MANAGED TRUSTED ACCESS SERVICE (MSS-TAS)

V062623

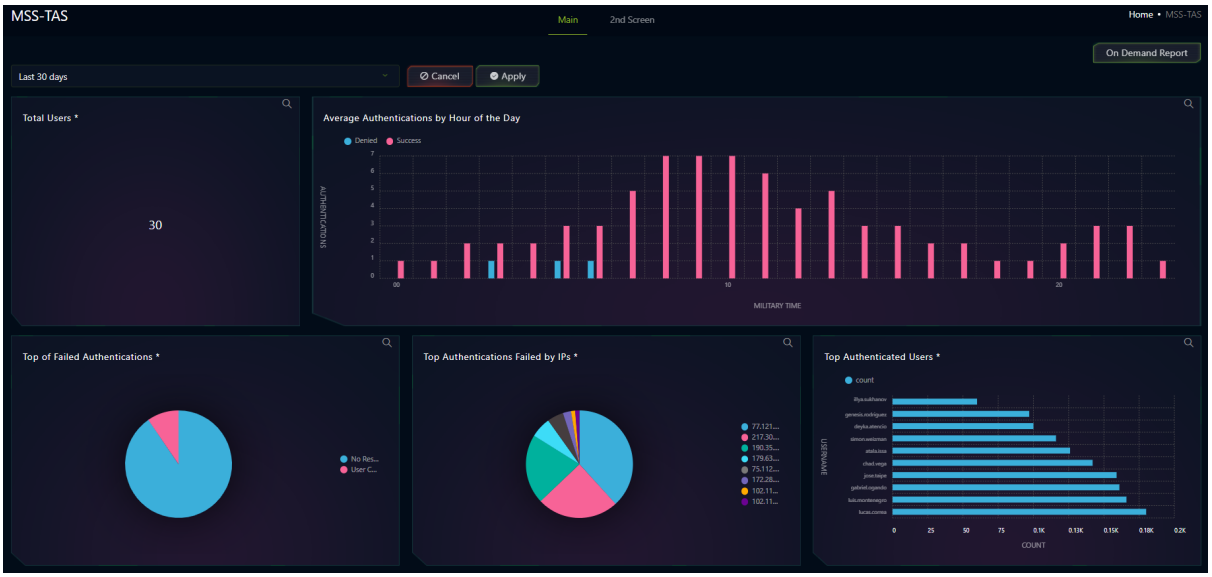
Revision V062623

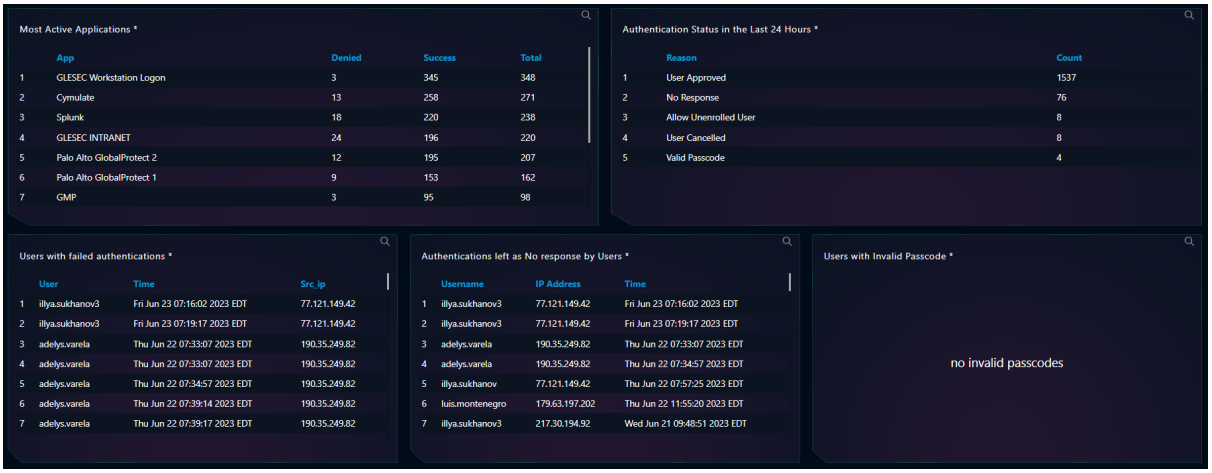
This document is a briefing that describes the operation and use of the Managed Trusted Access Service Protection, and it is meant for all users of SKYWATCH WEB Platform.

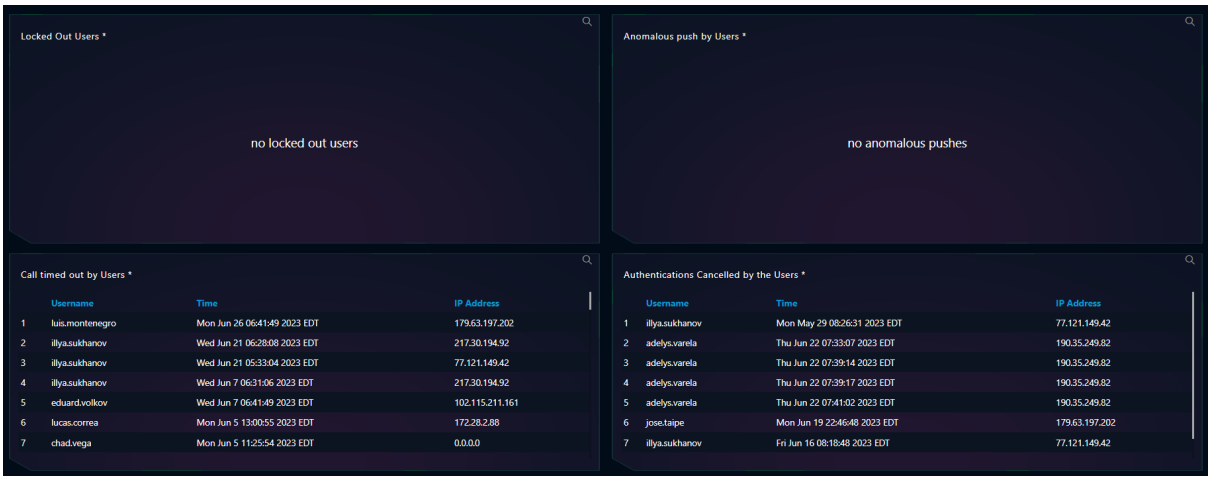
Purpose of this Dashboard

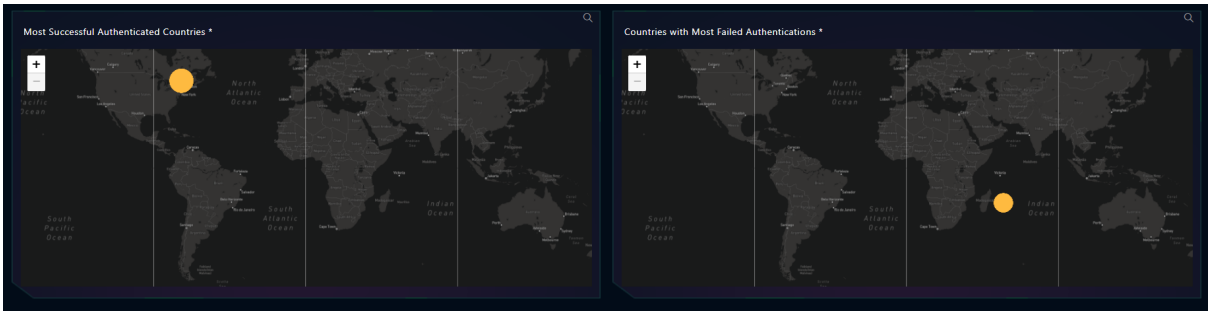
This SKYWATCH Dashboard(s) provide **visibility** to the technical and executive users of SKYWATCH for the **MSS-TAS** Service and the ability to generate an on-demand **report** for this service (with the information of the dashboard). These are two of deliverables for the service. There are more consolidated 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



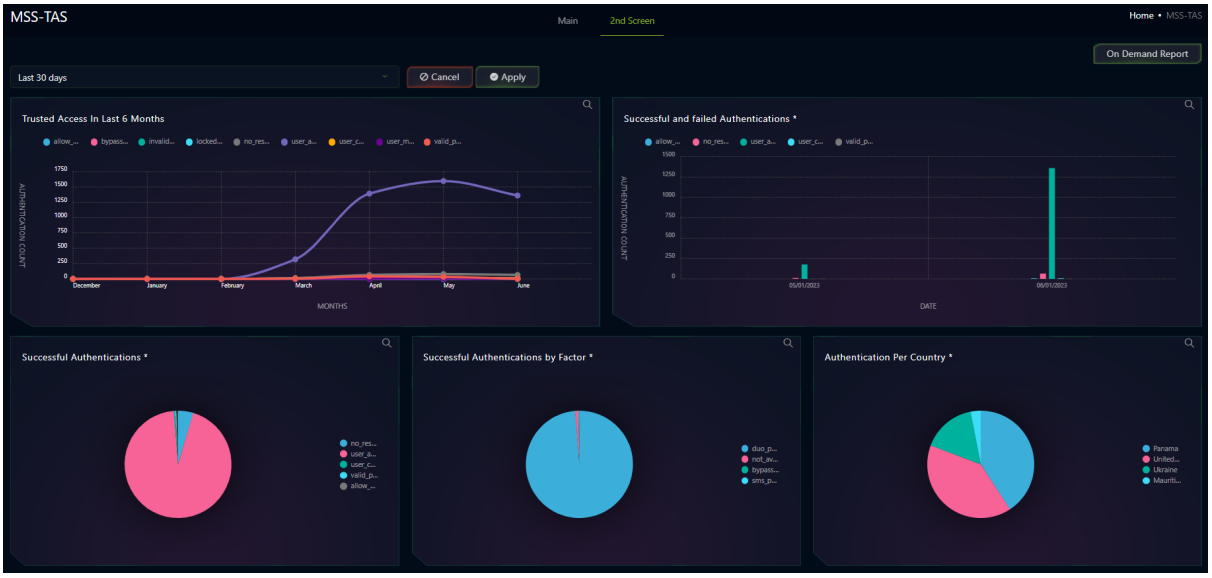






LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500



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

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

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

	This information can be used to gather insight as to the most common authentication factors used in successful authentications.
Authentication Per Country	Displays a pie chart showing the number of authentications detected per country. For the SKYWATCH WEB the refresh rate is once a day. The information represents data from last 24 hours. ***This information can be used to gather insight as to which countries generate the most authentication traffic.***
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.