORD:1

Note: Some fields in the list have been converted to Hex strings for visibility. For example the id field in the above example is actually a byte array and not a simple string. Attempting to modify or perform a query against that field would result in a failure. For example if our update command included the statement Where id=' 11E873FFF939B046B5CA0242AC120002' then SLAnalyzer would report that 0 rows were affected. See the next section which documents how to handle byte array data types. (**Handling** Bytea (Byte Array) **fields**)

Warning:

It is strongly recommended that you don't modify any database directly with this tool. It is meant as a method of viewing the database not changing the database. Making modifications to any database is at your own risk. Before you make any changes, it would be a good idea to have a valid backup in case you need to revert the changes.

For more information on valid commands and syntax please refer to the PostgreSQL documentation: https://www.postgresql.org/docs/10/sql-commands.html

Handling Bytea (Byte Array) fields.

The AAF id fields are defined in the PostgreSQL table as type bytea. For this reason they cannot be handled the same as other field types. SLAnalyzer automatically converts these values in the table to a hex string for easy viewing. But to modify or use this type of field in a command you must tell the PostgreSQL server how to handle the data format.

You can use either the displayed hex value or an escaped value for the id fields. The syntax is different depending on the type of data represented in the command.

For example

Hex value:

11E873FFFB053DA0B5540242AC120002

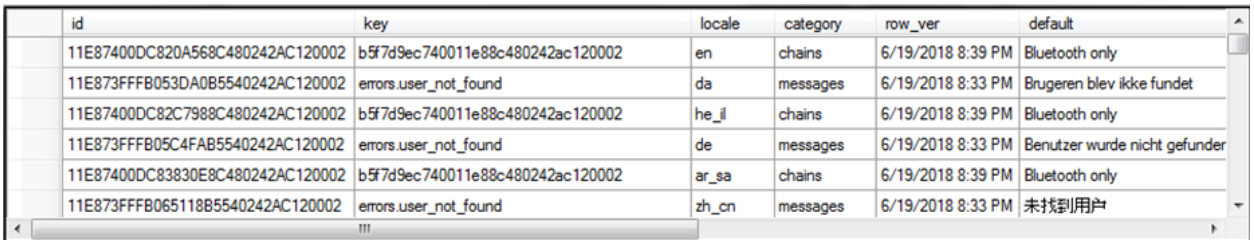
Escape value:

◀\350s\377\373|=\240\265T┐B\254↕\000┐

Using Hex value

First let's look at using the displayed Hex value.

If we type Select * from public.custom_messages; into the query window and then click the execute button we see.

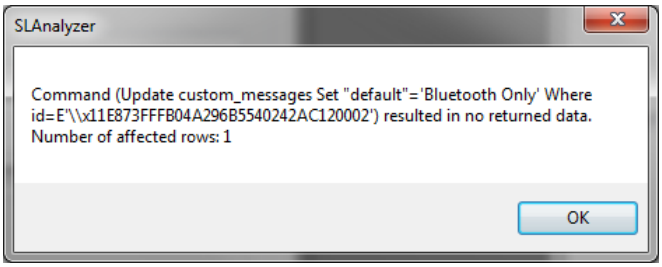


id	key	locale	category	row_ver	default
11E87400DC820A568C480242AC120002	b5f7d9ec740011e88c480242ac120002	en	chains	6/19/2018 8:39 PM	Bluetooth only
11E873FFFB053DA0B5540242AC120002	errors.user_not_found	da	messages	6/19/2018 8:33 PM	Brugeren blev ikke fundet
11E87400DC82C7988C480242AC120002	b5f7d9ec740011e88c480242ac120002	he_il	chains	6/19/2018 8:39 PM	Bluetooth only
11E873FFFB05C4FAB5540242AC120002	errors.user_not_found	de	messages	6/19/2018 8:33 PM	Benutzer wurde nicht gefunden
11E87400DC83830E8C480242AC120002	b5f7d9ec740011e88c480242ac120002	ar_sa	chains	6/19/2018 8:39 PM	Bluetooth only
11E873FFFB065118B5540242AC120002	errors.user_not_found	zh_cn	messages	6/19/2018 8:33 PM	未找到用户

To instruct the server that the value being passed for the id field is hex then we need to include the following: E'\\x<hex value of the id>';

Replace the text <hex value of the id> with the actual value of the id field seen in the select data.

```
Update public.custom_messages Set "default"='Bluetooth Only' Where
id=E'\\x11E873FFFB04A296B5540242AC120002';
```



We can also pass the id field in our Select query:

Select * from public.custom_messages where id=E'\\x11E873FFFB04A296B5540242AC120002';

id	key	locale	category	row_ver	default	message
11E873FFFB04A296B5540242AC120002	errors.user_not_found	zh_tw	messages	6/19/2018 8:33 PM	Bluetooth Only	

Using the escaped value

Since SLAnalyzer doesn't show the escaped value by default we can modify our select command to tell the server to return the escaped value.

Add the encode parameter to instruct the PostgreSQL server how to handle this datatype.

Include the encode(field_to_encode, 'escape') as fieldname_to_use

Select *, encode(id, 'escape') as id from public.custom_messages;

	default	message	tenant_id	id1
8 8:33 PM	User is not found		DEF0DEF0DEF0DEF0DEF0DEF0DEF0DEF0	\350s\377\372\374fb\265T┐B\254I\000┐
8 8:33 PM	משתמש לא נמצא		DEF0DEF0DEF0DEF0DEF0DEF0DEF0DEF0	\350s\377\372\375\210\265T┐B\254I\000┐
8 8:33 PM	لم يتم العثور على المستخدم		DEF0DEF0DEF0DEF0DEF0DEF0DEF0DEF0	\350s\377\372\376\207\370\265T┐B\254I\000┐
8 8:33 PM	Nie znaleziono użytkownika		DEF0DEF0DEF0DEF0DEF0DEF0DEF0DEF0	\350s\377\372\377aF\265T┐B\254I\000┐
8 8:33 PM	ユーザが見つかりません		DEF0DEF0DEF0DEF0DEF0DEF0DEF0DEF0	\350s\377\373\000<\222\265T┐B\254I\000┐
8 8:33 PM	L'utilisateur est introuvable		DEF0DEF0DEF0DEF0DEF0DEF0DEF0DEF0	\350s\377\373\000\375\370\265T┐B\254I\000┐

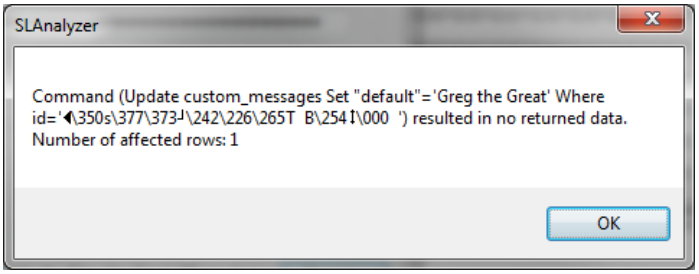
A new column is added at the end of the column data that contains the escaped value of the id. Since there was already a column called id then the new column called id1. You can use this value to perform an update of the selected message with this id.

Copy the id1 value for the message you want to change.

Update public.custom_messages Set "default"='Greg the Great' Where id='data_copied';

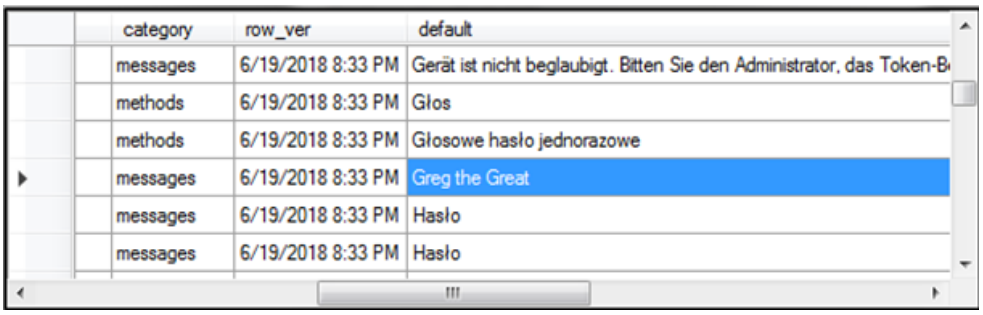
Replace the text data_copied with the id1 value copied from the previous select query.

After clicking the Execute button SLAnalyzer will display the following message. Note the query…



Now if we issue the Select query again we will see that the text for the message now reads as “Greg the Great”.

Select *, encode(id, 'escape') as id from public.custom_messages;

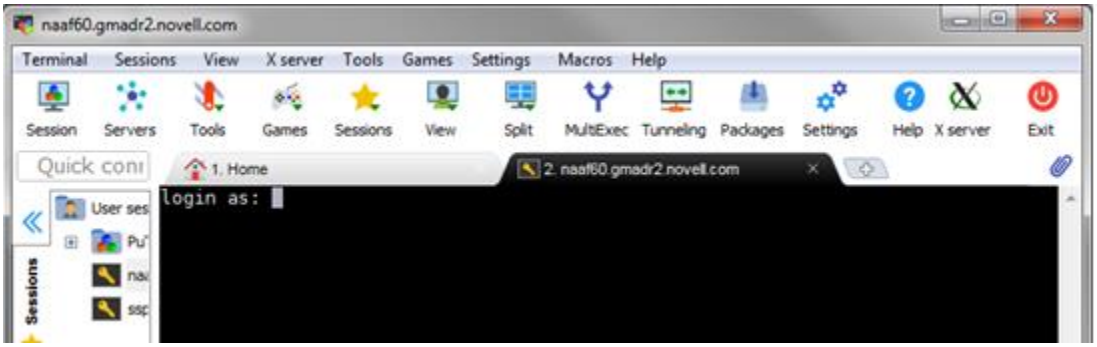


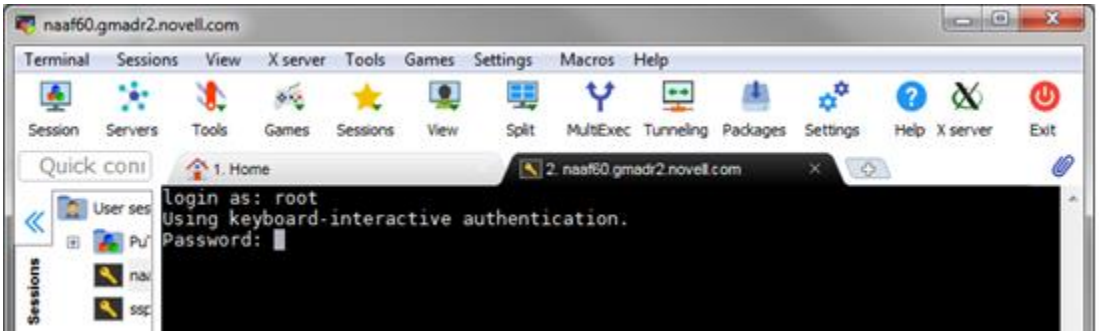
category	row_ver	default
messages	6/19/2018 8:33 PM	Gerät ist nicht beglaubigt. Bitten Sie den Administrator, das Token-B
methods	6/19/2018 8:33 PM	Głos
methods	6/19/2018 8:33 PM	Głosowe hasło jednorazowe
messages	6/19/2018 8:33 PM	Greg the Great
messages	6/19/2018 8:33 PM	Hasło
messages	6/19/2018 8:33 PM	Hasło

Steps to obtain PostgreSQL database user on AAF server

Follow the next steps to identify the password for the PostgreSQL aunet remote user. Note that you can obtain this same information from SLAnalyzer – Tools->Advanced Authentication->Find Postgres User

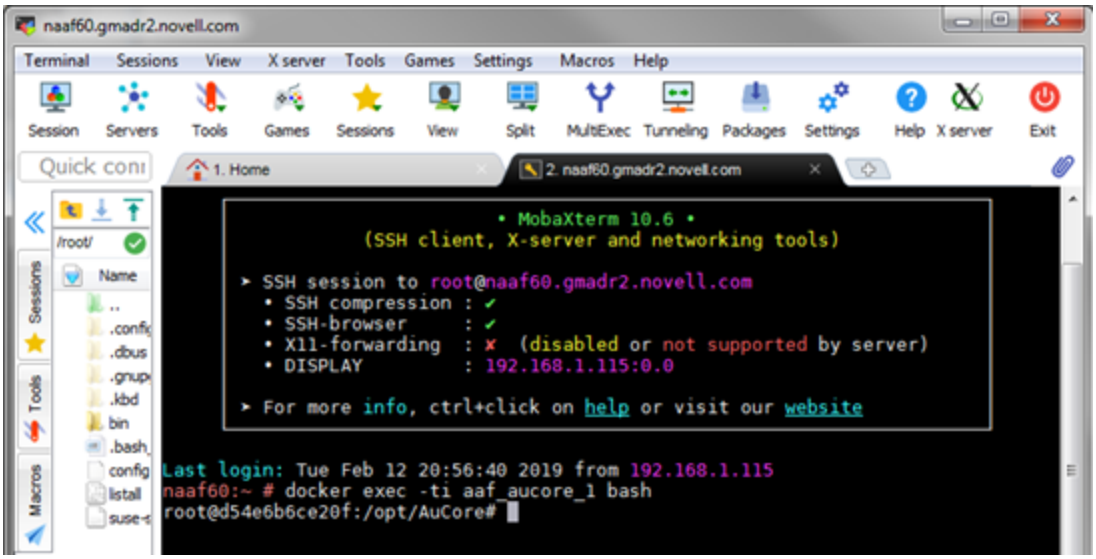
Using an SSH client or from the VM console, login as the root user. In this example we use an application called MobaXterm. https://mobaxterm.mobatek.net/download.html





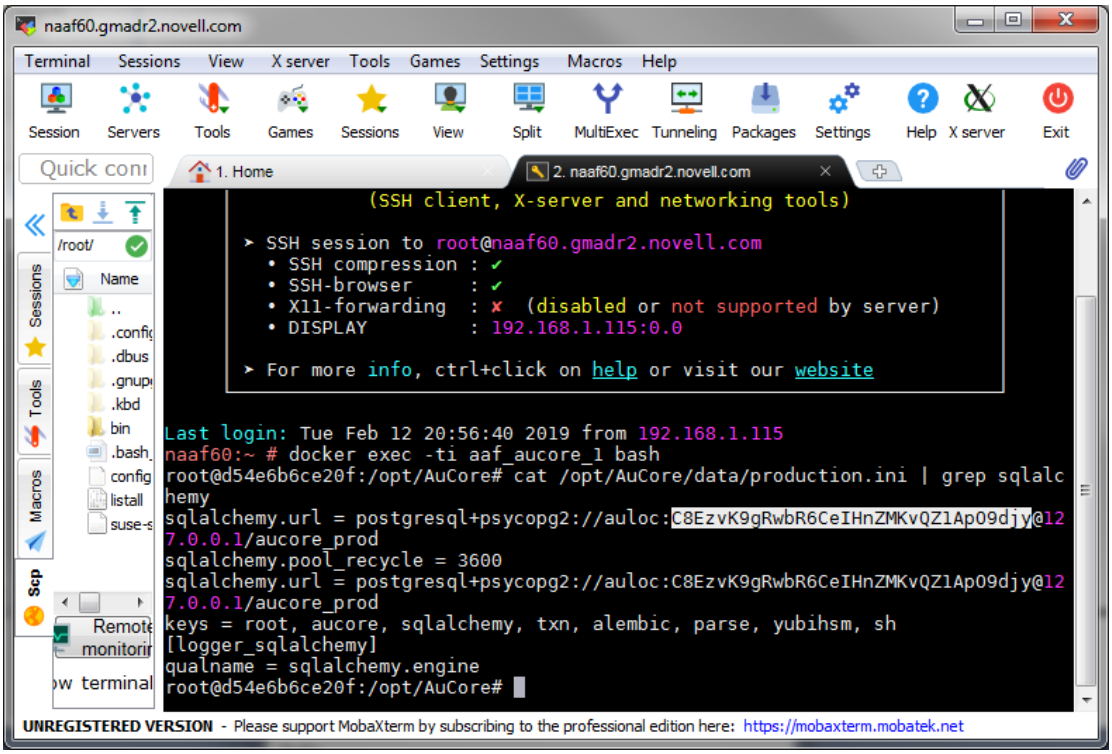
Type the following to open a bash shell to the AAF docker container “aaf_aucore_1”.

docker exec -ti aaf_aucore_1 bash



Now type the following command to display the PostgreSQL remote users' password.

cat /opt/AuCore/data/production.ini | grep sqlalchemy



Copy the password from the screen. The password is the value highlighted above between the : and @ symbols.

Paste this value into the SLAnalyzer SQLBrowser window as the Database User Credentials Password.

Web Browser

This tool allows the user to browse to web resources.

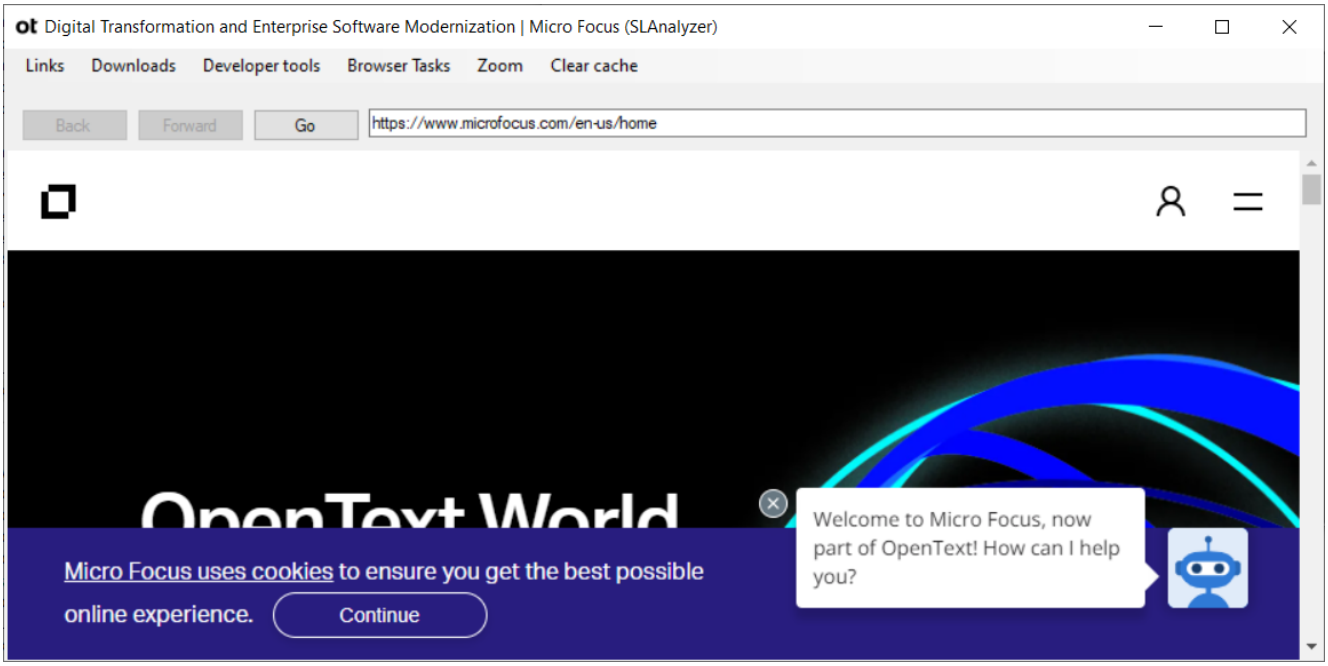


Figure 208 - Web Browser

Starting with SLAnalyzer version 9.0 the built-in web browser is Chromium based.

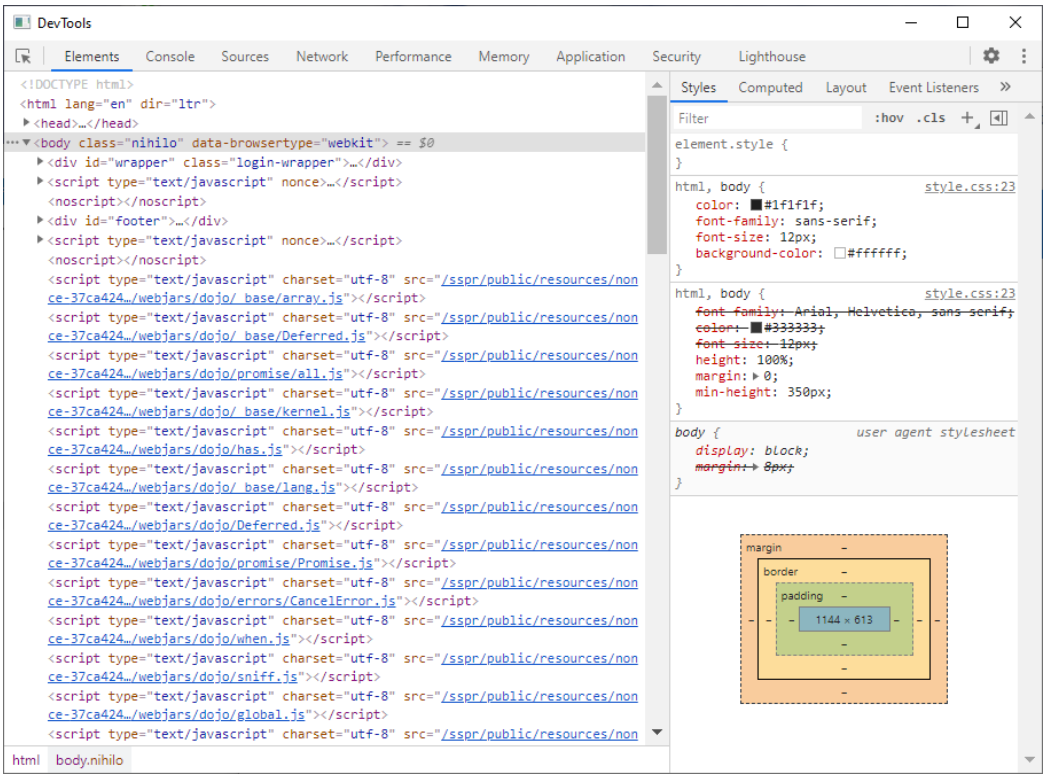
To navigate to a new web address type the address into the URL box and then click the Go button. To debug or trace the communications in the web browser, click on the Dev Tools button.

To save and or manage stored addresses click the Links button.

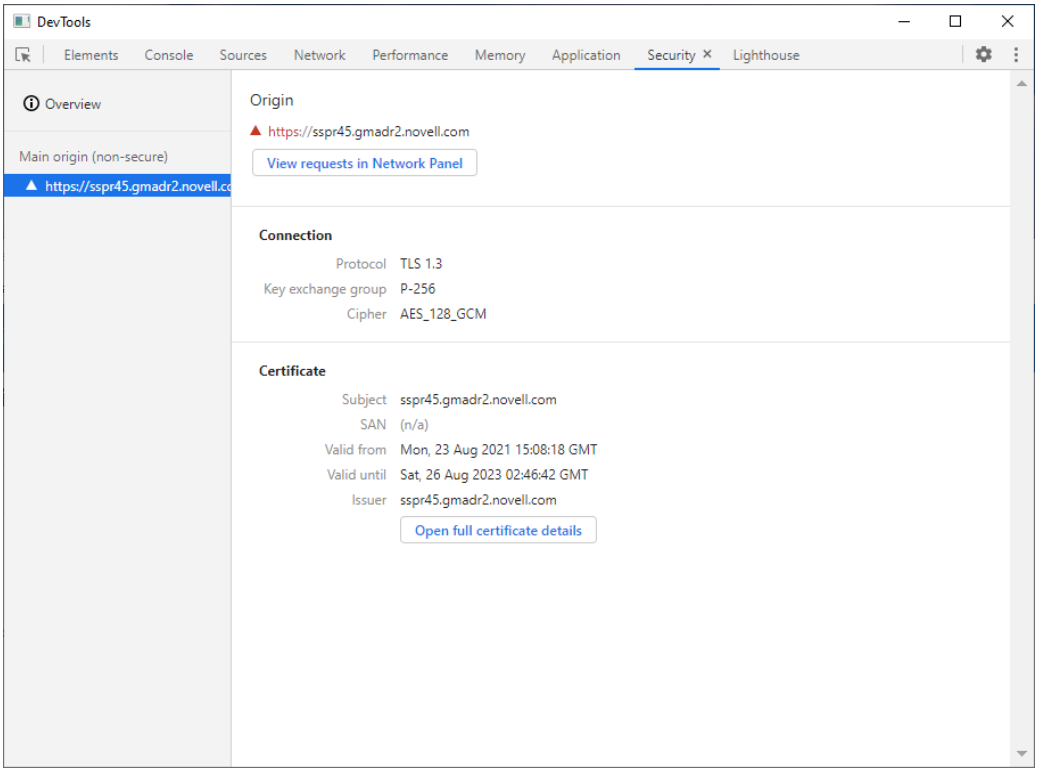
The Web Links menu displays the saved links and other links used by other SLAnalyzer profiles. For example, AAF links or SSPR links. Selecting a link from the Web Links menu and then clicking the Navigate button will close the Web Links menu and navigate to the selected URL.

Developer tools

The developer tools provide the ability to trace the browser communications on the internet. This is the same interface as seen in other browsers by pressing the F12 key.



The developer tools provide a wide variety of debugging. For example, to identify the certificate used for communications you could click on the Security tab.



Click on the network tab to save the traffic as a HAR file.

Click on the Elements tab to see elements on the currently displayed page.

Click on the Console tab to type in JAVA script commands and other live debugging.

Configure SLAnalyzer

Configuration settings are provided to allow the changing of the default report folder and the active set of filter type definitions.

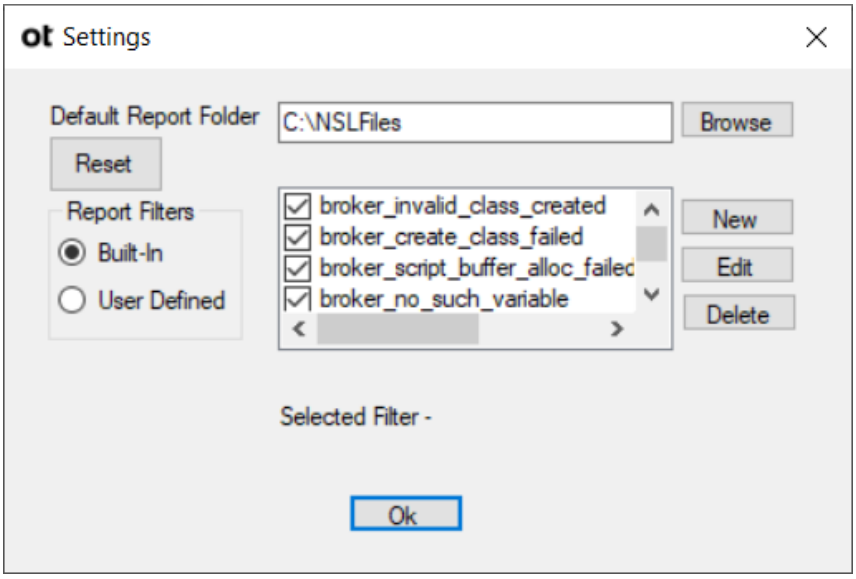


Figure 209 - SLAnalyzer settings

The configuration window has the following components

- Default Report Folder
- Reset button
- Report Filters type
- New button
- Edit button
- Delete button
- Ok button

Changing the default report folder

This location defaults to c:\nslfiles if the registry key does not exist. User can type in a folder location or use the browse button to locate a valid folder starting from the user's documents folder. Folder location is verified when the Ok button is pressed. If the user presses the Reset button the configuration registry key is deleted and SLAnalyzer will default back to the path of c:\nslfiles.

Click reset button to reset the default report folder to c:\nslfiles

Report Filter Type Definitions

Filters allow SLAnalyzer to colorize debug logs and files to highlight specific conditions or other information. For example colorizing and line that contains the word “Error” in the color “Red”. SLAnalyzer supports two different type of filters.

- Built-In
- User Defined

The ability to disable, modify, create and delete filters is available for both types.

Filter type colors are currently defined as:

- None - No colorization
- Error - Red
- Warning - Yellow
- Success - Green
- Label - Cyan
- SectionMark – Gray

After making filter changes click the Ok button to apply the changes.

Note that changes to the filters are not dynamic so any logs that are currently loaded will need to be reloaded to reflect the new filter modifications.

Built-In Filters

SLAnalyzer has a number of built-in report filters to identify and colorize specific information in log files.

When the radio button is clicked for Built-in, then a listing of the built-in filters is displayed. A check in the checkbox next to the filter name indicates that the filter is enabled and active.

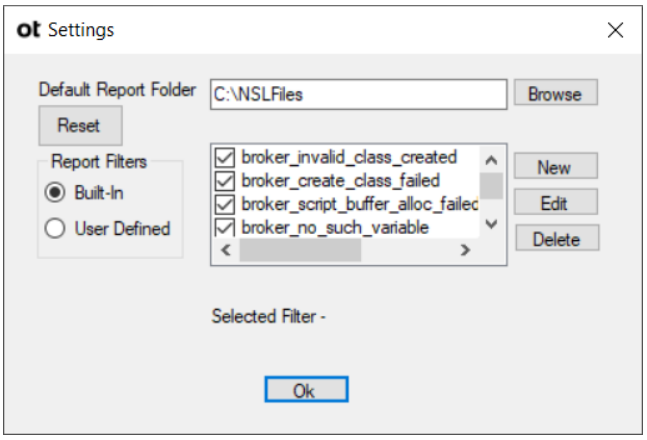


Figure 210 - Built-In report filters

Directly below the filter list window the text Selected Filter – will display the status of any filter selected in the filter list window.

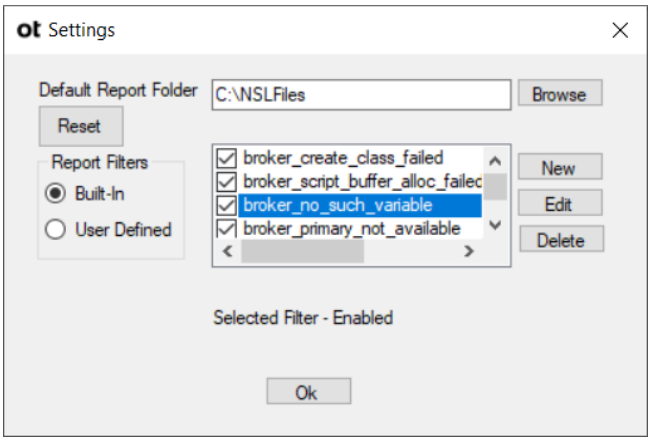


Figure 211 - Enabled built-in filter

User Defined Filters

Disabled and modified built-in filters are displayed in the User Defined list in addition to any user defined filters.

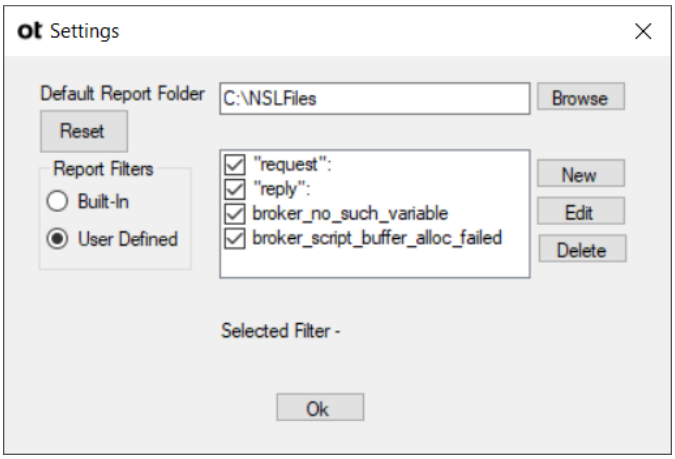


Figure 212 - User defined filters

Disabling a filter

Double clicking on a filter in the filter list will enable or disable that filter. The filter status will change to either enabled or disabled.

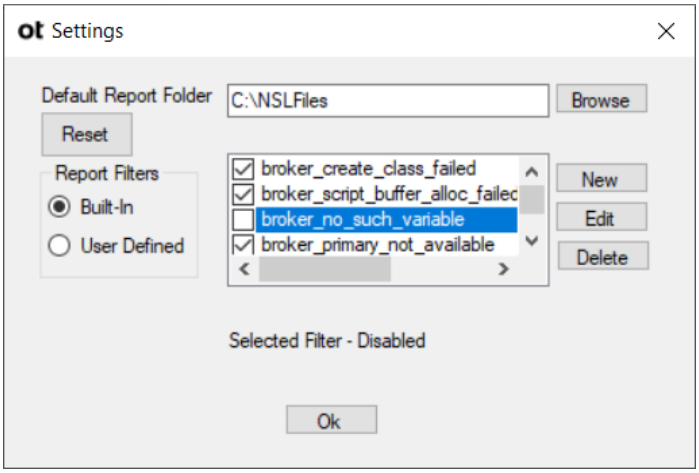


Figure 213 - Disabled built-in filter

Editing a filter

By highlighting any of the built-in or user defined filters from the list then clicking the Edit button, the user can edit the type defined for this filter, for example (None, Error, Warning, Success, Label, or SectionMark). Once a built-in filter has been modified it will display in both the Built-in and User defined lists.

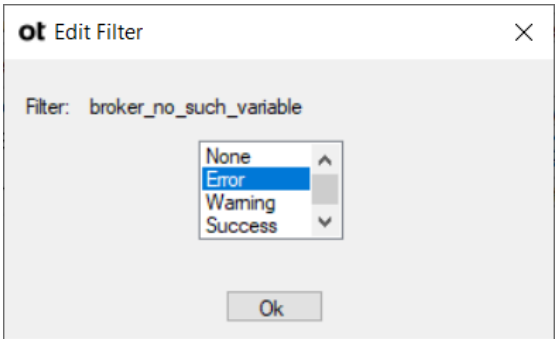


Figure 214 - Edit filter

Deleting a Filter

To delete a user defined filter for a built-in filter the user can highlight the filter and press the delete button. A message will be provided to let the user know that they have deleted the user defined filter for a built-in filter and that the filter will revert back to the default level.

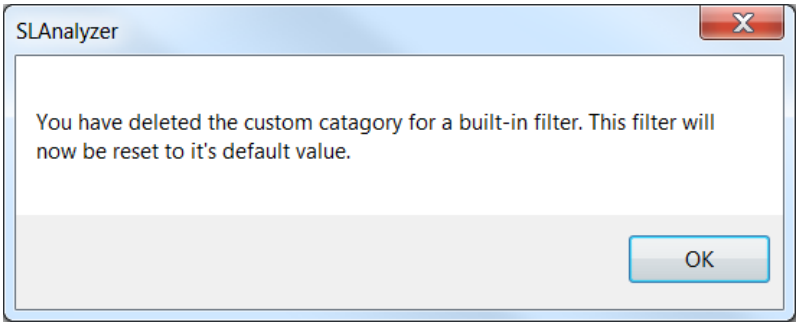


Figure 215 - Delete user defined filter

You cannot delete a built-in filter. You can only disable built-in filters.
If the user attempts to delete a built-in filter then an error message will be displayed.

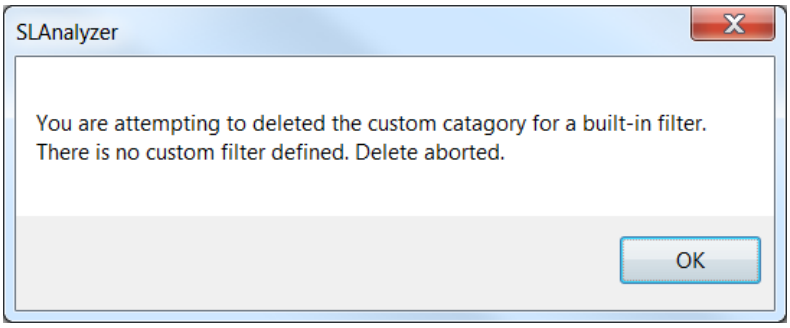


Figure 216 - Attempt to delete a built-in filter

Creating a new filter

By clicking the new filter button the user can create a new User defined filter. The filter can be any set of characters or words that the user would like to be identified when any of the log files are loaded. For example if the user defines a new filter of the words "loaded by" and then with the type of Warning then any log entries that are found with this sequence of words will be highlighted in the color defined for that specific filter type.

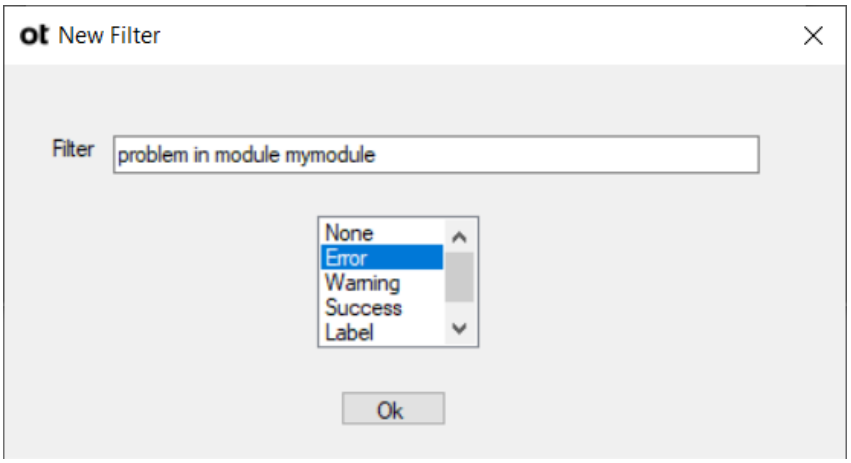


Figure 217 - Create new filter

Note that by identifying any sequence of words as the type Error, Warning, or Success allows for the setting of the filter from the main report window by selecting the desired type and then clicking the Filter button. Note that to set a filter you must have a file open and displayed.

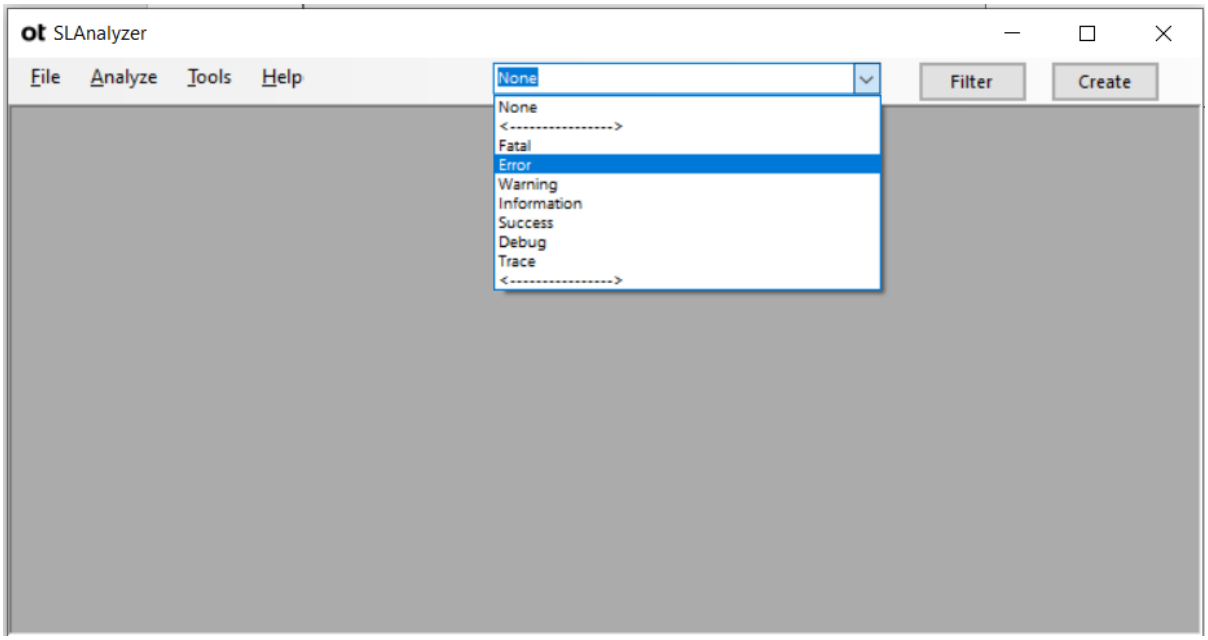


Figure 218 - Setting filter to Errors

Help Menu

The help menu contain links to additional resources and the about window. Clicking on a link will open the internal webbrowser window.

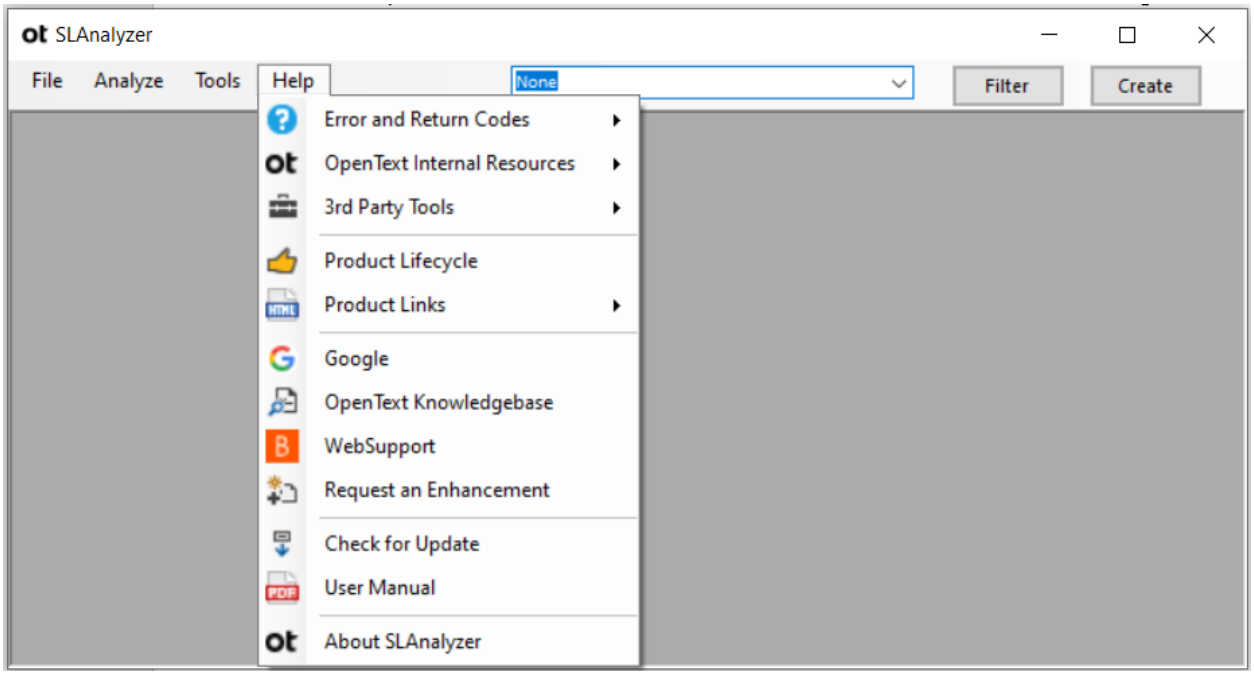


Figure 219 - Help menu

The help menu consists of the following links

- Error and Return Codes – Public URL's to lookup errors and return codes
- OpenText Internal Resources – URL's requiring Micro Focus login/VPN
- 3rd Party Tools – Useful tools to assist in debugging and troubleshooting
- Product Lifecycle – Micro Focus product lifecycle information
- Product Links – Links to online documentation and Wiki sites
- Google – Browser to google.com
- OpenText Knowledgebase – Micro Focus Support database
- WebSupport – Bomgar client session. (enter session ID)
- Request an Enhancement – Opens a browser to the ideas portal
- Check For Update – Performs check for update (same check as on load)
- User Manual – Opens current SLAnalyzer user manual
- About SLAnalyzer - About

Error and Return Codes

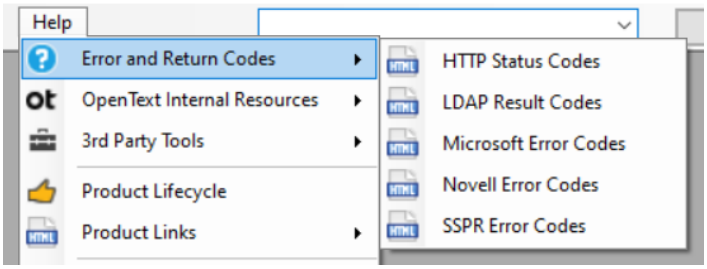


Figure 220 - Error and Return Codes

- HTTP Status Codes – Public website:
- LDAP Result Codes – Public website:
- Microsoft Error Codes – Public website:
- Novell Error Codes – Public website:
- SSPR Error Codes – Public website:

OpenText Internal Resources

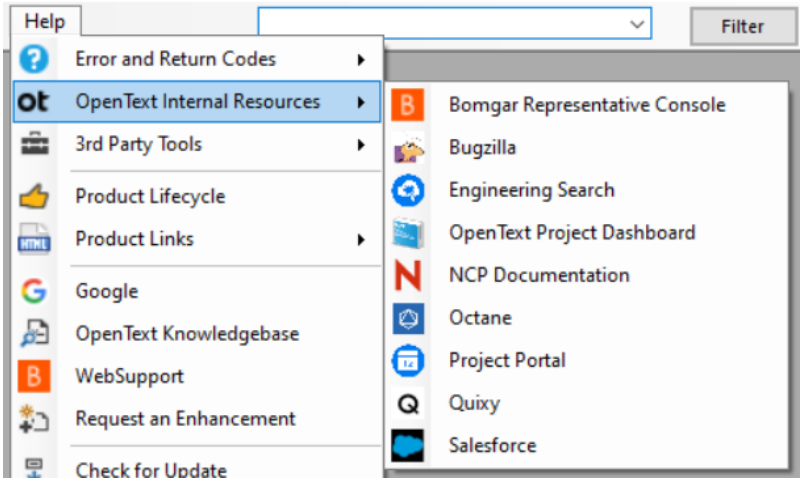


Figure 221 - Micro Focus Internal Resources

- Bomgar Representative Console – Requires login
- Bugzilla – Public (customer access) and Internal (private access)
- Engineering Search – Requires VPN
- OpenText Project Dashboard – Requires login
- NCP Documentation – Requires VPN
- Octane – Requires login
- Project Portal – Requires VPN
- Quixy – Requires login
- Sales Force – Requires login

3rd Party Tools

These links provide access to common tools used by Micro Focus support. These tools are supported by their respective provider.

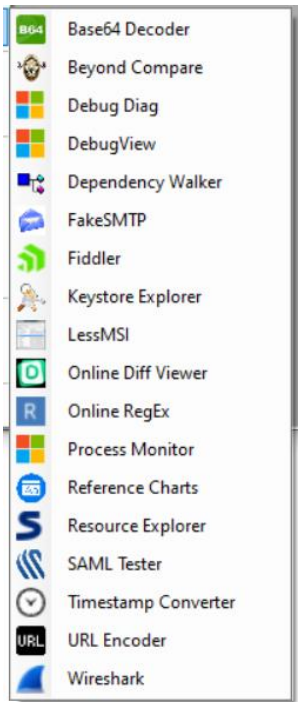


Figure 222 - 3rd Party Tools

- Base64 Decoder– Online resource to decode Base64 data
- Beyond Compare – Compare 2 files
- Debug Diag – Generate and configure Windows memory dumps
- DebugView – Debug Console for Windows
- Dependency Walker – View API information for DLL's
- FakeSMTP – Capture calls to SMTP server. For SSPR email testing
- Fiddler – Capture browser traffic
- Keystore Explorer – Graphical UI replacement for keytool
- LessMSI – extract and inspect MSI packages
- Online Diff Viewer – compare text based data.
- Online RegEx – Regular Expresions test site
- Process Monitor – Monitor windows processes
- Reference Charts – ASCII, HTML, Number conversion charts
- Resource Explorer – View/modify contents of resource DLL's
- Timestamp Converter – Convert AD/LDAP timestamp values. Also page for Unix Timestamp used by eDir and Linux.
- URL Encoder – URL Encoder/Decoder
- Wireshark – Capture and analysis of network traffic

Product Links

Provides quick links to product documentation and other useful resources. Wiki sites listed require Micro Focus login credentials.

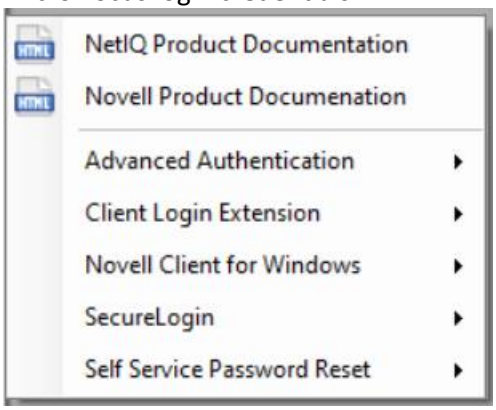


Figure 223 - Product Links

About SLAnalyzer

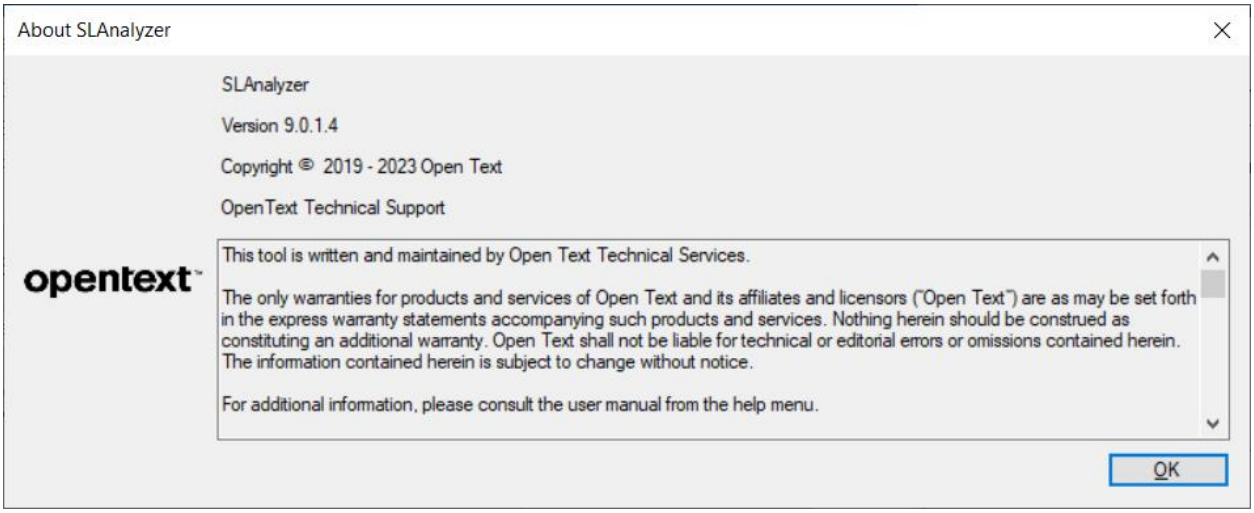


Figure 224 - About box

The about box displays information about the SLAnalyzer application and open-source libraries used.

Sample Reports

The following reports are provided as examples of the information provided by SLAnalyzer.

Sample Computer Information report

Report generated by: SLAnalyzer Version 3.0.0.0

##
Computer Information
##

########################
Hardware
########################
Manufacturer: VMware, Inc.
Model: VMware Virtual Platform
BIOS: 6.00
BIOS Date: 07/02/2012

Processor: AMD64
Processor Identifier: Intel64 Family 6 Model 37 Stepping 5, GenuineIntel
Processor Level: 6
Processor Revision: 2505
# of Processors: 1

########################
OS version
########################
Operating System: Microsoft Windows 7 Enterprise N Version 6.1.7601 SP 1.0

########################
Network Providers
########################
Provider Order: EACredentialManager,vmhgfs,RDPNP,LanmanWorkstation,webclient

Credential provider (EACredentialManager) exists in location specified
Details:
Provider name: C:\Windows\system32\EACredentialManager.dll
Vendor:
Description: slEmerge Application

Credential provider (vmhgfs) exists in location specified
Details:
Provider name: C:\Windows\System32\vmhgfs.dll
Vendor: VMware, Inc.
Description: VMware HGFS Provider

Credential provider (RDPNP) exists in location specified
Details:
Provider name: C:\Windows\System32\drprov.dll
Vendor: Microsoft Corporation
Description: Microsoft Remote Desktop Session Host Server Network Provider

Credential provider (LanmanWorkstation) exists in location specified
Details:
Provider name: C:\Windows\System32\ntlanman.dll
Vendor: Microsoft Corporation
Description: Microsoft® Lan Manager

Credential provider (webclient) exists in location specified
Details:
Provider name: C:\Windows\System32\davclnt.dll
Vendor: Microsoft Corporation
Description: Web DAV Client DLL

########################
Authentication Providers
########################
Credential Providers:

Auth Provider: ac.mscredprov.pincache
Auth Provider: GenericProvider
Auth Provider: NPProvider
Auth Provider: VaultCredProvider
Auth Provider: CLESelfSvcCredentialProvider
Auth Provider: PasswordProvider
Auth Provider: NLDAPCredentialProvider
Auth Provider: Smartcard Credential Provider
Auth Provider: Smartcard Pin Provider
Auth Provider: WinBio Credential Provider
Auth Provider: CLECredentialProvider
Auth Provider: CertCredProvider

######################
Software
######################
Installed programs:

######################
Windows Applications
######################
Application: Attachmate Java 7 Update 45 (x64)
Vendor: Attachmate Corporation
Version: 7.0.450
Language: 1033
Installation Path:
Installation Date: 20150713
Product ID: {0A63F60B-48B7-4C28-BAA8-4341170449E4}
Information Source: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{0A63F60B-48B7-4C28-BAA8-4341170449E4}
System Component: False

Application: Attachmate Reflection Pro 2014 (x64)
Vendor: Attachmate Corporation
Version: 15.6.636
Language: Not Defined
Installation Path: C:\Program Files (x86)\Attachmate\Reflection\
Installation Date: Not Defined
Product ID: ReflectionAS156R1_Release
Information Source: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\ReflectionAS156R1_Release
System Component: False

Application: Client Login Extension 3.9.0.0
Vendor: NetIQ Corporation
Version: 3.9.0
Language: 1033
Installation Path:
Installation Date: 20150812
Product ID: {18F58277-A5A6-4361-A26C-300047A0BBA5}
Information Source: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{18F58277-A5A6-4361-A26C-300047A0BBA5}
System Component: False

Application: Client Login Extension Configuration Utility Setup 3.8.1.0
Vendor: NetIQ Corporation
Version: 3.8.1
Language: 1033
Installation Path:
Installation Date: 20150729
Product ID: {6BA26A60-0A46-4937-8B04-FCC5902AF1F0}
Information Source: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{6BA26A60-0A46-4937-8B04-FCC5902AF1F0}
System Component: False

Application: Definition Update for Microsoft Office 2010 (KB3101540) 32-Bit Edition
Vendor: Microsoft

Version: Not Defined
Language: Not Defined
Installation Path: Not Defined
Installation Date: Not Defined
Product ID: {91140000-0012-0000-0000-0000000FF1CE}_Office14.STANDARDR_{E26C085F-C2D6-4BF0-B002-F539788473E4}
Information Source: HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{91140000-0012-0000-0000-0000000FF1CE}_Office14.STANDARDR_{E26C085F-C2D6-4BF0-B002-F539788473E4}
System Component: False

Application: Java 8 Update 51
Vendor: Oracle Corporation
Version: 8.0.510
Language: 1033
Installation Path:
Installation Date: 20150811
Product ID: {26A24AE4-039D-4CA4-87B4-2F83218051F0}
Information Source: HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{26A24AE4-039D-4CA4-87B4-2F83218051F0}
System Component: False

Application: Microsoft .NET Framework 4.5
Vendor: Microsoft Corporation
Version: 4.5.50709
Language: Not Defined
Installation Path: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SetupCache\
Installation Date: Not Defined
Product ID: {92FB6C44-E685-45AD-9B20-CADF4CABA132} - 1033
Information Source: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132} - 1033
System Component: False

######################
Windows system components
######################
Application: Attachmate Reflection Pro 2014 (x64)
Vendor: Attachmate Corporation
Version: 15.6.636
Language: 0
Installation Path: C:\Program Files (x86)\Attachmate\Reflection\
Installation Date: 20150713
Product ID: {A13CE473-359B-4341-A3B2-0F93880261D5}
Information Source: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{A13CE473-359B-4341-A3B2-0F93880261D5}
System Component: True

Application: Java Auto Updater
Vendor: Oracle Corporation
Version: 2.8.51.16
Language: 1033
Installation Path:
Installation Date: 20150811
Product ID: {4A03706F-666A-4037-7777-5F2748764D10}
Information Source: HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{4A03706F-666A-4037-7777-5F2748764D10}
System Component: True

Application: Microsoft .NET Framework 4.5
Vendor: Microsoft Corporation
Version: 4.5.50709
Language: 0
Installation Path:
Installation Date: 20151209
Product ID: {1AD147D0-BE0E-3D6C-AC11-64F6DC4163F1}
Information Source: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1AD147D0-BE0E-3D6C-AC11-64F6DC4163F1}
System Component: True

Windows Startup Programs
########################
Startup applications from: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
########################
Name: VMware User Process
Path: "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr

########################
Startup applications from: HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
########################
Name: SunJavaUpdateSched
Path: "C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"

########################
Startup applications from: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
########################
########################
Internet Browser
########################
Default Browser: c:\program files\internet explorer\iexplore.exe

########################
Microsoft Internet Explorer
########################
Microsoft Internet Explorer version: 11.0.9600.18426
Enable 3rd party browser extensions is: yes
Internet Explorer Browser Helper Objects:
Registry Location: SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Browser Helper Objects

BHO Module: {DBC80044-A445-435b-BC74-9C25C1C588A9}
Name: C:\Program Files (x86)\Java\jre1.8.0_73\bin\jp2ssv.dll
BHO Module: Enabled

BHO Module: {D0498E0A-45B7-42AE-A9AA-ABA463DBD3BF}
Name: C:\PROGRA~2\MIF5BA~1\Office15\GROOVEEX.DLL
BHO Module: Enabled
…
########################
Mozilla FireFox
########################

Mozilla FireFox version: 45.4.0

Mozilla FireFox Extension:
Name: {00CC6330-A221-429B-9FAD-FD29EC560D7A}
Value: C:\Program Files (x86)\ActivIdentity\ActivClient\Mozilla Extensions\{00CC6330-A221-429B-9FAD-FD29EC560D7A}\

Mozilla FireFox Extension:
Name: fiddlerhook@fiddler2.com
Value: C:\Program Files (x86)\Fiddler2\FiddlerHook

########################
Google Chrome
########################
Chrome browser found

Version: 54.0.2840.99

Chrome extension: aohghmighlieiainnegkcijnfilokake
Version: 0.9_0

```
{
  "appDesc": {
    "description": "App description.",
    "message": "Create and edit documents "
  },
  "appName": {
```

```
    "description": "App name.",
    "message": "Google Docs"
  }
}

Chrome extension: apdfllckaahabafndbhieahigkjlhalf
Version: 14.1_0
{
  "appDesc": {
    "description": "App description.",
    "message": "Google Drive: create, share and keep all your stuff in one place."
  },
  "appName": {
    "description": "App name.",
    "message": "Google Drive"
  }
}

########################
Environment
########################
User Name:              Greg
User Domain:            GMADR2
Computer Name:          WIN7VM
Home Path:              \Users\Greg.GMADR2
Logon Server:           \\WIN-V3JMMISD13E

System Path: C:\ProgramData\Oracle\Java\javapath;C:\Program Files\Attachmate\Reflection\;C:\Program Files
(x86)\Attachmate\Reflection\;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\
v1.0\;C:\Program Files (x86)\ActivIdentity\ActivClient\;C:\Program Files\ActivIdentity\ActivClient\

########################
System Resource Information
########################

Warning: SLAnalyzer does not have sufficient rights to read all information about running processes.
Run SLAnalyzer with Runas administrator to obtain all possible information for running processes.

Running Process: aaacachesrv

Process ID: {2044}
Window Title: {}
CPU % {0%}
Memory Usage: {8872} KB
VM Size: {3232} KB
Non-Paged Pool: {10.8515625} KB
Process is responding

Parent process information:
Parent Process ID: 720
Parent Process Name: services

…
########################
IP Configuration Information
########################

Windows IP Configuration

   Host Name . . . . . . . . . . . . : REMGMORRIS01
   Primary Dns Suffix  . . . . . . . : microfocus.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : gns.novell.com
                                       microfocus.com
```

```
   System Quarantine State . . . . . : Not Restricted
########################
ARP Information
########################

Interface: 127.0.0.1 --- 0x1
  Internet Address      Physical Address      Type
  224.0.0.2                         static
  224.0.0.22                        static
  239.255.255.250                   static
  239.255.255.253                   static

########################
DNS Information
########################

Windows IP Configuration

    naaf53.gmadr2.novell.com
    ----------------------------------------
    Record Name . . . . . : naaf53.gmadr2.novell.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 86400
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 192.168.1.245

########################
TCP Port Information
########################

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            REMGMORRIS01:0         LISTENING
  TCP    0.0.0.0:443            REMGMORRIS01:0         LISTENING
  TCP    0.0.0.0:445            REMGMORRIS01:0         LISTENING
  TCP    0.0.0.0:623            REMGMORRIS01:0         LISTENING

########################
Routing Table
########################
===========================================================================
Interface List
 19...c0 cb 38 cc 4b da ......Bluetooth Device (Personal Area Network) #3
 12...5c 26 0a 1c b0 3d ......Intel(R) 82577LM Gigabit Network Connection
 23...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 24...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  1...........................Software Loopback Interface 1

###########################################
End of Report.
###########################################
```

Sample Group Policy report

Report generated by: SLAnalyzer Version 3.0.0.0

```
######################
GPO Information
######################

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

Created On 12/10/2015 at 3:54:03 PM


RSOP data for GMADR2\Greg on WIN7VM : Logging Mode
-----------------------------------------------------

OS Configuration:          Member Workstation
OS Version:                6.1.7601
Site Name:                 Default-First-Site-Name
Roaming Profile:           N/A
Local Profile:             C:\Users\Greg.GMADR2
Connected over a slow link?: No


COMPUTER SETTINGS
------------------
   CN=WIN7VM,CN=Computers,DC=gmadr2,DC=novell,DC=com
   Last time Group Policy was applied: 12/10/2015 at 3:49:00 PM
   Group Policy was applied from:     WIN-V3JMMISD13E.gmadr2.novell.com
   Group Policy slow link threshold:  500 kbps
   Domain Name:                       GMADR2
   Domain Type:                       Windows 2000

   Applied Group Policy Objects
   -----------------------------
      Default Domain Policy

   The following GPOs were not applied because they were filtered out
   -------------------------------------------------------------------
      Local Group Policy
         Filtering:  Not Applied (Empty)

   The computer is a part of the following security groups
   -------------------------------------------------------
      BUILTIN\Administrators
      Everyone
      BUILTIN\Users
      NT AUTHORITY\NETWORK
      NT AUTHORITY\Authenticated Users
      This Organization
      WIN7VM$
      Domain Computers
      System Mandatory Level


USER SETTINGS
--------------
   CN=Greg Morris,CN=Users,DC=gmadr2,DC=novell,DC=com
   Last time Group Policy was applied: 12/10/2015 at 3:48:59 PM
   Group Policy was applied from:     WIN-V3JMMISD13E.gmadr2.novell.com
   Group Policy slow link threshold:  500 kbps
   Domain Name:                       GMADR2
   Domain Type:                       Windows 2000

   Applied Group Policy Objects
```

N/A

The following GPOs were not applied because they were filtered out
---
Default Domain Policy
Filtering: Not Applied (Empty)

Local Group Policy
Filtering: Not Applied (Empty)

The user is a part of the following security groups

Domain Users
Everyone
BUILTIN\Users
BUILTIN\Administrators
NT AUTHORITY\INTERACTIVE
CONSOLE LOGON
NT AUTHORITY\Authenticated Users
This Organization
LOCAL
Domain Admins
SSPR Admins
SSPR Help Desk
RestUsers
Schema Admins
Authenticore Admins
Authasas Advanced Authentication Admins
NetIQ Advanced Authentication Framework Admins
Denied RODC Password Replication Group
High Mandatory Level

##
End of Report.
##

Sample Registry report

Report generated by: SLAnalyzer Version 3.0.0.0

##########
Keys Defined in: HKEY_LOCAL_MACHINE\SOFTWARE\Protocom\SecureLogin
##########

Key: WEBSSO_DHTML
Type: DWord
Enables DHTML events on Internet Explorer and Mozilla Firefox browsers. On Internet Explorer supports DHTML events for modal and modeless windows.

Value	Description
0	Disables DHTML events.
1	Enables DHTML events for web pages. Additional events can be captures using -events argument. For information about -event, see 'Site/Endsite' in the NetIQ SecureLogin Application Definition Guide.

Value defined in registry: 0

Key: InternalVersion
Type: String
Version info of the NetIQ SecureLogin installer.

Value defined in registry: 8.0.3.0

Key: EnableWindowsEventlog
Type: DWord
Enable/Disable sending audit event to Windows event logger.

Value	Description
1	Enable
0	Disable (default)

Value defined in registry: 1

Key: DisableVPNCheck
Type: DWord
Check for VPN connection.

* Applicable in LDAP mode

Value	Description
1	Default, Authenticate the client with the LDAP server if the client is connected to a domain through VPN.
0	Do not Authenticate

Value defined in registry: 0

Key: DisableFlashSSO
Type: DWord
Disable Flash/Flex SSO extension

Value	Description
1	Disable
0	Enable

Value defined in registry: 0

Key: CacheDirectory

Type: String
Specifies that the local cache file is saved in a custom location.

* At install, SecureLogin allows you to choose a custom location for the cache file, or specify the user profile.
* If a custom location is selected, the CACHEDIRECTORY registry key is enabled; and the local file cache will be stored in the named location.
* Once set, this key will overwrite the UseUserProfileDirectory registry setting

Value	Description
c:\path	Stores the cache file for every user on this machine in named location

---
Value defined in registry: %LOCALAPPDATA%

##########
Keys Defined in: HKEY_LOCAL_MACHINE\SOFTWARE\Protocom\SecureLogin\JavaSSO
##########

Key: JREInstallDir
Type: String
Record the JRE location against which one SecureLogin is installed

* When SecureLogin detects a new JRE and installs its component against it, then a registry key is created to keep track of the supported JRE
* In versions prior to 6.1 this key was referencing the only supported JRE
* In SecureLogin 6.1 and later, this key is used for backward compatibility purpose only as SecureLogin is able to install and work with several JREs.

Value	Description
path	Path to the JRE directory

Value defined in registry: C:\Program Files (x86)\Java\jre1.6.0_03

Key: Installed
Type: DWord
Dynamic value indicating if SecureLogin was able to install the JAVASSO module at load time.

Value	Description
1	Installed.
0	Not installed.

Value defined in registry: 1

##########
Keys Defined in: HKEY_LOCAL_MACHINE\SOFTWARE\Protocom\SecureLogin\Logging
##########

##########
Keys Defined in: HKEY_LOCAL_MACHINE\SOFTWARE\Protocom\SecureLogin\Security
##########

Key: SecondaryStore
Type: String
Secifies the secondary data store

* Available in Version 6.0 releases and later
* Used to specify whether or not there is a local cache, or whether credentials are stored on a smart card in place of a local cache.
* The secondary store is set to file by SecureLogin at install, unless smart card support is selected, in which case the secondary store will be set to smart card

* Note that even if the registry entry shows smart card for the secondary store, the file cache will still be used until the preference ‘Store credentials on card’ is set; that is, this setting specifies the smart card preferences are allowed to be used, the preference enforces the smart card setting

* Note that this registry key should NOT be changed manually, as the secondary store mode relies on files that would normally be made available at installation

Value	Description
File	Local file cache, no smart card support
Smartcard	Option to use store on card, or PKI encryption of credentials

NOTE: Full implementation depends on applying smart card preferences through admin console
---
Value defined in registry: FILE

Key: PrimaryStore
Type: String
Specifies the primary directory mode

* Available in Version 6.0 releases and later
* Used to specify the primary directory mode.
* The primary directory store is set by SecureLogin at install, depending on the selected install options. The registry keys set out in this section are created as part of install process, based on those selected options.
* Note that this registry key should NOT be changed manually, as the directory mode relies on files that would normally be made available at installation.

Value:	Description:
NDS	eDirectory (Novell client required)
Dummy	No directory – standalone mode
MAD	Microsoft Active Directory
LDAP	LDAP Directory
SecretStore	Novell eDirectory with SecretStore (relies on Novell client)
LDAPSecretStore	LDAP login to eDirectory with SecretStore (no Novell client)

Value defined in registry: DUMMY

##########
Keys Defined in: HKEY_LOCAL_MACHINE\SOFTWARE\Protocom\SecureLogin\Volatile
##########

##########
Keys Defined in: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Protocom
##########

##########
Keys Defined in: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Protocom\SecureLogin
##########

##########
Keys Defined in: HKEY_CURRENT_USER\SOFTWARE\Protocom\SecureLogin
##########

Key: WizardGUIRect
Type: String

Value defined in registry: 1551,107,1265,700,0

Key: SeamlessStandalone
Type: DWord
Defines the standalone behavior

* Available in 6.0 and onwards

* Defines the standalone behavior in regards to credentials to use to start SecureLogin.
* Either SecureLogin starts using the logged in user's credentials or it is in multiple account mode and starts prompting for the users to select their account

Value	Description
1	When login credentials are used to start SSO (single user mode)
0	When multiple users mode is on.

Value defined in registry: 1

Key: RestoreStatus
Type: DWord

Value defined in registry: 1

Key: OfflineWarningSuppressed
Type: DWord
Enable/Disable the warning message when logging in the workstation in offline mode.

Value defined in registry: 1

Key: MainGUIRect
Type: String

Value defined in registry: 133,-20,1143,500,1

Key: LogFileDirectory
Type: String
Specifies the path to the SSODebug.txt file.

* If present in either HKLM or HKCU, SecureLogin will create the log file in the path specified.
* If this key is not defined then the default log path is set to the value of the registry key 'CacheDirectory'.

Value	Description
path	String representing the desired path.

Value defined in registry: %LOCALAPPDATA%

Key: LastNDSUser
Type: String
Last NDS user that SecureLogin successfully connected to eDirectory with.

Value Data Type: REG_SZ
Help/Comment: Represented in the dot format. IE admin.novell

Value defined in registry: CN=admin.O=novell.T=OESTREE

Key: LastCacheUser
Type: String
Last user that successfully loaded from cache file.

Value defined in registry: Greg

Key: DisplayInitialLoadSplash
Type: DWord
Disables the SecureLogin splash screen at startup

* Available in 6.1 and onwards
* This key is created by default and linked to the preference: 'Display splash screen on start up'

Value	Description
1	Default setting: Display SecureLogin splash screen at startup
0	Disable SecureLogin splash screen at startup

Value defined in registry: 1

##########
Keys Defined in: HKEY_CURRENT_USER\SOFTWARE\Protocom\SecureLogin\LDAP Settings
##########

Key: SSL Cert File
Type: String
SSL certificate to use for secure LDAP connection

Value	Description
C:\\CertLocation\\client.der	Path to SSL certificate file.

Value defined in registry: C:\Program Files\NetIQ\SecureLogin\rootcert.der
---

Key: SecondaryPort
Type: DWord
Specifies Secondary LDAP connection port

Value	Description
636	LDAP port of secondary LDAP connection

Value defined in registry: 636

Key: SecondaryHost
Type: String
Specifies Secondary LDAP connection

Value	Description
IP Address	IP address of secondary LDAP connection. Used if primary connection failes

---
Value defined in registry:

Key: PrimaryPort
Type: DWord
Specifies Primary LDAP connection port

Value	Description
636	LDAP port of primary LDAP connection

Value defined in registry: 636

Key: PrimaryHost
Type: String
Specifies Primary LDAP connection

Value	Description
IP Address	IP address of primary LDAP connection

Value defined in registry: 192.168.1.243

Key: NonSecureLDAPPort

Type: DWord

Value defined in registry: 389

Key: LastUser
Type: String
Last user the SecureLogin was able to successfully connect to the LDAP directory with.

Value defined in registry: cn=admin,o=novell

Key: CustomSearchFilter
Type: String
Customize the LDAP search filter

* This key has been introduced in SecureLogin 6.1 Hotfix FIXC0803002
* Relevant only in LDAP mode
* By default, if the registry key/value is not specified, SecureLogin will now use the attributes supplied to build the search filter eg: (|(uid=*fred*)(samAccountname=*fred*))
* If the registry key is populated with a value, then SecureLogin will attempt to use that value as the search filter and will ignore the attributes listed in the LDAP login dialog.
* The CustomSearchFilter is built in the form eg: (&(objectClass=orgPerson)((orgUserAliases=%s@*)) where%s is detected and replaced with the username provided to end up as (&(objectClass=orgmPerson)((orgUserAliases=fred@*)). Any search filter can be used here and any instance of%s will be replaced with the username.
* This key is not created by default

Value	Description
string	The string value can be assigned as: (&(objectClass=geoPerson)(geoUserAliases=<user>@*))

Value defined in registry:

Key: CacheSecretsBad
Type: DWord

Value defined in registry: 1

Key: AttributesToSearch
Type: String
Specifies what attributes are used during the ldap search

* Available in SecureLogin 3.5.x and later.
* Set to a list of search attributes used in LDAP search.
* Only first five attributes specified are considered.

Note: any publicly readable attribute can be specified as a search attribute, for example 'fullName' 'givenName' 'sn' 'cn' 'uid', separated by spaces. To minimize search time, however, list as few attributes as are absolutely needed.

Also note that you do not need to provide ' ' while specifying the attribute entries.

Value	Description
string	Space seperated string of attributes to search

Value defined in registry: name sn givenname cn uid samAccountName
---

##########
Keys Defined in: HKEY_CURRENT_USER\SOFTWARE\Protocom\SecureLogin\Logging
##########

##########
Keys Defined in: HKEY_CURRENT_USER\SOFTWARE\Protocom\SecureLogin\msi
##########

Key: shortcuts_tray
Type: DWord

Value defined in registry: 1

Key: shortcuts_tlaunch
Type: DWord

Value defined in registry: 1

Key: shortcuts_help
Type: DWord

Value defined in registry: 1

Key: shortcuts_folder
Type: DWord

Value defined in registry: 1

Key: shortcuts_finder
Type: DWord

Value defined in registry: 1

##########
Keys Defined in: HKEY_CURRENT_USER\SOFTWARE\Protocom\SecureLogin\Volatile
##########

##
End of Report.
##

Sample Logging report

Report generated by: SLAnalyzer Version 3.0.0.0

##########
Debug Logging
##########
Checking for logging status.

SecureLogin client debug logging. (ssodebug.txt)
Workstation level logging is currently disabled
User level logging is currently disabled
Virtual Store logging is currently disabled

LDAPAuth client debugging
LDAPAuth debug logging disabled.

Virtual channel debugging
Virtual channel debug logging disabled.

Novell client debugging
Novell client debug logging is disabled.

NMAS client debugging
NMAS client debugging is disabled.

SecretStore client debugging
SecretStore debug logging disabled.

SecureWorkstation client debugging
SecureWorkstation client debugging is disabled.

DAS client debugging
DAS client debugging is disabled.

CLE debugging
CLE debugging is disabled.

PCProx client debugging
PCProx client debugging is disabled.

##########
End of Report.
##########

Sample SecureLogin report

Report generated by: SLAnalyzer Version 3.0.0.0

##
SecureLogin Client Information
##
SecureLogin version: 8.0.3.0
SecureLogin is installed in the path of: C:\Program Files\NetIQ\SecureLogin\
SecureLogin installed language: English

Warning: Trial version of SecureLogin detected

######################
NSL client files
######################
SecureLogin client files.
File: C:\Program Files\NetIQ\SecureLogin\debugmonitor.dll, Version: 8.0.3.0, Size: 48824
File: C:\Program Files\NetIQ\SecureLogin\debugmonitor64.dll, Version: 8.0.3.0, Size: 483000
File: C:\Program Files\NetIQ\SecureLogin\EventLogger.dll, Version: 8.0.3.0, Size: 437944
File: C:\Program Files\NetIQ\SecureLogin\EventLogger64.dll, Version: 8.0.3.0, Size: 647352
File: C:\Program Files\NetIQ\SecureLogin\EventMessages.dll, Version: 8.0.3.0, Size: 81592
File: C:\Program Files\NetIQ\SecureLogin\iesso.dll, Version: 8.0.3.0, Size: 2010808
File: C:\Program Files\NetIQ\SecureLogin\iesso64.dll, Version: 8.0.3.0, Size: 3614392
File: C:\Program Files\NetIQ\SecureLogin\Interop.COMBROKERLib.dll, Version: 8.0.3.31, Size: 40632
File: C:\Program Files\NetIQ\SecureLogin\jaccess.jar, Version: Not Set, Size: 43224
File: C:\Program Files\NetIQ\SecureLogin\javasso.jar, Version: Not Set, Size: 448707
File: C:\Program Files\NetIQ\SecureLogin\LDAPSDK.dll, Version: 3.5.2, Size: 350168
File: C:\Program Files\NetIQ\SecureLogin\LDAPSSL.dll, Version: 3.5.1, Size: 953816
File: C:\Program Files\NetIQ\SecureLogin\localhero.dll, Version: 8.0.3.0, Size: 2846392
File: C:\Program Files\NetIQ\SecureLogin\loginwatch.exe, Version: 8.0.3.0, Size: 503480
File: C:\Program Files\NetIQ\SecureLogin\loginwatch64.exe, Version: 8.0.3.0, Size: 563896
File: C:\Program Files\NetIQ\SecureLogin\nrmonitor.dll, Version: 8.0.3.0, Size: 65208
File: C:\Program Files\NetIQ\SecureLogin\Pathan.dll, Version: Not Set, Size: 454656
File: C:\Program Files\NetIQ\SecureLogin\Pathan64.dll, Version: Not Set, Size: 519680
File: C:\Program Files\NetIQ\SecureLogin\pbscrpt.dll, Version: 8.0.3.0, Size: 646840
File: C:\Program Files\NetIQ\SecureLogin\renNLDAPlgn.exe, Version: 8.0.0.217, Size: 53944
File: C:\Program Files\NetIQ\SecureLogin\scptedit2.dll, Version: 8.0.3.0, Size: 2244280
File: C:\Program Files\NetIQ\SecureLogin\SecureLogin.chm, Version: Not Set, Size: 231950
File: C:\Program Files\NetIQ\SecureLogin\slapi.dll, Version: 8.0.3.0, Size: 183992
File: C:\Program Files\NetIQ\SecureLogin\slapi64.dll, Version: 8.0.3.0, Size: 250040
File: C:\Program Files\NetIQ\SecureLogin\slbroker.dll, Version: 8.0.3.0, Size: 241336
File: C:\Program Files\NetIQ\SecureLogin\slbroker64.dll, Version: 8.0.3.0, Size: 336056
File: C:\Program Files\NetIQ\SecureLogin\slbroker64.exe, Version: 8.0.3.0, Size: 5699768
File: C:\Program Files\NetIQ\SecureLogin\slcaptain.dll, Version: 8.0.3.0, Size: 151224
File: C:\Program Files\NetIQ\SecureLogin\slcaptain64.dll, Version: 8.0.3.0, Size: 207544
File: C:\Program Files\NetIQ\SecureLogin\slcredman.dll, Version: 8.0.1.0 FTF not for production use, Size: 204800
File: C:\Program Files\NetIQ\SecureLogin\slcredman64.dll, Version: 8.0.3.0, Size: 302776
File: C:\Program Files\NetIQ\SecureLogin\sldotnetsso.exe, Version: 8.0.3.31, Size: 495288
File: C:\Program Files\NetIQ\SecureLogin\sldotnetsso.exe.config, Version: Not Set, Size: 268
File: C:\Program Files\NetIQ\SecureLogin\sldotnetsso64.exe, Version: 8.0.3.31, Size: 491192
File: C:\Program Files\NetIQ\SecureLogin\sldotnetsso64.exe.config, Version: Not Set, Size: 268
File: C:\Program Files\NetIQ\SecureLogin\slGUICommon.dll, Version: 8.0.3.0, Size: 724664
File: C:\Program Files\NetIQ\SecureLogin\slimport.dll, Version: 8.0.3.0, Size: 2084536
File: C:\Program Files\NetIQ\SecureLogin\sljava.dll, Version: 8.0.3.0, Size: 1310392
File: C:\Program Files\NetIQ\SecureLogin\sljava64.dll, Version: 8.0.3.0, Size: 2386616
File: C:\Program Files\NetIQ\SecureLogin\slmadgear.dll, Version: 8.0.3.0, Size: 130744
File: C:\Program Files\NetIQ\SecureLogin\slmadgear64.dll, Version: 8.0.3.0, Size: 175800
File: C:\Program Files\NetIQ\SecureLogin\slNRMonitorServer.exe, Version: 8.0.3.0, Size: 495288
File: C:\Program Files\NetIQ\SecureLogin\slproto.exe, Version: 8.0.3.0, Size: 1834680
File: C:\Program Files\NetIQ\SecureLogin\sltoken.dll, Version: 8.0.3.0, Size: 265912
File: C:\Program Files\NetIQ\SecureLogin\sltoken64.dll, Version: 8.0.3.0, Size: 357560
File: C:\Program Files\NetIQ\SecureLogin\slwinsso.exe, Version: 8.0.3.0, Size: 483000
File: C:\Program Files\NetIQ\SecureLogin\slwinsso64.exe, Version: 8.0.3.0, Size: 522936
File: C:\Program Files\NetIQ\SecureLogin\slwizard.dll, Version: 8.0.3.0, Size: 1900216
File: C:\Program Files\NetIQ\SecureLogin\slwizardhook.dll, Version: 8.0.3.0, Size: 855736

File: C:\Program Files\NetIQ\SecureLogin\slwizardhook64.dll, Version: 8.0.3.0, Size: 1562808
File: C:\Program Files\NetIQ\SecureLogin\slwxbase.dll, Version: 8.0.3.0, Size: 138936
File: C:\Program Files\NetIQ\SecureLogin\SSManager.exe, Version: 3.4.2.1.4, Size: 1331200
File: C:\Program Files\NetIQ\SecureLogin\ssoext.dll, Version: 8.0.3.0, Size: 130744
File: C:\Program Files\NetIQ\SecureLogin\TLaunch.exe, Version: 8.0.3.0, Size: 1064632
File: C:\Program Files\NetIQ\SecureLogin\tlaunch.ico, Version: Not Set, Size: 766
File: C:\Program Files\NetIQ\SecureLogin\tlaunch.ini, Version: Not Set, Size: 7875
File: C:\Program Files\NetIQ\SecureLogin\TLaunch64.exe, Version: 8.0.3.0, Size: 1948344
File: C:\Program Files\NetIQ\SecureLogin\tlaunch64.ini, Version: Not Set, Size: 7566
File: C:\Program Files\NetIQ\SecureLogin\transform.dat, Version: Not Set, Size: 20319
File: C:\Program Files\NetIQ\SecureLogin\ttermpro.exe, Version: 8.0.3.0, Size: 478904
File: C:\Program Files\NetIQ\SecureLogin\ttermpro64.exe, Version: 8.0.3.0, Size: 520888
File: C:\Program Files\NetIQ\SecureLogin\winsso.dll, Version: 8.0.3.0, Size: 1138360
File: C:\Program Files\NetIQ\SecureLogin\winsso64.dll, Version: 8.0.3.0, Size: 1921720
File: C:\Program Files\NetIQ\SecureLogin\wintool.exe, Version: 8.0.3.0, Size: 532152
File: C:\Program Files\NetIQ\SecureLogin\wintool64.exe, Version: 8.0.3.0, Size: 604856
File: C:\Program Files\NetIQ\SecureLogin\wizard.xsd, Version: Not Set, Size: 22409
File: C:\Program Files\NetIQ\SecureLogin\wxbase28u_vc_AI.dll, Version: wxWidgets Library 2.8.7, Size: 1302528
File: C:\Program Files\NetIQ\SecureLogin\wxmsw28u_adv_vc_AI.dll, Version: wxWidgets Library 2.8.7, Size: 712704
File: C:\Program Files\NetIQ\SecureLogin\wxmsw28u_core_vc_AI.dll, Version: wxWidgets Library 2.8.7, Size: 3080192
File: C:\Program Files\NetIQ\SecureLogin\wxmsw28u_html_vc_AI.dll, Version: wxWidgets Library 2.8.7, Size: 507904
File: C:\Program Files\NetIQ\SecureLogin\wxmsw28u_stc_vc_AI.dll, Version: wxWidgets Library 2.8.7, Size: 548864
File: C:\Program Files\NetIQ\SecureLogin\wxmsw290u_propgrid_vc_AI.dll, Version: wxWidgets Library 2.8.7, Size: 552960
File: C:\Program Files\NetIQ\SecureLogin\Xalan-C_1_10.dll, Version: 1, 10, 0, 0, Size: 1818624
File: C:\Program Files\NetIQ\SecureLogin\Xalan-C_1_1064.dll, Version: 1, 10, 0, 0, Size: 2944000
File: C:\Program Files\NetIQ\SecureLogin\XalanMessages_1_10.dll, Version: Not Set, Size: 40960
File: C:\Program Files\NetIQ\SecureLogin\XalanMessages_1_1064.dll, Version: Not Set, Size: 43008
File: C:\Program Files\NetIQ\SecureLogin\xbean.jar, Version: Not Set, Size: 1950111
File: C:\Program Files\NetIQ\SecureLogin\xerces-c_2_7.dll, Version: 2, 7, 0, Size: 1888256
File: C:\Program Files\NetIQ\SecureLogin\xerces-c_2_7_64.dll, Version: 2, 7, 0, Size: 2713088
File: C:\Program Files\NetIQ\SecureLogin\xercesImpl.jar, Version: Not Set, Size: 1010675
File: C:\Program Files\NetIQ\SecureLogin\xml-apis.jar, Version: Not Set, Size: 109318
File: C:\Program Files\NetIQ\SecureLogin\xsec_1_1_0.dll, Version: 0, 1, 1, 0, Size: 421888
File: C:\Program Files\NetIQ\SecureLogin\xsec_1_2_064.dll, Version: 0, 1, 2, 0, Size: 556032
File: C:\Program Files\NetIQ\SecureLogin\xsldll.dll, Version: 8.0.3.0, Size: 147128
File: C:\Program Files\NetIQ\SecureLogin\xsldll64.dll, Version: 8.0.3.0, Size: 203960

##########
NSL Processes
##########
Checking NSL processes.
NSL client is running
slwinsso is running
slbroker64 is running
slwinsso64 is running
Remote service monitoring is enabled. slNRMonitorServer is running.
Published application monitoring is not enabled. slwts is not running.
Depreciated published application trigger is not enabled. sllauncher is not being used.

##########
Primary NSL mode
##########
Checking NSL client configuration:
SecureLogin mode:
Primary: Stand Alone

##########
Secondary NSL mode
##########
Secondary: FILE
Cache file found: C:\Users\Greg\AppData\Local\SecureLogin\Cache\V3SLC\Greg.cache

##########
NSL diagnostics
##########
Communicating with SecureLogin client for realtime statistics.

Securelogin is online
SecureLogin client is active
Using offline cache
NSL Database version: 3.5 / 5.5
Current NSL User: Greg
Warning: No passphrase found. This is normal if you are not logged into the directory.
Current NSL User Passphrase Question:

GINA credentials exist.
GINA credentials are valid.
########################
NSL Preferences
########################
WinSSOActive: Enabled - From object: Greg
IESSOActive: Enabled - From object: Greg
EnableLogging: Disabled - From object: Greg
WinSSOPasswordDetect: Disabled - From object: Greg
DisplayPasswords: Enabled - From object: Greg
WebSSOPasswordDetect: Disabled - From object: Greg
UseCacheFiles: Enabled - From object: Greg
RequireProtoPassword: Disabled - From object: Greg
StopWalkingHere: Enabled - From object: Greg
JavaEnableSSO: Enabled - From object: Greg
JavaEnableAddPrompt: Disabled - From object: Greg
AllowAPIAccess: Enabled - From object: Greg
AllowedAPILicenceKeys: Disabled - From object:
SSODatastoreVersion: 6.0
StopWalkingHere: Enabled
AllowedAPILicenceKeys: Disabled
AppliedSSODataStoreVersion: 6

########################
NSL applications
########################

Web applications

Application: 1. /IC
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = False
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = Preference not set. Using default.
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
Password
Username
SLDescription

Credentials linked to this application:
Value: /IC
Target Value: /IC

Application: 2. aol.com
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = False
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.

AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = Preference not set. Using default.
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
Password
Username
SLDescription

Credentials linked to this application:
Value: aol.com
Target Value: aol.com

Windows applications

Application: 1. tn5250
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = False
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = True
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = Preference not set. Using default.
PromptForReauthentication = False
ReauthenticationMethod = False

Variables used by this application:
No entries found.

Credentials linked to this application:
No entries found.

Application: 2. vs.exe
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = False
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = Preference not set. Using default.
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
No entries found.

Credentials linked to this application:
No entries found.

Terminal_Emulator applications

Application: 1. test
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = False
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.

IEParallelExecution = Preference not set. Using default.
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
No entries found.

Credentials linked to this application:
No entries found.

Application: 2. Runas
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = Preference not set. Using default.
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = Preference not set. Using default.
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
No entries found.

Credentials linked to this application:
No entries found.

Win32_Daemon applications
No applications defined for this type.

Mainframe_Daemon applications
No applications defined for this type.

SSO_Notes applications
No applications defined for this type.

Password_Policy applications

Application: 1. NDSPasswordPolicy
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = Preference not set. Using default.
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = Preference not set. Using default.
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
No entries found.

Credentials linked to this application:
No entries found.

Startup applications

Application: 1. XStartupScript
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = Preference not set. Using default.

ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = False
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = Preference not set. Using default.
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
No entries found.

Credentials linked to this application:
No entries found.

Application: 2. backup user data
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = Preference not set. Using default.
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = False
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = Preference not set. Using default.
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
No entries found.

Credentials linked to this application:
No entries found.

Java applications

Application: 1. altar.term
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = False
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = Preference not set. Using default.
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
password
username
SLDescription

Credentials linked to this application:
Value: altar.term
Target Value: altar.term

Application: 2. com.test.main
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = Preference not set. Using default.
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = False
AllowAPIAccessToPlatform = Preference not set. Using default.

SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = Preference not set. Using default.
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
Password
Username

Credentials linked to this application:
Value: com.test.main
Target Value: com.test.main

Generic applications
No applications defined for this type.

Advanced_Web applications

Application: 1. provo.novell.com
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = False
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = True
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
No entries found.

Credentials linked to this application:
Value: provo.novell.com
Target Value: innerweb.novell.com

Application: 2. siebelprd.innerweb.novell.com
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = False
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = False
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = True
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
No entries found.

Credentials linked to this application:
No entries found.

Web_Wizard_Script applications

Application: 1. adp.com
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = False
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.

AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = True
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
No entries found.

Credentials linked to this application:
Value: adp.com
Target Value: WebRH

Application: 2. basf.com
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = False
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = True
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
No entries found.

Credentials linked to this application:
Value: basf.com
Target Value: basf.com #1
Value: basf.com
Target Value: basf.com #2

Web_Wizard applications

Application: 1. 1.215
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = False
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = True
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
No entries found.

Credentials linked to this application:
Value: 1.215
Target Value: 1.215 #1

Application: 2. 76.104

Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = Preference not set. Using default.
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.
AllowAPIAccessToPlatform = Preference not set. Using default.

SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = True
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
No entries found.

Credentials linked to this application:
Value: 76.104
Target Value: 76.104 #1

Generic_Wizard_Windows applications

Application: 1. SLAnalyzer
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = False
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = Preference not set. Using default.
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
password
username

Credentials linked to this application:
Value: SLAnalyzer
Target Value: SLAnalyzer

Application: 2. Extranet.exe
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = False
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = Preference not set. Using default.
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
No entries found.

Credentials linked to this application:
No entries found.

Generic_Wizard_Java applications
No applications defined for this type.

Generic_Wizard_Web applications

Application: 1. gmorlpt
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = False
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.

AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = True
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
No entries found.

Credentials linked to this application:
No entries found.

Application: 2. login.hema
Script Preferences:
UseEnhancedProtection = Preference not set. Using default.
IEPasswordFieldMustExist = Preference not set. Using default.
PlatformDescription = False
ShowInAppLauncher = Preference not set. Using default.
ScriptEnabled = Preference not set. Using default.
AllowAPIAccessToPlatform = Preference not set. Using default.
SyncPlatFormToHandHeldDevice = Preference not set. Using default.
IEParallelExecution = True
PromptForReauthentication = Preference not set. Using default.
ReauthenticationMethod = Preference not set. Using default.

Variables used by this application:
password
username
SLDescription

Credentials linked to this application:
Value: login.hema
Target Value: login.hema

Generic_Wizard_T applications
No applications defined for this type.

########################
NSL Logins
########################
Logins defined:
Login: 1. MS FTP
Login: 2. /IC
Login: 3. axs
Login: 4. OGE

########################
NSL Credential Sets
########################
Normal Credential Sets defined:
Credential: 1. /IC
Credential: 2. WebRH
Credential: 3. MS FTP
Credential: 4. upc.nl
Credential: 5. VW.EXE

SetPlat Credential Sets defined:
SetPlat CredSet: 1. WebRH
SetPlat CredSet: 2. 1.215 #1
SetPlat CredSet: 3. 76.104 #1
SetPlat CredSet: 4. 77.141 #1

Total Number of Credentials: 227

########################
Corporate Redirection Information

########################
########################
DotNet
########################
Support for DotNet applications is enabled.
sldotnetsso64 is running

########################
Flash
########################
Support for Flash/Flex applications is enabled.

########################
JAVA runtime environment
########################
Support for Java applications is enabled.
JRE found at: C:\Program Files (x86)\Java\jre1.6.0_03

Validating proper JRE configuration.

JAVA Properties found:
C:\Program Files (x86)\Java\jre1.6.0_03\lib\accessibility.properties
#Wed Jul 22 14:53:46 CDT 2015
assistive_technologies=com.actividentity.sso.javasso.awt_swing.JavaSSOHook

C:\Program Files (x86)\Java\jre1.6.0_03\lib\awt.properties
#Wed Jul 22 14:53:46 CDT 2015
AWT.EventQueueClass=com.sun.java.accessibility.util.EventQueueMonitor
AWT.assistive_technologies=com.actividentity.sso.javasso.awt_swing.JavaSSOHook

SecureLogin JAVA libraries found:
C:\Program Files (x86)\Java\jre1.6.0_03\lib\ext\jaccess.jar
C:\Program Files (x86)\Java\jre1.6.0_03\lib\ext\javasso.jar
C:\Program Files (x86)\Java\jre1.6.0_03\lib\ext\xbean.jar

##
End of Report.
##

Sample Installation report (SecureLogin)

Report generated by: SLAnalyzer Version 3.0.0.0

######################
SecureLogin Installation Logs
######################

Contents of installation log (log.txt)

Product Version is 8.0.3.0
Destination Folder: C:\Program Files\NetIQ\SecureLogin\
Cache Folder: %LOCALAPPDATA%
Protocol for eDir: NA
LDAP mode selected: NA
LDAP credential association: NONE
LDAP server address: LDAP server address
LDAP port: 636
SecretStore client selected: 0
NMAS client selected: 0
GPO selected: No
PCPROX method selected: 0
Post Login Method Secure WorkStation selected: 0
Smartcard selected: No
Smatcard dll: NA
CSP: Microsoft Smart Card Key Storage Provider
Terminal Server installed: No
Novell Client Installed: No
Citrix Server installed: No
NICI installed: No
FireFox not present
Run NSL at startup : No
Install Admin Tools: No
Install Citrix: No
Install Secureworkstation: No
Install Desktop Automation Services: No
Windows Build: No
Service Pack level: 1
VersionNT: 601

Contents of response file (responsefile.ini)

INSTALLDIR=C:\Program Files\NetIQ\SecureLogin\
X_CACHEDIR=%LOCALAPPDATA%
X_PRIMARYSTORE=DUMMY
X_NONEDIRLDAP=No
ADDLOCAL=Help,FileExtension,SeamlessMAD,WinSSO,JavaSSO,TermSSO,IESSO,FireFoxSSO,DotNetSSO,FlashSSO,RunAtStartup,Desktop,CredSto
re,DirectorySignon,SSOAut,ReadMe,PrimaryStore,WindowsEventLog,Auditing
LDAPSERVERADDRESS=LDAP server address
LDAPPORT=636
LDAPSERVERADDRESS=LDAP server address
LDAPPORT=636
LDAPSERVERADDRESS1=
LDAPPORT1=636
LDAPSERVERADDRESS2=
LDAPPORT2=
X_SMARTCARDLIB=
X_CSP=Microsoft Smart Card Key Storage Provider
X_STOREONCARD=
EA_FAILRETRIES=3
EA_LOCKTIMEOUT=30
EA_SSPRURL=
EA_REQTIMEOUT=300
LOCATIONFORXML=
DASSERVER=
DASCONFIGOBJECT=

READERPORT=-1
CARDREADER=
AIRID=0
RETRIES=0
TREE=
SERVER=
SEQUENCE=
LDAPSERVER=
ALTERNATE1=
ALTERNATE2=
X_SYSLOGSERVERURI=
X_SYSLOGLANGUAGEID=#1033

##
End of Report.
##

Sample Tlaunch report

Report generated by: SLAnalyzer Version 3.0.0.0

```
########################
Processing Tlaunch.ini.
########################
[Eicon Aviva]
TerminalType=WinHLLAPI
HllapiDLLName=C:\Program Files\Eicon\Aviva\whllapi.dll
HllapiFunctionName=WinHLLAPI
HomeDirectory=C:\Program Files\Eicon\Aviva
EmulatorPath=C:\Program Files\Eicon\Aviva\app32d.exe
SessionFile01=C:\Program Files\EICON\Aviva\Administrator\Mainframe Session.a3d
SessionFile02=C:\Program Files\Eicon\Aviva\Administrator\Session2.a3d
Attempting analysis on WINHLLAPI interface.
Warning: Emulator executable not found. Skipping analysis.
[WRQ Reflection]
TerminalType=HLLAPI
HllapiDLLName=C:\temp\zHllap32.dll
HllapiFunctionName=hllapi
HomeDirectory=C:\Program Files\Reflection
EmulatorPath=C:\Program Files\Novell\SecureLogin\tlaunch.exe
SessionFile01=C:\WinNT\profiles\administrator\personal\reflection\session1.rsf
Attempting analysis on HLLAPI interface.
Emulator executable found.
HLLAPI DLL found.
Warning: SLAnalyzer cannot validate 32 bit emulator library when ran on a 64 bit workstation.
To properly analyze a 32 bit emulator library you must run SLAnalyzer from a 32 bit workstation.

########################
Processing Tlaunch64.ini.
########################
[Eicon Aviva]
TerminalType=WinHLLAPI
HllapiDLLName=C:\Program Files\Eicon\Aviva\whllapi.dll
HllapiFunctionName=WinHLLAPI
HomeDirectory=C:\Program Files\Eicon\Aviva
EmulatorPath=C:\Program Files\Eicon\Aviva\app32d.exe
SessionFile01=C:\Program Files\EICON\Aviva\Administrator\Mainframe Session.a3d
SessionFile02=C:\Program Files\Eicon\Aviva\Administrator\Session2.a3d
Attempting analysis on WINHLLAPI interface.
Warning: Emulator executable not found. Skipping analysis.
[WRQ Reflection]
TerminalType=HLLAPI
HllapiDLLName=C:\Windows\System32\ncpwin32.dll
HllapiFunctionName=NWNCPInit
HomeDirectory=C:\Program Files\Reflection
EmulatorPath=C:\Program Files\Novell\SecureLogin\tlaunch64.exe
SessionFile01=C:\WinNT\profiles\administrator\personal\reflection\session1.rsf
Attempting analysis on HLLAPI interface.
Emulator executable found.
HLLAPI DLL found.
Processing 64 bit library on 64 bit operating system.
Successfully loaded HLLAPI DLL: C:\Windows\System32\ncpwin32.dll
Found DLL entry point - NWNCPInit in library - C:\Windows\System32\ncpwin32.dll
Emulator configuration analysis completed successfully.

########################################
End of Report.
########################################
```

Sample eDirectory with Novell Client report

Report generated by: SLAnalyzer Version 3.0.0.0

########################
SLP Information
########################

Novell Client Service Location Diagnostic Utility
SLPInfo 5.0.63.5695

============ Directory Agents ============
DA IP Address Host Name
[0] Performing SLP Directory Agent discovery...

=============== Scope List ===============
[0] Performing SLP Directory Agent and scope discovery...

DEFAULT

================= Trees ==================
Tree Name IP Address
[0] Performing discovery of eDirectory trees...
[1] Performing discovery of eDirectory trees...

OESTREE 192.168.1.243

================ Servers =================
Server Name IP Address
[0] Performing discovery of NCP servers...
[1] Performing discovery of NCP servers...

linux-61w4 192.168.1.243

########################
eDirectory
########################

NCP Connection established.
Successfully connected to eDirectory
Successfully obtained Primary NCP connection.
Successfully opened connection reference.
eDirectory connection established.

Connected to server as user: CN=admin
Connected to server: CN=GMORRISVM65
User object's parent container: O=novell.

Allocated memory to read attribute data.
Allocated memory to store attribute names.
Initialized allocated memory to store attribute names.

Successfull read of attribute names.
Successfully read 33 attributes.
Attributes defined on user object:

Attribute: ACL
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: CN
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: Group Membership
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: Login Script

Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: Login Time
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: Network Address
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: Object Class
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: Public Key
Effective Rights: [Create,Read,]
Attribute: Security Equals
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: Surname
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: Message Server
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: Language
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: Last Login Time
Effective Rights: [Create,Read,]
Attribute: Full Name
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: Revision
Effective Rights: [Create,Read,]
Attribute: Given Name
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: Equivalent To Me
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: Used By
Effective Rights: [Create,Read,]
Attribute: GUID
Effective Rights: [Create,Read,]
Attribute: uniqueID
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: modifiersName
Effective Rights: [Create,Read,]
Attribute: userCertificate
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
Attribute: NDSPKI:userCertificateInfo
Effective Rights: [Create,Read,Write,Add Self,Supervisor]
##
End of Report.
##

Sample LDAP report

Report generated by: SLAnalyzer Version 3.0.0.0

########################
LDAP
########################

Primary: LDAP Directory
Validating LDAP information:
Primary LDAP server: 192.168.1.242
Primary LDAP server port: 636
SSL Certificate File: C:\Program Files\NetIQ\SecureLogin\rootcert.der

Testing Primary LDAP connection.
LDAP User: cn=admin,o=novell

Attributes found on object:
rbsownedcollections2
ndspkiusercertificateinfo
protocom-sso-security-prefs-checksum
equivalenttome
protocom-sso-entries
sn
cn
loginscript
securityequals
nrdregistrydata
protocom-sso-security-prefs
protocom-sso-entries-checksum
objectclass
messageserver
language
acl
groupmembership
usercertificate;binary
protocom-sso-auth-data
logintime
fullname
nrdregistryindex
uid
rbsassignedroles2
givenname

Secondary LDAP server: 192.168.1.242
Secondary LDAP server port: 636

Testing Secondary LDAP connection.
LDAP User: cn=admin,o=novell

Attributes found on object:
rbsownedcollections2
ndspkiusercertificateinfo
protocom-sso-security-prefs-checksum
equivalenttome
protocom-sso-entries
sn
cn
loginscript
securityequals
nrdregistrydata
protocom-sso-security-prefs
protocom-sso-entries-checksum
objectclass
messageserver
language

acl
groupmembership
usercertificate;binary
protocom-sso-auth-data
logintime
fullname
nrdregistryindex
uid
rbsassignedroles2
givenname

##
End of Report.
##

Sample AD report

Report generated by: SLAnalyzer Version 3.0.0.0

########################
Active Directory
########################
MS connection details:
Domain: GMADR2
User: CN=admin.O=novell.T=GMORTREE
Connected to AD as User: Greg Morris

Search for SecureLogin attributes returned the following list:
protocom-sso-auth-data
protocom-sso-entries-checksum
adspath
protocom-sso-entries
##
End of Report.
##

Sample LDAP SecretStore Report

Report generated by: SLAnalyzer Version 3.0.0.0

########################
LDAP SecretStore
########################

Checking Secret Store Services
Analyze SecretStore over LDAP connection.

Secret Store client found:
C:\Program Files\NetIQ\SecureLogin\nssldp.dll
C:\Program Files\NetIQ\SecureLogin\nssncp.dll
C:\Program Files\NetIQ\SecureLogin\nsss.dll

Using user name as defined by SecureLogin - cn=testusergm,o=novell
SecretStore client version - 30405
SecretStore server version - 30402
SecretStore Tree - SWAINTREE
SecretStore Server - 151.155.215.28
SecretStore Port - 636

Number of Secrets - 4
Secrets stored for this user :
gmtestsecret
SS_CredSet:GMAppCred
SS_App:yahoo.com
SS_CredSet:GINACredentials

GINA Credentials:
tree=636
isPin=false
server=151.155.215.28
context=GMORWIN7
password=novell
username=testusergm
SecretStore Connection terminated.

##
End of Report.
##

Sample CLE report

Report generated by: SLAnalyzer Version 3.0.0.0

######################
Client Login Extension
######################
Checking for CLE.

CLE credential provider found.
File: C:\Windows\System32\CLECredentialProvider.dll, Version: 3. 9. 0. 0, Size: 692224
File: C:\Windows\System32\CLECredentialProviderFilter.dll, Version: 3. 9. 0. 0, Size: 260608
File: C:\Windows\System32\CLESelfSvcCredentialProvider.dll, Version: 3. 9. 0. 0, Size: 680448
File: C:\Windows\System32\EACredentialManager.dll, Version: 3.9.0.0, Size: 562176
File: C:\Windows\System32\IDMClientLoginExtensionCustomAction.dll, Version: 3, 8, 1, 0, Size: 117248
File: C:\Windows\System32\NclePwmHelper.dll, Version: 3. 9. 0. 0, Size: 322560
File: C:\Windows\System32\NcleResources.dll, Version: 3. 9. 0. 0, Size: 6656
File: C:\Windows\System32\NCLoginExtension.dll, Version: 3, 8, 0, 0, Size: 82432
File: C:\Windows\System32\RestrictedBrowserDLL.dll, Version: 3. 9. 0. 0, Size: 2726400
File: C:\Windows\System32\RestrictedBrowserEXE.exe, Version: 3. 9. 0. 0, Size: 125440

Emergency Access path is C:\Program Files\NCLE\EmergencyAccess\
Emergency Access files found:
File: C:\Program Files\NCLE\EmergencyAccess\slEmergencyAccess.dll, Version: 3.9.0.0, Size: 596480
File: C:\Program Files\NCLE\EmergencyAccess\slEmergencyAccess.dll.new, Version: 3.8.1.0, Size: 597504
File: C:\Program Files\NCLE\EmergencyAccess\slEmergencyAccessLocalization.dll, Version: 3.9.0.0, Size: 5632
File: C:\Program Files\NCLE\EmergencyAccess\slEmergencyAccessMonitor.exe, Version: 3.9.0.0, Size: 156160
File: C:\Program Files\NCLE\EmergencyAccess\slEmergencyAccessTray.exe, Version: 3.9.0.0, Size: 161280

Found CLE Auth Provider: CLESelfSvcCredentialProvider
Found CLE Auth Provider: CLECredentialProvider

Emerency Access is enabled.
Emerency Access is registered as a network provider.

Testing Emergency Access cache file creation with encryption.
Creating file: C:\Users\GREG~2.GMA\AppData\Local\Temp\SLAnalyzer\test.xml
File: C:\Users\GREG~2.GMA\AppData\Local\Temp\SLAnalyzer\test.xml was successfully created
File: C:\Users\GREG~2.GMA\AppData\Local\Temp\SLAnalyzer\test.xml was closed successfully
File: C:\Users\GREG~2.GMA\AppData\Local\Temp\SLAnalyzer\test.xml was encrypted successfully
File: C:\Users\GREG~2.GMA\AppData\Local\Temp\SLAnalyzer\test.xml was decrypted successfully
File: C:\Users\GREG~2.GMA\AppData\Local\Temp\SLAnalyzer\test.xml was deleted successfully
CLE Emergency Access encrypted file test completed successfully

Version of IE being utilized is: 11.0.9600.18098

Local host name: WIN7VM
CLE URI Server Address: 192.168.1.238
Attempting to contact URI at: https://sspr.gmadr2.novell.com:8443/sspr/public/ForgottenPassword

Certificate name: CN=sspr.gmadr2.novell.com, OU=sspr, O=support, C=NetIQ
Certificate serial number: 34DF2278
Certificate valid from: 11/23/2015 2:57:17 PM until 2/21/2016 2:57:17 PM
Success: SSL Connection state shows no errors

Local IP Address: 192.168.3.138
Local TCP Port: 49642

Remote IP Address: 192.168.1.238
Remote TCP Port: 8443

Certificate name: CN=sspr.gmadr2.novell.com, OU=sspr, O=support, C=NetIQ
Certificate serial number: 34DF2278
Certificate valid from: 11/23/2015 2:57:17 PM until 2/21/2016 2:57:17 PM
Success: SSL Connection state shows no errors

Local IP Address: 192.168.3.138
Local TCP Port: 49643

Remote IP Address: 192.168.1.238
Remote TCP Port: 8443

Success: Browser operation succeeded.

########################
REST
########################
Checking for REST API.

Rest URL is defined in the registry as: https://sspr.gmadr2.novell.com:8443/sspr/public/rest

Checking server health by submitting the following Rest Command:
https://sspr.gmadr2.novell.com:8443/sspr/public/rest/health

Certificate name: CN=sspr.gmadr2.novell.com, OU=sspr, O=support, C=NetIQ
Certificate serial number: 34DF2278
Certificate valid from: 11/23/2015 2:57:17 PM until 2/21/2016 2:57:17 PM
Success: SSL Connection state shows no errors
HTTP Status code: OK

Server Response:
{"error":false
"errorCode":0
"data":{"timestamp":"2015-12-10T22:04:54Z"
"overall":"CONFIG"
"records":[{"status":"CONFIG"
"topic":"Configuration"
"detail":"AppProperty ⇨ ldap.promiscuousEnable setting should be set to false for proper security"}
{"status":"CONFIG"
"topic":"Configuration"
"detail":"LDAP ⇨ LDAP Directories ⇨ default ⇨ LDAP Proxy Password strength of password is weak (33/100); increase password length/complexity for proper security"}
{"status":"CONFIG"
"topic":"Configuration"
"detail":"Settings ⇨ Security ⇨ Web Security ⇨ Require HTTPS setting should be set to true for proper security"}
{"status":"GOOD"
"topic":"LDAP"
"detail":"All configured LDAP servers are reachable"}
{"status":"GOOD"
"topic":"LDAP"
"detail":"LDAP test user account is functioning normally for profile default"}
{"status":"GOOD"
"topic":"LocalDB"
"detail":"LocalDB and related services are operating correctly"}
{"status":"GOOD"
"topic":"Platform"
"detail":"Java platform is operating normally"}]}}

Getting server statistics by submitting the following Rest Command:
https://sspr.gmadr2.novell.com:8443/sspr/public/rest/statistics

HTTP Status code: No Content

Server Response:

Getting challenge questions by submitting the following Rest Command:
https://sspr.gmadr2.novell.com:8443/sspr/public/rest/challenges

Certificate name: CN=sspr.gmadr2.novell.com, OU=sspr, O=support, C=NetIQ
Certificate serial number: 34DF2278

Certificate valid from: 11/23/2015 2:57:17 PM until 2/21/2016 2:57:17 PM
Success: SSL Connection state shows no errors
HTTP Status code: OK

Server Response:
{"error":false
"errorCode":0
"data":{"username":"default"
"challenges":[{"challengeText":"What is the name of your favorite teacher?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":0
"enforceWordlist":false}
{"challengeText":"What is the name of your favorite pet?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":0
"enforceWordlist":false}
{"challengeText":"What was your favorite show as a child?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":0
"enforceWordlist":false}
{"challengeText":"What is your favorite food?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":0
"enforceWordlist":false}
{"challengeText":"What is your favorite team?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":0
"enforceWordlist":false}]
"minimumRandoms":2
"policy":{"challenges":[{"challengeText":"What is the name of the main character in your favorite book?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}
{"challengeText":"What is the name of your favorite teacher?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}
{"challengeText":"What is the name of your favorite pet?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}
{"challengeText":"What was the name of your childhood best friend?"

"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}
{"challengeText":"What was your favorite show as a child?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}
{"challengeText":"Who is your favorite author?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}
{"challengeText":"What is your favorite food?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}
{"challengeText":"What is your partner's nickname?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}
{"challengeText":"What is your favorite team?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}
{"challengeText":"What street did you grow up on?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}
{"challengeText":"What city / town were you born in?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}
{"challengeText":"What is your favorite vehicle?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}
{"challengeText":"If you could meet someone from history
who would it be?"
"minLength":4
"maxLength":200

"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}
{"challengeText":"What is your least favorite film of all time?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}
{"challengeText":"Who was your least favorite teacher?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}
{"challengeText":"What food do you dislike the most?"
"minLength":4
"maxLength":200
"adminDefined":true
"required":false
"maxQuestionCharsInAnswer":3
"enforceWordlist":true}]
"minimumRandoms":2}}}

Getting user status by submitting the following Rest Command:
https://sspr.gmadr2.novell.com:8443/sspr/public/rest/status

HTTP Status code: OK

Server Response:
{"error":false
"errorCode":0
"data":{"userDN":"CN=Administrator
cn=users
dc=gmadr2
dc=novell
dc=com"
"ldapProfile":"default"
"userID":"Administrator"
"userEmailAddress":"testuser@gmail.com"
"passwordExpirationTime":"2015-11-23T19:03:45Z"
"passwordLastModifiedTime":"2015-10-12T19:03:45Z"
"requiresNewPassword":true
"requiresResponseConfig":false
"requiresUpdateProfile":false
"requiresInteraction":true
"passwordStatus":{"expired":true
"preExpired":true
"violatesPolicy":false
"warnPeriod":false}
"passwordPolicy":{"DisallowCurrent":"true"
"MinimumNumeric":"0"
"AllowNumeric":"true"
"MaximumSpecial":"0"
"AllowLastCharSpecial":"true"
"CharGroupsValues":".*[0-9]\n.*[^A-Za-z0-9]\n.*[A-Z]\n.*[a-z]"
"MinimumLength":"5"
"EnforceAtLogin":"false"
"AllowFirstCharNumeric":"true"
"MaximumUpperCase":"0"
"MinimumLowerCase":"0"
"UniqueRequired":"false"
"AllowAdminChange":"true"

"PolicyEnabled":"true"
"ADComplexityMaxViolations":"2"
"MaximumLength":"64"
"DisallowedValues":"password\ntest\n+"
"MinimumUnique":"0"
"MinimumLifetime":"0"
"CaseSensitive":"true"
"MaximumUnique":"0"
"AllowLastCharNumeric":"true"
"RegExNoMatch":""
"RegExMatch":""
"ExpirationInterval":"0"
"AllowFirstCharSpecial":"true"
"MinimumSpecial":"0"
"MaximumSequentialRepeat":"0"
"MinimumUpperCase":"0"
"EnableWordlist":"true"
"MaximumRepeat":"0"
"DisallowedAttributes":"givenName\ncn\nsn"
"MaximumLowerCase":"0"
"ChangeMessage":""
"AllowUserChange":"true"
"MaximumNumeric":"0"
"AllowSpecial":"true"
"ChallengeResponseEnabled":"false"}
"passwordRules":["Password is case sensitive."
"Must be at least 5 character long."
"Must not include any of the following values: password test +"
"Must not include part of your name or username."
"Must not include a common word or commonly used sequence of characters."]}}

##########
Keys Defined in: HKEY_CURRENT_USER\SOFTWARE\Protocom\SecureLogin
##########

Key: OfflineWarningSuppressed
Type: DWord
Enable/Disable the warning message when logging in the workstation in offline mode.

Value defined in registry: 1

Key: MainGUIRect
Type: String

Value defined in registry: 370,180,700,500,1

Key: LastNDSUser
Type: String
Last NDS user that SecureLogin successfully connected to eDirectory with.

Value Data Type: REG_SZ
Help/Comment: Represented in the dot format. IE admin.novell

Value defined in registry: CN=admin.O=novell.T=GMORTREE

Key: LastCacheUser
Type: String
Last user that successfully loaded from cache file.

Value defined in registry: CN=admin.O=novell.T=GMORTREE

Key: DisplayInitialLoadSplash
Type: DWord
Disables the SecureLogin splash screen at startup

* Available in 6.1 and onwards
* This key is created by default and linked to the preference: 'Display splash screen on start up'

Value	Description
1	Default setting: Display SecureLogin splash screen at startup
0	Disable SecureLogin splash screen at startup

Value defined in registry: 1

##########
Keys Defined in: HKEY_LOCAL_MACHINE\SOFTWARE\Novell\MsPssGina
##########

Key: SelfSvcCredProv
Type: DWord
Dword value enabling the CLE tile feature. CLE logins combined into a single CLE login tile.

0 - Disabled
1 - Enabled

Value defined in registry: 0

Key: SASChangePassword
Type: DWord
Dword value to enable the change password with CLE/SSPR feature when the user presses Alt-Ctl-Del.

1 - Enable
0 - Disable

Value defined in registry: 1

Key: LinkURL
Type: String
Specify the URL that the Client Login Extension - restricted browser uses to connect to the User Application Forgotten Password page. You can use either a DNS name or an IP address. An example of a URL using a DNS name that links to the Forgotten Password page is: https://<server>:<port>/IDM/jsps/pwdmgt/ForgotPassword.jsp
This URL can also be configured to access the external password WAR. To do this, see Installing the User Application on an Application Server in the NetIQ Identity Manager Setup Guide.

IMPORTANT: You must have a valid URL pointing to the User Application's Forgotten Password page; otherwise, the client connection might fail and you might not be able to log in through the workstation.
To redirect to a local SSPR server use a link similar to https://<DNSName_or_IPAddress>:<Port>/sspr..

IE. https://192.168.1.110:8443/sspr

Value defined in registry: https://sspr.gmadr2.novell.com:8443/sspr/public/ForgottenPassword
---

Key: LinkText
Type: String
Specify the text to be displayed on the link to the restricted browser that the Client Login Extension uses.
The default text is Forgotten Password. Note that the text for the button in the Novell Client is provided by the Novell Client and cannot be changed here.

Value defined in registry: Forgotten Password

Key: LastLoggedinTime
Type: String

Runtime value indicating the last time the user logged in.

Value defined in registry: 2015:12:10,15:10

Key: EnableIntegration
Type: DWord
This option allows you to enable the challenge response enrollment and password expiration features.

If you select this option, the Force user for challenge response enrollment option and REST URI field are enabled.

NOTE:To enable this feature, you must have already configured SSPR, as described in Section 4.2.1, Configuring SSPR for Enabling Challenge Response Force Enrollment and Section 4.2.2, Configuring SSPR for Enabling Password Expiration Warning.

0 - Disabled
1 - Enabled

Value defined in registry: 1

Key: EmergencyAccess
Type: DWord
Dword value indicating if Emergency Access is enabled.

0 - Disabled
1 - Enabled

Value defined in registry: 1

Key: EAWarnTimeout
Type: DWord
DWord value representing the Warning time. Default is 30 seconds
---
Value defined in registry: 30

Key: EASysLogoutTime
Type: DWord
Dword value representing the Session Time Allowed. Default 30 minutes
---
Value defined in registry: 30

Key: EAMaxRetryCount
Type: DWord
Dword value representing the maximum number of retries.

Value defined in registry: 3

Key: EACRDialogMsg
Type: String
String value of custom message to display to the user when they are prompted for their Challenge Response answers when using Emergency Access.

Value defined in registry: Emergency Access is for temporary use.

Key: EAAdminMessage
Type: String
String value providing the message to display to the user

Value defined in registry: You are using Emergency Access

Key: CustomPlugin
Type: String
String value representing the path and filename of the emergency access dll.

IE. C:\Program Files\NCLE\EmergencyAccess\slEmergencyAccess.dll
---
Value defined in registry: C:\Program Files\NCLE\EmergencyAccess\slEmergencyAccess.dll
---

Key: cleTileLargeText
Type: String
String value representing the text to display with the CLE credential tile.

Value defined in registry:

Key: cleTileBitmapPath
Type: String

Value defined in registry:

Key: ChallengeRespLogonUIMsg
Type: String
This option is enabled only if you select Force user for challenge response enrollment. Specify the message that you want to display when the user is prompted for force enrollment.

Value defined in registry: You must setup your challenge response data
---

##########
Keys Defined in: HKEY_LOCAL_MACHINE\SOFTWARE\Novell\MsPssGina\CPFILTERLIST
##########

##########
Keys Defined in: HKEY_LOCAL_MACHINE\SOFTWARE\Novell\MsPssGina\CPFILTERLIST\{6f45dc1e-5384-457a-bc13-2cd81b0d28ed}
##########

Key: (Default)
Type: String
Value defined in registry: PasswordProvider

##########
Keys Defined in: HKEY_LOCAL_MACHINE\SOFTWARE\Novell\PSS
##########

Key: LogDir
Type: String
Path to create debug log files for CLE. Logfiles will be created with the file names: RestrictedBrowserDLL.log and RestrictedBrowserEXE.log
---
Value defined in registry: C:\NSLFiles\

##########
Keys Defined in: HKEY_LOCAL_MACHINE\SOFTWARE\Novell\RestrictedBrowser
##########

Key: WhiteListURL
Type: String

String value with simicolon seperated list of URLs allowed for restricted browser to access.

Value defined in registry: https://innerweb.novell.com;https://www.google.com
---

Key: RestUri
Type: String
Specify the URI that the Client Login Extension - restricted browser uses to connect to the SSPR server by using rest calls. You can use either a DNS name or an IP address. An example of a URI using a DNS name is:
https://<server>:<port>/sspr/public/rest

Value defined in registry: https://sspr.gmadr2.novell.com:8443/sspr/public/rest
---

Key: ProxyServer
Type: String
Provides the IP address/DNS name and the port number of the proxy server.

Value defined in registry:

Key: ForceUserEnrollment
Type: DWord
Force users to set up their challenge response before logging into the computer. However, if you do not select this option, the user can choose not to set up any challenge response and proceed to log in.
Value of 1 will force user enrollment

Value defined in registry: 1

Key: EnableWindowsServerSupport
Type: DWord
Dword value indicating if Windows server support is enabled.

0 - Disabled
1 - Enabled

Value defined in registry: 1

Key: EnableURLRedirection
Type: DWord
Dword value indicating if URL Redirection is enabled.

0 - Disabled
1 - Enabled

Value defined in registry: 1

Key: EnableTLS1.2Support
Type: DWord
Dword value indicating if TLS 1.2 support is enabled. If disabled then SSL v3 will be used.

0 - Disabled
1 - Enabled

Value defined in registry: 1

Key: EnableProxy
Type: String
In an environment where Internet is not directly accessible and the Client Login Extension needs to access it, you need to connect the Client Login Extension to a proxy server.
A value of 1 enables the use of a proxy server.

Value defined in registry: 0

##########
Keys Defined in: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Novell
##########

##########
Keys Defined in: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Novell\NICI (Shared) U.S./Worldwide (128 bit)
##########

##########
Keys Defined in: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Novell\NICI (Shared) U.S./Worldwide (128 bit)\2.7.6
##########

##########
Keys Defined in: HKEY_CURRENT_USER\SOFTWARE\Novell\Login\LDAP
##########

Key: PrintableName
Type: String
Dynamic value - represents the name of the last authenticated user
---
Value defined in registry: Admin for Tree

Key: DefaultDN
Type: String
Dynamic value - represents the DN of the user

Value defined in registry: cn=admin,o=novell

##########
Keys Defined in: HKEY_CURRENT_USER\SOFTWARE\Novell\Parameters
##########

Key: NWLANGUAGE
Type: String
Installed Language of the Novell client for Windows.

Value defined in registry: ENGLISH

##########
Keys Defined in: HKEY_CURRENT_USER\SOFTWARE\Novell\SLAnalyzer
##########

Key: ReportLogDirectory
Type: String

Value defined in registry: C:\Users\Greg.GMADR2\Documents\SLAnalyzer
---

##
End of Report.
##

Sample AAF report

Report generated by: SLAnalyzer Version 3.0.0.5

########################
Advanced Authentication Framework
########################
########################
Contents of: C:\ProgramData\NetIQ\Device Service\config.properties
########################
#General
host.ports=8440;8441;8442

#PKI plugin
pki.vendorModule=auto

fingerprint.mode=3

#Card plugin
card.omnikeyEnabled=true
card.rfideasEnabled=false
card.smarfidEnabled=false
card.desfireEnabled=true

########################
Contents of: C:\ProgramData\NetIQ\Installer\81114F55-2321-40DD-A62D-7FC676F07EA7.ini
########################
[Install]
InstallDir=C:\Program Files\NetIQ\Windows Client\
Version=5.4.183.0
ProductName=Windows Client

########################
Contents of: C:\ProgramData\NetIQ\Installer\EA779D51-8567-48BC-9206-41C6981EA87D.ini
########################
[Install]
InstallDir=C:\Program Files (x86)\NetIQ\Device Service\
Version=5.4.138.0
ProductName=Device Service

########################
Contents of: C:\ProgramData\NetIQ\Installer\ef3dd092-dace-4e92-b011-66c369ba7512.ini
########################
[Install]
InstallDir=C:\Program Files (x86)\NetIQ\WBF Capture Service\
Version=5.2.41.0
ProductName=WBF Capture Service

########################
Contents of: C:\ProgramData\NetIQ\Logging\config.properties
########################
logEnabled=False
########################
Contents of: C:\ProgramData\NetIQ\WBF Capture Service\config.properties
########################
port=8442

########################
Contents of: C:\ProgramData\NetIQ\Windows Client\config.properties
########################
discovery.host: naaf54.gmadr2.novell.com
endpoint_id: df19953c810311e696ef000c296f406a
endpoint_name: REMGMORRIS01.microfocus.com

endpoint_secret: 1V0djKQTj0mT7bs283dUJJ62FusROTlm
logo_cache_path: C:\\ProgramData\\NetIQ\\Windows Client\\logocache

##
End of Report.
##

Sample LDAP Server Information (Active Directory)

Active Directory (Windows 2008 R2)

Get LDAP Server Information
Logged in as: cn=ssprproxyuser ldap,cn=users,dc=gmadr2,dc=novell,dc=com

RootDSE information:
supportedcapabilities = 1.2.840.113556.1.4.800
supportedcapabilities = 1.2.840.113556.1.4.1670
supportedcapabilities = 1.2.840.113556.1.4.1791
supportedcapabilities = 1.2.840.113556.1.4.1935
supportedcapabilities = 1.2.840.113556.1.4.2080

supportedldappolicies = MaxPoolThreads
supportedldappolicies = MaxDatagramRecv
supportedldappolicies = MaxReceiveBuffer
supportedldappolicies = InitRecvTimeout
supportedldappolicies = MaxConnections
supportedldappolicies = MaxConnIdleTime
supportedldappolicies = MaxPageSize
supportedldappolicies = MaxQueryDuration
supportedldappolicies = MaxTempTableSize
supportedldappolicies = MaxResultSetSize
supportedldappolicies = MinResultSets
supportedldappolicies = MaxResultSetsPerConn
supportedldappolicies = MaxNotificationPerConn
supportedldappolicies = MaxValRange
supportedldappolicies = ThreadMemoryLimit
supportedldappolicies = SystemMemoryLimitPercent

highestcommittedusn = 593065

namingcontexts = DC=gmadr2,DC=novell,DC=com
namingcontexts = CN=Configuration,DC=gmadr2,DC=novell,DC=com
namingcontexts = CN=Schema,CN=Configuration,DC=gmadr2,DC=novell,DC=com
namingcontexts = DC=DomainDnsZones,DC=gmadr2,DC=novell,DC=com
namingcontexts = DC=ForestDnsZones,DC=gmadr2,DC=novell,DC=com

subschemasubentry = CN=Aggregate,CN=Schema,CN=Configuration,DC=gmadr2,DC=novell,DC=com

dnshostname = WIN-V3JMMISD13E.gmadr2.novell.com

configurationnamingcontext = CN=Configuration,DC=gmadr2,DC=novell,DC=com

forestfunctionality = 2

issynchronized = TRUE

ldapservicename = gmadr2.novell.com:win-v3jmmisd13e$@GMADR2.NOVELL.COM

domaincontrollerfunctionality = 4

dsservicename = CN=NTDS Settings,CN=WIN-V3JMMISD13E,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC

supportedsaslmechanisms = GSSAPI
supportedsaslmechanisms = GSS-SPNEGO
supportedsaslmechanisms = EXTERNAL
supportedsaslmechanisms = DIGEST-MD5

supportedldapversion = 3
supportedldapversion = 2

defaultnamingcontext = DC=gmadr2,DC=novell,DC=com

currenttime = 20170301181411.0Z

supportedcontrol = 1.2.840.113556.1.4.319
supportedcontrol = 1.2.840.113556.1.4.801
supportedcontrol = 1.2.840.113556.1.4.473
supportedcontrol = 1.2.840.113556.1.4.528
supportedcontrol = 1.2.840.113556.1.4.417
supportedcontrol = 1.2.840.113556.1.4.619
supportedcontrol = 1.2.840.113556.1.4.841
supportedcontrol = 1.2.840.113556.1.4.529
supportedcontrol = 1.2.840.113556.1.4.805
supportedcontrol = 1.2.840.113556.1.4.521
supportedcontrol = 1.2.840.113556.1.4.970
supportedcontrol = 1.2.840.113556.1.4.1338
supportedcontrol = 1.2.840.113556.1.4.474
supportedcontrol = 1.2.840.113556.1.4.1339
supportedcontrol = 1.2.840.113556.1.4.1340
supportedcontrol = 1.2.840.113556.1.4.1413
supportedcontrol = 2.16.840.1.113730.3.4.9
supportedcontrol = 2.16.840.1.113730.3.4.10
supportedcontrol = 1.2.840.113556.1.4.1504
supportedcontrol = 1.2.840.113556.1.4.1852
supportedcontrol = 1.2.840.113556.1.4.802
supportedcontrol = 1.2.840.113556.1.4.1907
supportedcontrol = 1.2.840.113556.1.4.1948
supportedcontrol = 1.2.840.113556.1.4.1974
supportedcontrol = 1.2.840.113556.1.4.1341
supportedcontrol = 1.2.840.113556.1.4.2026
supportedcontrol = 1.2.840.113556.1.4.2064
supportedcontrol = 1.2.840.113556.1.4.2065
supportedcontrol = 1.2.840.113556.1.4.2066

servername = CN=WIN-V3JMMISD13E,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=gmadr2,DC=novell

schemanamingcontext = CN=Schema,CN=Configuration,DC=gmadr2,DC=novell,DC=com

isglobalcatalogready = TRUE

domainfunctionality = 2

rootdomainnamingcontext = DC=gmadr2,DC=novell,DC=com

Sample LDAP Server Information (eDirectory)

eDirectory (OES)

Get LDAP Server Information

Logged in as: cn=ssprproxyuser,o=novell

RootDSE information:

errors = 99

chainings = 0

unauthbinds = 0

supportedfeatures = 1.3.6.1.4.1.4203.1.5.1
supportedfeatures = 2.16.840.1.113719.1.27.99.1

outbytes = 22058038

compareops = 0

modifyentryops = 369

wholesubtreesearchops = 154

readops = 587

supportedextension = 2.16.840.1.113719.1.148.100.1
supportedextension = 2.16.840.1.113719.1.148.100.3
supportedextension = 2.16.840.1.113719.1.148.100.5
supportedextension = 2.16.840.1.113719.1.148.100.7
supportedextension = 2.16.840.1.113719.1.148.100.9
supportedextension = 2.16.840.1.113719.1.148.100.11
supportedextension = 2.16.840.1.113719.1.148.100.13
supportedextension = 2.16.840.1.113719.1.148.100.15
supportedextension = 2.16.840.1.113719.1.148.100.17
supportedextension = 2.16.840.1.113719.1.39.42.100.1
supportedextension = 2.16.840.1.113719.1.39.42.100.3
supportedextension = 2.16.840.1.113719.1.39.42.100.5
supportedextension = 2.16.840.1.113719.1.39.42.100.7
supportedextension = 2.16.840.1.113719.1.39.42.100.9
supportedextension = 2.16.840.1.113719.1.39.42.100.11
supportedextension = 2.16.840.1.113719.1.39.42.100.13
supportedextension = 2.16.840.1.113719.1.39.42.100.15
supportedextension = 2.16.840.1.113719.1.39.42.100.17
supportedextension = 2.16.840.1.113719.1.39.42.100.19
supportedextension = 2.16.840.1.113719.1.39.42.100.21
supportedextension = 2.16.840.1.113719.1.39.42.100.23
supportedextension = 2.16.840.1.113719.1.39.42.100.25
supportedextension = 2.16.840.1.113719.1.27.100.1
supportedextension = 2.16.840.1.113719.1.27.100.3
supportedextension = 2.16.840.1.113719.1.27.100.5
supportedextension = 2.16.840.1.113719.1.27.100.7
supportedextension = 2.16.840.1.113719.1.27.100.11

supportedextension = 2.16.840.1.113719.1.27.100.13
supportedextension = 2.16.840.1.113719.1.27.100.15
supportedextension = 2.16.840.1.113719.1.27.100.17
supportedextension = 2.16.840.1.113719.1.27.100.19
supportedextension = 2.16.840.1.113719.1.27.100.21
supportedextension = 2.16.840.1.113719.1.27.100.23
supportedextension = 2.16.840.1.113719.1.27.100.25
supportedextension = 2.16.840.1.113719.1.27.100.27
supportedextension = 2.16.840.1.113719.1.27.100.29
supportedextension = 2.16.840.1.113719.1.27.100.31
supportedextension = 2.16.840.1.113719.1.27.100.33
supportedextension = 2.16.840.1.113719.1.27.100.35
supportedextension = 2.16.840.1.113719.1.27.100.37
supportedextension = 2.16.840.1.113719.1.27.100.39
supportedextension = 2.16.840.1.113719.1.27.100.41
supportedextension = 2.16.840.1.113719.1.27.100.96
supportedextension = 2.16.840.1.113719.1.27.100.98
supportedextension = 2.16.840.1.113719.1.27.100.101
supportedextension = 2.16.840.1.113719.1.27.100.103
supportedextension = 2.16.840.1.113719.1.142.100.1
supportedextension = 2.16.840.1.113719.1.142.100.4
supportedextension = 2.16.840.1.113719.1.142.100.6
supportedextension = 2.16.840.1.113719.1.27.100.9
supportedextension = 2.16.840.1.113719.1.27.100.43
supportedextension = 2.16.840.1.113719.1.27.100.45
supportedextension = 2.16.840.1.113719.1.27.100.47
supportedextension = 2.16.840.1.113719.1.27.100.49
supportedextension = 2.16.840.1.113719.1.27.100.51
supportedextension = 2.16.840.1.113719.1.27.100.53
supportedextension = 2.16.840.1.113719.1.27.100.55
supportedextension = 1.3.6.1.4.1.1466.20037
supportedextension = 2.16.840.1.113719.1.27.100.79
supportedextension = 2.16.840.1.113719.1.27.100.84
supportedextension = 2.16.840.1.113719.1.27.103.1
supportedextension = 2.16.840.1.113719.1.27.103.2

simpleauthbinds = 920

directorytreename = OESTREE

listops = 0

referralsreturned = 0

securityerrors = 142

supportedgroupingtypes = 2.16.840.1.113719.1.27.103.8

repupdatesout = 0

supportedsaslmechanisms = NMAS_LOGIN

vendorversion = LDAP Agent for NetIQ eDirectory 8.8 SP8 (20804.02)

subschemasubentry = cn=schema

strongauthbinds = 0

repupdatesin = 0

dsaname = cn=linux-61w4,o=novell

onelevelsearchops = 0

inops = 4387

modifyrdnops = 0

searchops = 741

supportedcontrol = 2.16.840.1.113719.1.27.101.6
supportedcontrol = 2.16.840.1.113719.1.27.101.5
supportedcontrol = 1.2.840.113556.1.4.319
supportedcontrol = 2.16.840.1.113730.3.4.3
supportedcontrol = 2.16.840.1.113730.3.4.2
supportedcontrol = 2.16.840.1.113719.1.27.103.7
supportedcontrol = 2.16.840.1.113719.1.27.101.40
supportedcontrol = 2.16.840.1.113719.1.27.101.41
supportedcontrol = 1.2.840.113556.1.4.1413
supportedcontrol = 1.2.840.113556.1.4.805

abandonops = 0

vendorname = NetIQ Corporation

inbytes = 141561

addentryops = 0

bindsecurityerrors = 26

supportedldapversion = 2
supportedldapversion = 3

extendedops = 68

removeentryops = 0

Appendix - Figures

Figure 1 - Initialization error 18
Figure 2 - Update prompt 23
Figure 3 - File open menu 24
Figure 4 - Opening a compressed file 26
Figure 5 - Extracted content 26
Figure 6 - Large file detected 27
Figure 7 - Split file? 27
Figure 8 - Segments already found 28
Figure 9 - Create segment progress 28
Figure 10 - Segment list 28
Figure 11 - Split completed 29
Figure 12 – File Menu 31
Figure 13 - Moved column 33
Figure 14 - Sorted on Module column 34
Figure 15 - Comments field 35
Figure 16 - Unsaved comments prompt 36
Figure 17 - Prompt to overwrite backup file 36
Figure 18 - Copying data from the XML data window 37
Figure 19 - Copying data from the JSON data window 37
Figure 20 - Find XML/JSON text 38
Figure 21 - Found XML/JSON data 38
Figure 22 - Expand All 39
Figure 23 - Collapse All 39
Figure 24 - Tooltip display 40
Figure 25 - View Line 40
Figure 26 - Copying the full line from a log file 41
Figure 27 - Copying a single column's data 42
Figure 28 - Copying multiple rows of data 43
Figure 29 - Copy multiple rows non-adjacent 43
Figure 30 - Find window 44
Figure 31 - Find 44
Figure 32 - Find failure 45
Figure 33 - Found items 45
Figure 34- Find All 45
Figure 35 - Log file jump to line number 46
Figure 36 - Invalid line 46
Figure 37 - Selecting a filter 50
Figure 38 - Repositioned line matching selected filter 50
Figure 39 - Filter button 51
Figure 40 - Filtered log 51

Figure 41 - Create Custom Display Filter window 52
Figure 42 - Creating a custom filter 52
Figure 43 - Displayed custom filter 53
Figure 44 - Creating a complex custom filter 53
Figure 45 - Displayed complex custom filter 54
Figure 46 - Filter User='greg' 55
Figure 47 - Filter [perpetrator id]='administrator' 55
Figure 48 - Filter Message Like '%Get request%' 56
Figure 49 - Filter [perpetrator id]='administrator' And Message='authenticated' 56
Figure 50 - Opened SLAnalyzer report 58
Figure 51 - Opened Novell client provider log 58
Figure 52 - Opened SecretStore debug log 59
Figure 53 - Opened SecureLogin debug log 59
Figure 54 - CLE eadebug.txt file 60
Figure 55 - Opened DAS log 60
Figure 56 - Opened NDS trace file 61
Figure 57 - Opened SSPR debug log 61
Figure 58 - Opened JSON file 62
Figure 59 - Opened XML file 62
Figure 60 - Opened csv file 63
Figure 61 - Opened AAF Database 64
Figure 62 - Opened AAF Debug Log 64
Figure 63 - Log file opened with the generic log reader 65
Figure 64 - CSV header prompt 66
Figure 65 - Opened csv file 66
Figure 66 - Formatted JSON data window 67
Figure 67 - Formatted XML data window 67
Figure 68 - Opened html file 68
Figure 69 - Opened ZEN message log 68
Figure 70 - Analyze menu 78
Figure 71 - Configuration Report 79
Figure 72 - Click to save tip 80
Figure 73 – Save report as Report Format (*.txt) 81
Figure 74 - Save report as XML (*.xml) 81
Figure 75 - Optional My Computer reports 85
Figure 76 - My Computer/ARP table 86
Figure 77 - My Computer/DNS Information 88
Figure 78 - My Computer/Internet Browsers 88
Figure 79 - My Computer/IP configuration 89
Figure 80 - My Computer/GPO Information 89
Figure 81 - My Computer/TCP port information 90
Figure 82 - My Computer/Routing table 91

Figure 83 – My Computer/Windows event logs 91
Figure 84 - Analyze AAF 92
Figure 85 - AD report 93
Figure 86 - CLE report 94
Figure 87 - LDAP report 96
Figure 88 - Novell Client report 97
Figure 89 - Secret Store report 98
Figure 90 - Optional SecureLogin reports 100
Figure 91 - Tools Menu 104
Figure 92 - Run as administrator 105
Figure 93 - User level debugging 106
Figure 94 - Machine level debugging 107
Figure 95 - Change debug file location 108
Figure 96 - Static log path 109
Figure 97 - SecureLogin module logging 110
Figure 98 - SecureLogin module logging with items set 110
Figure 99 - Debug Console window 114
Figure 100 - Debug Process Filters 114
Figure 101 - File Browser 115
Figure 102 - View registry keys 116
Figure 103 - Registry key detail 116
Figure 104 - Explore Product Related Registry Keys 117
Figure 105 - Find registry key 118
Figure 106 - Move forward 118
Figure 107 - Group Policy Tools 119
Figure 108 - GPO HTML Report 120
Figure 109 - GPO generate report 121
Figure 110 - GPO report 121
Figure 111 - Force update 122
Figure 112 - SSPR REST Client 132
Figure 113 - REST API Description 134
Figure 114 - REST Request window 134
Figure 115 - REST Reply window 134
Figure 116 - Certificate details 134
Figure 117 - Get Challenge Questions Parameters 155
Figure 118 - Post Challenge Answers Parameters 157
Figure 119 - Challenge Answer Restrictions 158
Figure 120 - Entering a Challenge Answer 158
Figure 121 - Answered question updated 159
Figure 122 - Prompt for no answers defined 159
Figure 123 - No answers aborting call. 159
Figure 124 - Post Verify Responses 161

Figure 125 - Post Verify Responses Parameters 162
Figure 126 - Verify Responses Challenge Prompt 162
Figure 127 - Delete Challenge Answers 164
Figure 128 - Post Check Password 166
Figure 129 - Post Check Password Parameters 166
Figure 130 - Get Health 168
Figure 131 - Get Health Parameters 168
Figure 132 - Server Health 169
Figure 133 - Get Profile 171
Figure 134 - Server profile settings 171
Figure 135 - Post Profile 173
Figure 136 - Post Profile Parameters 174
Figure 137 - Modifying profile data 174
Figure 138 - Get Random Password 176
Figure 139 - Get Random Password Parameters 176
Figure 140 - Post Random Password 178
Figure 141 - Post Random Password Parameters 178
Figure 142 - Post Set Password 180
Figure 143 - Post Set Password Parameters 181
Figure 144 - Get Statistics 183
Figure 145 - Get Statistics Parameters 183
Figure 146 - Get Status 185
Figure 147 - Get Status Parameters 185
Figure 148 - Post Verify OTP 187
Figure 149 – Post Verify OTP Parameters 187
Figure 150 - Setup Mobile App Authentication 188
Figure 151 - SSPR Quick Links 194
Figure 152 - SSPR Rights Validator 195
Figure 153 - SSPR Rights Validator report 197
Figure 154- SSPR Rights Validator AD/eDirectory data table menu 198
Figure 155 - SSPR Rights Validator LDAP data table menu 198
Figure 156 - AD Read all attribute values 201
Figure 157 - SSPR AD Rights Validator 212
Figure 158 - SSPR eDirectory Rights Validator 213
Figure 159 - SSPR LDAP Rights Validator 214
Figure 160 - Advanced Authentication 219
Figure 161 - AAF REST Request window 224
Figure 162 - AAF REST Reply window 224
Figure 163 - Certificate details 224
Figure 164 - AAF appliance Quick links 225
Figure 165 - Browser window 225
Figure 166 - AAF 5.x Rest Client status message 226

Figure 167 - AAF Packet Data window 227
Figure 168 - Enrollment window 237
Figure 169 - Enrollment window with selected item 238
Figure 170 - Password enrollment 239
Figure 171 - HOTP enrollment 241
Figure 172 - Radius enrollment 242
Figure 173 - Security Question enrollment (SMARTPHONE:1) Smartphone enrollment 243
Figure 174 - Smartphone enrollment 244
Figure 175 - TOTP enrollment 244
Figure 176 - Voice enrollment 245
Figure 177 - Build enrolled methods database 266
Figure 178 - Login Event Reflection 374
Figure 179 - SLAnalyzer endpoint 376
Figure 180 - Cached SLAnalyzer endpoint data 376
Figure 181 - AAF Logon parameters 379
Figure 182 - AAF Add new event 379
Figure 183 - AAF Update Methods 379
Figure 184 - Logon select event and method 381
Figure 185 - Select Method to update 385
Figure 186 - LDAP browser 493
Figure 187 - LDAP Login Settings 494
Figure 188 - Beavertail 494
Figure 189 - LDAP Search criteria 495
Figure 190 - LDAP connection parameters 496
Figure 191 - LDAP Object window 496
Figure 192 - LDAP Attribute window 496
Figure 193 - Viewing LDAP attribute data 497
Figure 196 - LDAP users 498
Figure 197 - LDAP browser login as test 499
Figure 198 - LDAP browser logged in as admin 500
Figure 199 - LDAP Browser validate SSPR setting 501
Figure 200 - JSON console window 502
Figure 201 - Copy JSON data 502
Figure 202 - Process JSON data 503
Figure 203 - JSON console window with data 503
Figure 204 - Connect to SQL server with IP address 516
Figure 205 - Connect to SQL server with DNS name 517
Figure 206 - Return all columns and records 518
Figure 207 - Return specific columns for all records 518
Figure 208 - Return all columns when record equals value 519
Figure 209 - Return all columns when record contains specified data 519
Figure 210 - Web Browser 534

Figure 211 - SLAnalyzer settings 537
Figure 212 - Built-In report filters 540
Figure 213 - Enabled built-in filter 540
Figure 214 - User defined filters 541
Figure 215 - Disabled built-in filter 542
Figure 216 - Edit filter 542
Figure 217 - Delete user defined filter 543
Figure 218 - Attempt to delete a built-in filter 543
Figure 219 - Create new filter 544
Figure 220 - Setting filter to Errors 544
Figure 221 - Help menu 545
Figure 222 - Error and Return Codes 546
Figure 223 - Micro Focus Internal Resources 547
Figure 224 - 3rd Party Tools 548
Figure 225 - Product Links 549
Figure 226 - About box 550