|  |
| --- |
| **Government of Ontario** |
| **Access Restriction Unified: User Manual** |
| **Technical Support Office** |

|  |
| --- |
| **Version: 0.3**  **4/20/2017** |

©2016 The Technical Support Office. All rights reserved.

This documentation is furnished *AS IS* and is subject to change without notice and therefore should not be construed as a commitment by the Technical Support Office. This documentation may *not* be copied, modified or distributed in any way without the express authorization of the Technical Support Office. This documentation may be used only in connection with the Technical Support Office’s products and services. Use, duplication, reproduction, release, modification, disclosure or transfer of this documentation is restricted in accordance with the Government of Ontario’s policies and regulations. This documentation qualifies as computer software documentation and any use shall be governed solely by these terms. All other use is strictly prohibited. The Technical Support Office assumes no responsibility or liability for any errors or inaccuracies that appear in this documentation.

# Revisions

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Owner |
| September 13, 2016 | 0.1 | Initial version | TSO |
| September 21, 2016 | 0.2 | Updated sesudo commands | TSO |
| April 20, 2017 | 0.3 | Added content for access\_restriction\_cmd | TSO |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[Revisions 2](#_Toc480444928)

[Introduction 4](#_Toc480444929)

[User Manual 4](#_Toc480444930)

[Configuration Prerequisites 5](#_Toc480444931)

[Email 7](#_Toc480444932)

[Access Restriction 9](#_Toc480444933)

[Operations 10](#_Toc480444934)

[Changing Access Restriction 10](#_Toc480444935)

[Multiple Configurations 13](#_Toc480444936)

[Command line 16](#_Toc480444937)

[Enable Access Restriction 17](#_Toc480444938)

[Disable Access Restriction 17](#_Toc480444939)

# Introduction

## User Manual

This user manual contains instructions for the TSO’s in-house **Access Restriction Unified (AR)** tool. It describes the functionality, and uses output and screenshots from version 1.1 of the software.

There are several versions of the *User Manual*, therefore, you should refer to the version appropriate for the variant you are configuring and running.

# Configuration Prerequisites

Before enabling or disabling **access restriction**, you are required to fill out the directives shown in the table below. These directives can be found by following the instructions below:

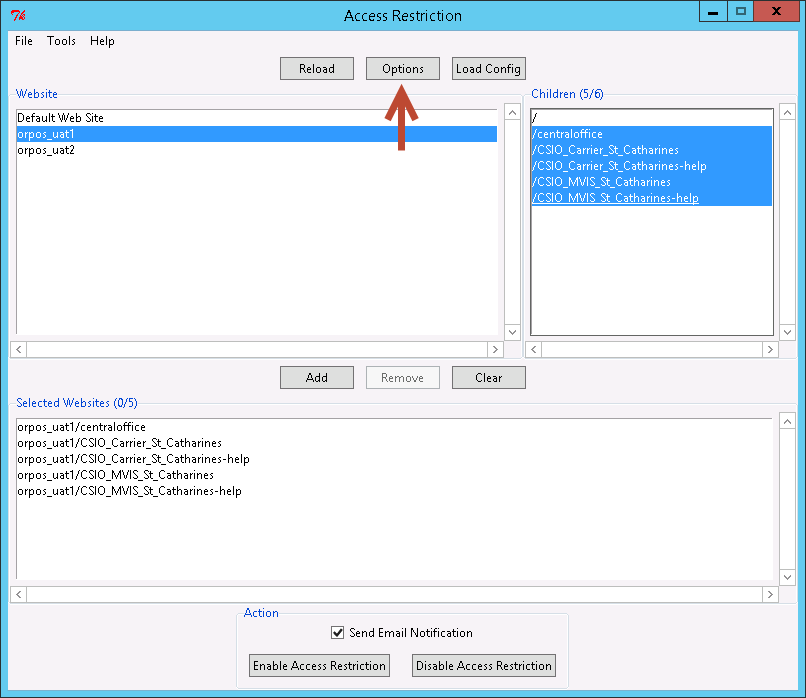
* Open the **command prompt**
* Run the following command to find the associated **sesudo rule** for the **access\_restriction.exe** utility

|  |
| --- |
| sesudo -list 2>&1|find /i "access\_restriction" |
| App06 : D:\MTO\ARTool\access\_restriction.exe |

* In the illustration above, the **sesudo rule** for the **access\_restriciton.exe** utility is called **App06**
* Run the following **sesudo** command below to invoke rule **App06**

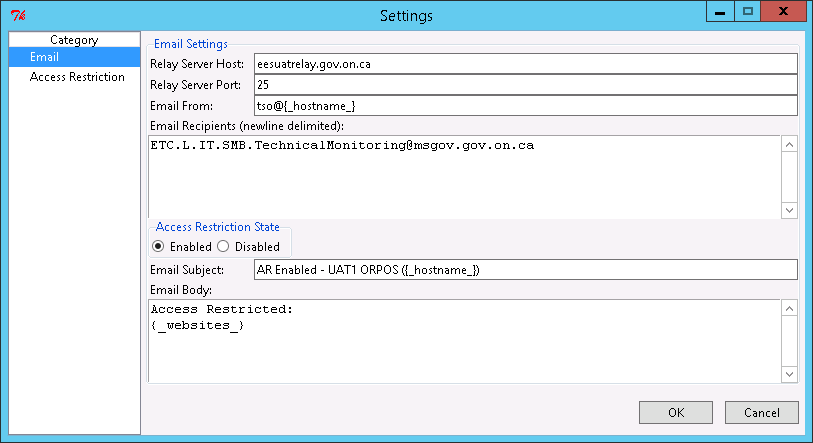
|  |
| --- |
| sesudo –do App06 |

* Click on the **Options** button.



## Email

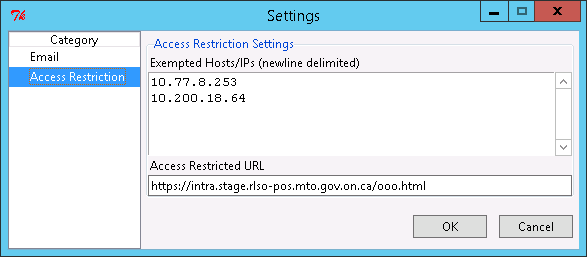
In the **Category** panel, select **Email** as shown below. To save the changes, click **OK**; to discard the changes; click **Cancel**.



|  |  |  |
| --- | --- | --- |
| Directive | Value Description | Examples |
| Relay Server Host | The email SMTP server (also known as, relay) hostname or IP | eesrelay.gov.on.ca  eesuatrelay.gov.on.ca  eesdevrelay.gov.on.ca |
| Relay Server Port | The email SMTP server’s listening port number | 25 |
| Email From | The value of the FROM header of the email.  Optionally, the variable {\_username\_} can be used which will be automatically replaced with the current Windows username.  Optionally, the variable {\_hostname\_} can be used which will be automatically replaced with the current Windows server hostname. | john.doe@ontario.ca  {\_username\_}@{\_hostname\_}  donotreply@{\_hostname\_} |
| Email Recipients | The list of recipients the email notification will be sent to. Each email is separated by a newline. | support.team@ontario.ca |
| Access Restriction Enabled/Disabled | The state of Access Restriction (AR).  For your convenience, it’s possible to pre-configured two states of AR: Enabled or Disabled |  |
| Subject | The value of the SUBJECT header of the email.  Optionally, the variable {\_hostname\_} can be used which will be automatically replaced with the current Windows server hostname. | AR Enabled - PROD APPXYZ  AR Disabled - PROD APPXYZ |
| Body | The value of the BODY of the email.  Optionally, the variable {\_websites\_} can be used which will be automatically replaced with the selected websites | AR has been enabled: {\_websites\_}  Open to public: {\_websites\_} |

## Access Restriction

In the **Category** panel, select **Access Restriction** as shown below. To save the changes, click **OK**; to discard the changes; click **Cancel**.



|  |  |  |
| --- | --- | --- |
| Directive | Value Description | Examples |
| Exempted Hosts/IPs | List of hosts/IPs that will still be able to access the websites even with access restriction is still enabled | 10.77.8.253  10.200.18.64 |
| Access Restricted URL | Definition of the URL visitors to the websites will be redirected to if access restriction is enabled | http://xyz/ooo.html |

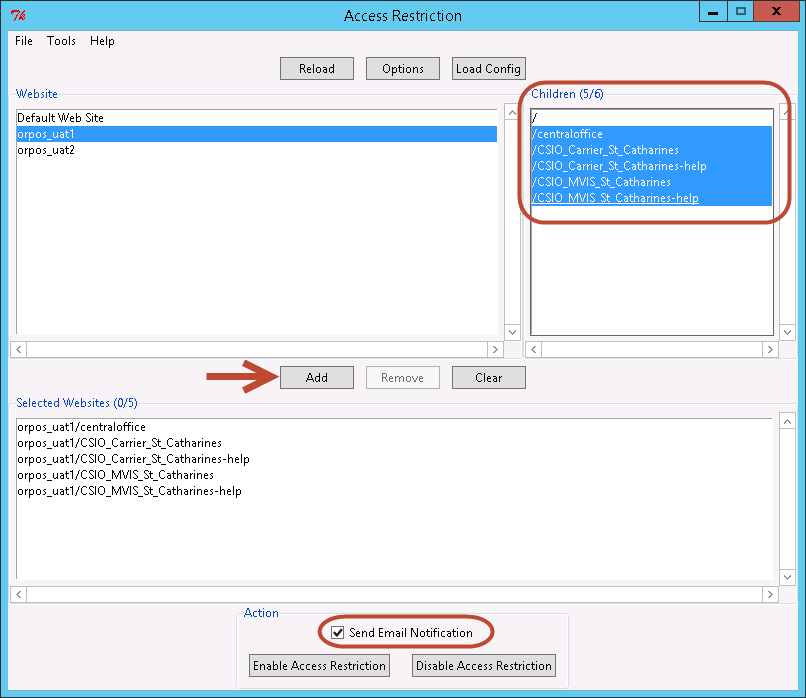
# Operations

Before enabling or disabling **access restriction** on certain websites, you are required to run this application with **Local Administrator** rights of the target Windows server with IIS installed.

## Changing Access Restriction

This section describes the steps to enableordisable **access restriction**.

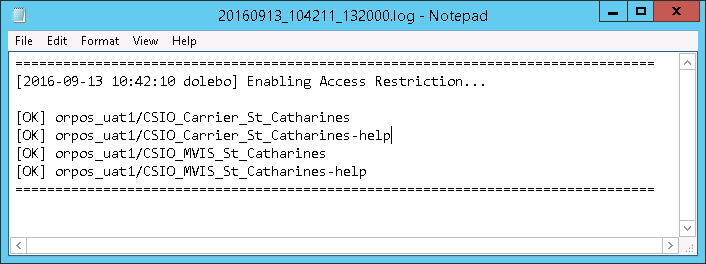
* Change directory to where the **Access Restriction** tool reside. E.g. **D:\MTO\ARTools**
* Right click on **access\_restriction.exe** and select **Run as administrator**
* In the **Website** panel, select the parent website
* In the **Children** panel, select the child websites (for **multiple selection**, press and hold Ctrl; to **select all**, hold Ctrl and press the “a” key)



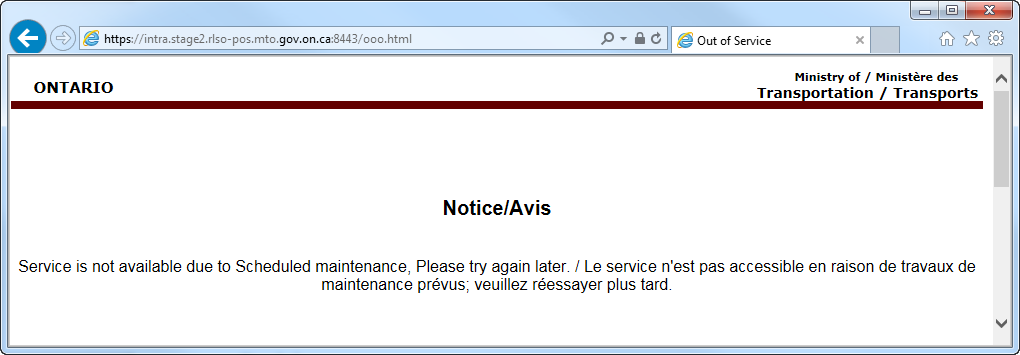
* In the illustration above, we selected the following and click **Add**:
  + Centraloffice
  + CISO\_Carrier\_St\_Catherines
  + CISO\_Carrier\_St\_Catherines-help
  + CISO\_MVIS\_St\_Catherines
  + CISO\_MVIS\_St\_Catherines-help
* Once the selected websites are added to the bottom panel, to enable access restriction, click the **Enable Access Restriction** button
* To disable access restriction, click the **Disable Access Restriction** button
* To send email notification, click the **Send Email Notification** checkbox



* Click **OK**



* Review the logs and ensure that all of the results show **[OK]**
* **Verify** the websites with access restriction **enabled** and you should be presented with the maintenance notice screen below



## Multiple Configurations

In the event that you need to quickly load multiple configuration files, prior to starting the **Access Restriction** application, make a copy of the **access\_restriction.ini** file (e.g. **access\_restriction2.ini**).

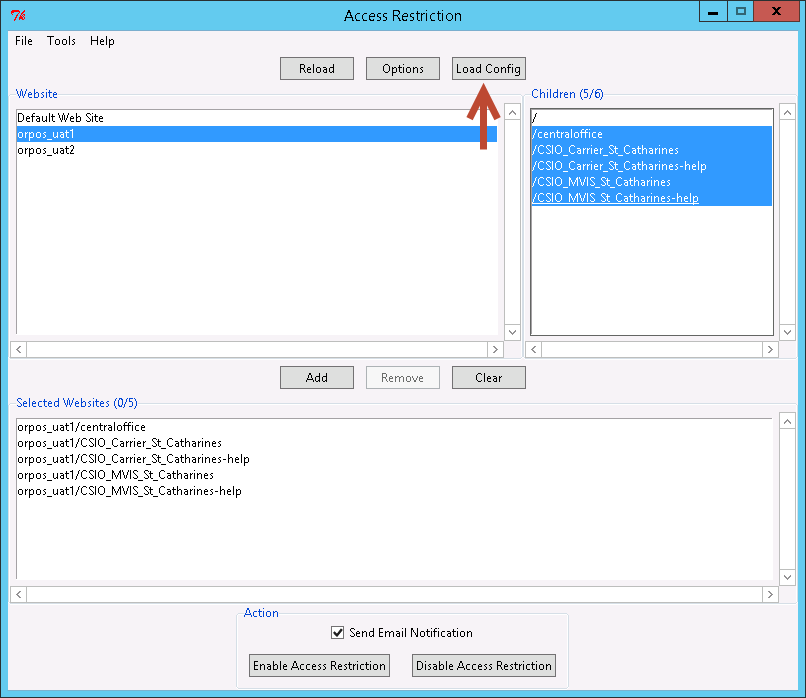
* Open the **command prompt**
* Run the following command to find the associated **sesudo rule** for the **access\_restriction.exe** utility

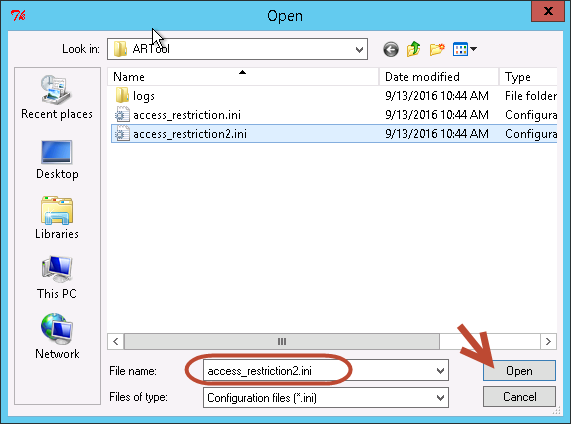
|  |
| --- |
| sesudo -list 2>&1|find /i "access\_restriction" |
| App06 : D:\MTO\ARTool\access\_restriction.exe |

* In the illustration above, the **sesudo rule** for the **access\_restriciton.exe** utility is called **App06**
* Run the following **sesudo** command below to invoke rule **App06**

|  |
| --- |
| sesudo –do App06 |

* Click the **Load Config** button





* Select **access\_restriction2.ini** and click **Open**
* Any changes to the configurations will not be saved to the **access\_restriction2.ini** file

## Command line

Since version 1.1, **Access Restriction** supports command line interface (e.g. useful for batch processing) via **access\_restriction\_cmd.exe**. Similar to the main utility, requires local admin privileges which can be gained via sesudo. Please see the example below

* Open the **command prompt**
* Run the following command to find the associated **sesudo rule** for the **access\_restriction\_cmd.exe** utility

|  |
| --- |
| sesudo -list 2>&1|find /i "access\_restriction\_cmd" |
| App06 : D:\MTO\ARTool\access\_restriction\_cmd.exe |

* In the illustration above, the **sesudo rule** for the **access\_restriction\_cmd.exe** utility is called **App06**
* Run the following **sesudo** command below to invoke rule **App06**

|  |
| --- |
| sesudo –do App06 |

The access\_restriction\_cmd.exe utility requires an existing access\_restriction.ini configuration file to run. Within the configuration file, ensure that that the following sections have been properly set:

|  |  |
| --- | --- |
| Section | Description |
| data | List of websites whose the state will be changed |
| email | Email configurations to be used to send out notification |
| access\_restriction | AR related information to be used during state change |

To access the help prompt, invoke the -h or --help argument:

|  |
| --- |
| access\_restriction\_cmd.exe |
| Usage: access\_restriction\_cmd.exe -c config.ini [enable|disable]  Options:  --version show program's version number and exit  -h, --help show this help message and exit  -c CONFIG, --config=CONFIG  use this configuration file |

### Enable Access Restriction

To enable access restriction via **access\_restriction\_cmd.exe,** run the following command line with local admin privileges

|  |
| --- |
| access\_restriction\_cmd.exe -c config.ini enable |

### Disable Access Restriction

To disable access restriction via **access\_restriction\_cmd.exe,** run the following command line with local admin privileges

|  |
| --- |
| access\_restriction\_cmd.exe -c config.ini disable |