



MANAGED TRUSTED ACCESS SERVICE (MSS-TAS)

V062623

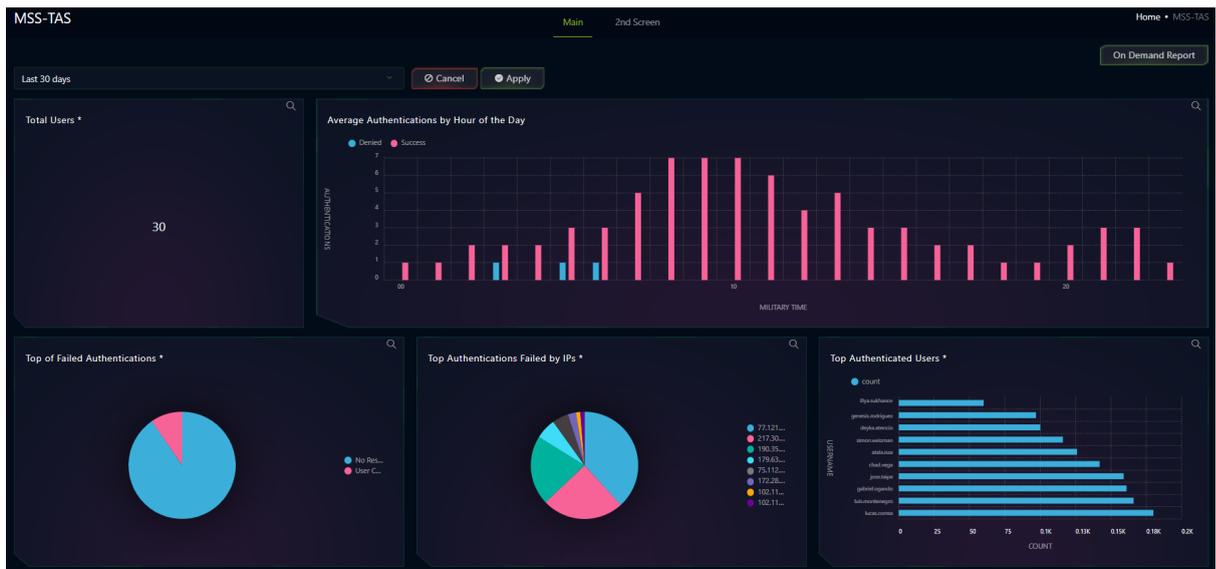
Revision V062623

This document is a briefing that describes the operation and use of the Managed Trusted Access Service Protection, and it is meant for all users of SKYWATCH WEB Platform.

Purpose of this Dashboard

This SKYWATCH Dashboard(s) provide **visibility** to the technical and executive users of SKYWATCH for the **MSS-TAS** Service and the ability to generate an on-demand **report** for this service (with the information of the dashboard). These are two of deliverables for the service. There are more consolidated reports that combine the information of this service with other contracted services. Also certain of the parameters defined on this Dashboard are used as indicators to trigger SKYWATCH automations (GLESEC NOTABLE EVENTS – GNE) and this activates the GLESEC OPERATION CENTER(s) (GOC) to action to further investigate and for incident-response purpose.

The following presents the SKYWATCH MSS-TAS



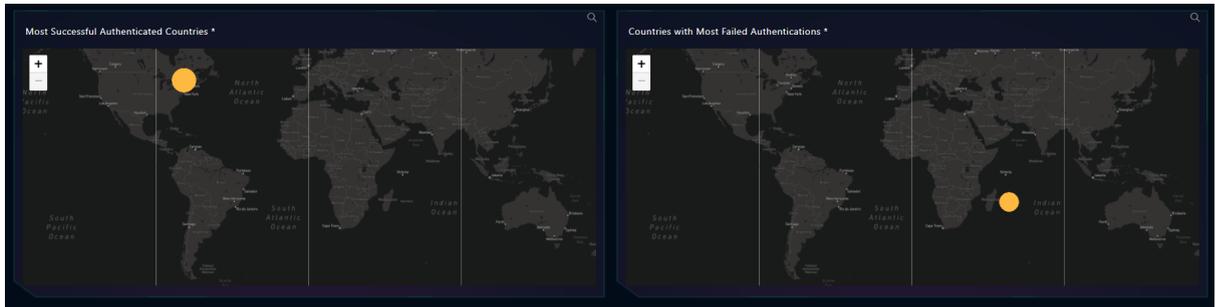


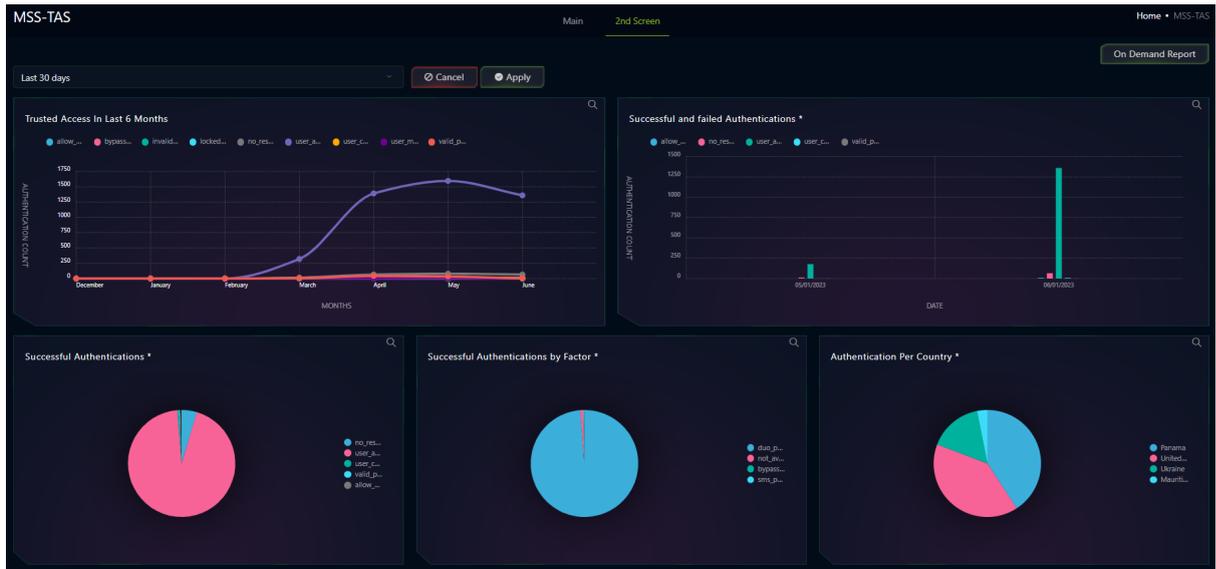
Most Active Applications *				Authentication Status in the Last 24 Hours *	
App	Denied	Success	Total	Reason	Count
1 GLESEC Workstation Logon	3	345	348	1 User Approved	1537
2 Cymulate	13	258	271	2 No Response	76
3 Splunk	18	220	238	3 Allow Unenrolled User	8
4 GLESEC INTRANET	24	196	220	4 User Cancelled	8
5 Palo Alto GlobalProtect 2	12	195	207	5 Valid Passcode	4
6 Palo Alto GlobalProtect 1	9	153	162		
7 GMP	3	95	98		

Users with failed authentications *			Authentications left as No response by Users *			Users with Invalid Passcode *
User	Time	Src ip	Username	IP Address	Time	
1 iliyasukhanov3	Fri Jun 23 07:16:02 2023 EDT	77.121.149.42	1 iliyasukhanov3	77.121.149.42	Fri Jun 23 07:16:02 2023 EDT	no invalid passcodes
2 iliyasukhanov3	Fri Jun 23 07:19:17 2023 EDT	77.121.149.42	2 iliyasukhanov3	77.121.149.42	Fri Jun 23 07:19:17 2023 EDT	
3 adelys.varela	Thu Jun 22 07:33:07 2023 EDT	190.35.249.82	3 adelys.varela	190.35.249.82	Thu Jun 22 07:33:07 2023 EDT	
4 adelys.varela	Thu Jun 22 07:33:07 2023 EDT	190.35.249.82	4 adelys.varela	190.35.249.82	Thu Jun 22 07:34:57 2023 EDT	
5 adelys.varela	Thu Jun 22 07:34:57 2023 EDT	190.35.249.82	5 iliyasukhanov	77.121.149.42	Thu Jun 22 07:57:25 2023 EDT	
6 adelys.varela	Thu Jun 22 07:39:14 2023 EDT	190.35.249.82	6 luis.montenegro	179.63.197.202	Thu Jun 22 11:55:20 2023 EDT	
7 adelys.varela	Thu Jun 22 07:39:17 2023 EDT	190.35.249.82	7 iliyasukhanov3	217.30.194.92	Wed Jun 21 09:48:51 2023 EDT	

Locked Out Users *	Anomalous push by Users *
no locked out users	no anomalous pushes

Call timed out by Users *			Authentications Cancelled by the Users *		
Username	Time	IP Address	Username	Time	IP Address
1 luis.montenegro	Mon Jun 26 06:41:49 2023 EDT	179.63.197.202	1 iliyasukhanov	Mon May 29 08:26:31 2023 EDT	77.121.149.42
2 iliyasukhanov	Wed Jun 21 06:28:08 2023 EDT	217.30.194.92	2 adelys.varela	Thu Jun 22 07:33:07 2023 EDT	190.35.249.82
3 iliyasukhanov	Wed Jun 21 05:33:04 2023 EDT	77.121.149.42	3 adelys.varela	Thu Jun 22 07:39:14 2023 EDT	190.35.249.82
4 iliyasukhanov	Wed Jun 7 06:31:06 2023 EDT	217.30.194.92	4 adelys.varela	Thu Jun 22 07:39:17 2023 EDT	190.35.249.82
5 eduard.volkov	Wed Jun 7 06:41:49 2023 EDT	102.115.211.161	5 adelys.varela	Thu Jun 22 07:41:02 2023 EDT	190.35.249.82
6 lucas.correa	Mon Jun 5 13:00:55 2023 EDT	172.28.2.88	6 jose.taipe	Mon Jun 19 22:46:48 2023 EDT	179.63.197.202
7 chad.vega	Mon Jun 5 11:25:54 2023 EDT	0.0.0.0	7 iliyasukhanov	Fri Jun 16 08:18:48 2023 EDT	77.121.149.42





Detailed Description of functionality of the MSS-BOT Dashboard

Below the description and use cases of each of the components.

ITEM	DESCRIPTION
Main	
Total Users	<p>Displays the # of registered users.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used as an indicator of the amount of registered users in the solution.</i></p>
Average Authentications by Hour of the Day	<p>Displays the average # of successful and denied authentications for every hour in a day.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to determine the most common times that authentications occur.</i></p>
Top of Failed Authentications	<p>Displays a pie chart showing the top reasons for failed authentications.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to determine the most common reasons why authentications are failing.</i></p>
Top Authentications Failed by IPs	<p>Displays a pie chart showing the ip addresses with the highest amount of failed authentications..</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to determine if a high number of failed authentications are originating from unknown Ip addresses..</i></p>





<p>Top Authenticated Users</p>	<p>Displays the users with the highest number of authentications..</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to determine which users are using the authentication solution the most.</i></p>
<p>Most Active Applications</p>	<p>Displays the # of authentications for each configured application.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to determine which applications receive the highest amount of authentication traffic.</i></p>
<p>Authentication Status in the Last 24 Hours</p>	<p>Displays a pie chart showing the number of occurrences for each authentication status.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to determine the most common authentication statuses.</i></p>
<p>Users with Failed Authentications</p>	<p>Displays a table of the users with the most failed authentications and their originating ip address.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to help detect authentications for users coming from unknown ip addresses.</i></p>
<p>Authentications left as no response by Users</p>	<p>Displays a table of authentications that the user did not respond to</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used in collaboration with other modules to help detect authentications that may have been attempted outside of standard waking hours and have thus been left with no response.</i></p>
<p>Users with Invalid Passcode</p>	<p>Displays a table of authentications that failed because the user inputted an invalid passcode.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to detect if attackers are attempting to login to a user's account with invalid credentials.</i></p>
<p>Locked Out Users</p>	<p>Displays a table of users that have been locked out of their account.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to indicate which users have been locked out of their accounts.</i></p>
<p>Anomalous push by Users</p>	<p>Displays table of anomalous push incidents for each user.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to indicate if any anomalous pushes have been detected and for which user(s), if any.</i></p>





<p>Call timed out by Users</p>	<p>Displays a table of timed out authentications for each user..</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to determine which users are allowing authentications to time out..</i></p>
<p>Authentications Canceled by the Users</p>	<p>Displays a table of authentications that were canceled by the user..</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to determine which users are canceling authentication requests.</i></p>
<p>Most successful Authenticated Countries</p>	<p>Displays a map showing the countries that have the highest number of successful authentications.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to quickly spot when successful authentications occur in anomalous countries.</i></p>
<p>Countries with Most Failed Authentications</p>	<p>Displays a map showing the countries that have the highest number of failed authentications.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to quickly spot if failed authentications are occurring in anomalous countries..</i></p>
<p>2nd Screen</p>	
<p>Trusted Access in Last 6 Months</p>	<p>Displays a line graph showing the frequency of authentication responses over the last 6 months.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to determine if there is a trend in the occurrence authentication statuses.</i></p>
<p>Successful and Failed Authentications</p>	<p>Displays the # of authentications for the current month and previous month.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to quickly assess the change in authentication activity between the current month and previous month.</i></p>
<p>Successful Authentications</p>	<p>Displays a pie chart showing the number of occurrences for every reason for a successful authentication.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to gather insight as to the most common reasons why authentications are successful.</i></p>
<p>Successful Authentications by Factor</p>	<p>Displays a pie chart showing the number of times each authentication factor is used in a successful authentication.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p>





	<i>This information can be used to gather insight as to the most common authentication factors used in successful authentications.</i>
Authentication Per Country	<p>Displays a pie chart showing the number of authentications detected per country.</p> <p>For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours.</p> <p><i>This information can be used to gather insight as to which countries generate the most authentication traffic.</i></p>
REPORT	This action button will generate a MSS-TAS REPORT based on the data of the dashboard with the corresponding TLP AMBER designation.
Manual	Presents this document.

