**About this experience**

Review the Secure Score tool in your tenant and learn how to improve your security position and then get the Secure Score of your tenant with the API.

**Introducing Secure Score**

**Office 365 Secure Score** provides visibility into your Office 365 security position and ways to improve it.

In this section, you will see some of the feature that are included in Secure Score.

We will be:

* Reviewing a secure score
* Modeling how we can increase the score
* Comparing the score with the average Office 365 score
* Reviewing our historical score and the actions we have taken to get that score.

**Dashboard**

|  |  |
| --- | --- |
| **Demo Script** | **Click Steps** |
| To start things off, here's how you can find **Secure Score.** You go to <https://securescore.office.com> and here you need to provide global administrative credentials.  Once I have authenticated, you see the Secure Score **Dashboard**.  First you will see you Secure Score Summary showing your score. The numerator is the total points you have based on the security features you have enabled. The denominator is the maximum number of points you can acquire if you enabled all features your tenant has access to.  To the right of the summary is information on what is new and the current attack risks that you could be mitigating better.  To learn more about each of these risks you could click on them to see some additional information.  You can also learn about how your score stacks up against the average Office 365 score in the comparison window under the risk assessment.  Secure Score also shares with you suggestions around how you can improve your score with the Action Pane.  In the pane you can see a target score of X and this is based on the slider underneath it. Moving the slider to the right or left will increase or decrease the number of actions in your list and adjust the target score.  Suggestions are prioritized based on the effectiveness of the action and level of impact to end users. Actions that are highly effective with low level of user impact are placed at the top, followed by actions that are less effective and more impactful to users.  You can also filter actions in the list with criteria such as actions that have low end user impact, or actions that apply to user accounts. The target score adjusts dynamically based on your selection to show you how much your score will increase if you take all of the actions in the queue. The target score adjusts dynamically based on your selection to show you how much your score will increase if you take all of the actions in the queue.  If you click on an action in the queue you can see more details about that action include a description of what the recommendation is, what threat is being mitigated, and what is the status of that action in your organization. If you need more information, click 'Learn More' to open a pane with additional explanation.  Secure Score also tracks your score over time. Let's see what looks like with the Score Analyzer. | * 1. Go to <http://securescore.office.com> and login with the global admin account for your demo tenant.                    * 1. Click on one of the **risk assessment** links      * 1. Review the **compare your score** box            * 1. **Move the slider in the action pane** left and right to show the target score change   2. Review the actions in the queue          * 1. Use the **filter drop down** box to scope the actions show only low user impact actions   2. Click on an action in the queue      * 1. Click the **Learn More button** to get additional details on the action      * 1. Close the Learn More box and click on the Score Analyzer tab at the top of the page |

**Score Analyzer**

|  |  |
| --- | --- |
| **Demo Script** | **Click Steps** |
| The Score Analyzer consist of a few parts. First you see the graph which allows you to view your past scores and compare it to average score. You can choose a custom date range or click one of the pre-built filters.  When you click on a specific date in the graph you will see the score on that date and a table on how your score was calculated based on the three categories of actions: account, data and device.  Below this table are the specific actions you completed on this date and how many points you accrued for this action along with all the other actions that were available to you but did not complete.  To make sharing the actions you have completed with the rest of your team or your leadership easier you can export this information out to a CSV or PDF file.  As you can see Office 365 Secure Score provides visibility into your Office 365 security position and ways to improve it.  In this walkthrough, you have seen you how you can:  • Review a secure score  • Model how you can increase your score  • Compare your score with the average Office 365 score  • Review your historical score and the actions you have taken to get that score. | * 1. Click on one of the **filters** (7 days, 30 days, or 3 months)      * 1. **Click on a date** and **show the table below the graph** that outlines how the score was calculated.        * 1. Scroll down to All Actions box and **show the completed actions and incomplete actions tabs**.      * 1. Scroll back up and **press export button** to the right of the date filters in the graph and choose – **PDF Action List** and review the generated PDF |

**Acquire the secure score of your tenant with the API**

Ok - but why would partners want to do this?

1. Monitor and report on your secure score in downstream reporting tools.
2. Track your security configuration baseline.
3. Integrate the data into compliance or cybersecurity insurance applications.
4. Integrate Secure Score data into your SIEM or CASB to drive a hybrid or multi-cloud framework for security analytics.

Acquiring the secure score data from the API in a secure way requires you to setup a few pre-requisites.

To get the data we will need to choose a consumption model either a Service-To-Service Authentication model or a user OAuth model. For our purposes today let’s opt for the user OAuth model which will require an administrator to provide their logon credentials each time you pull data from the Secure Score API. Reference information about this model is located here: <https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-v2-protocols-oauth-code>.

Next, we will need to register an application in Azure Active Directory (AAD) in order to call the Secure Score API. The steps to create this application are below:

Navigate to AAD Portal, select your tenant directory, click App registrations, click New application registration

Machine generated alternative text:
Microsoft Azure 
Dashboard 
All resources 
(O) Resource groups 
App Services 
Function Apps 
SQL databases 
Azure Cosmos DB 
Virtual machines 
Load balancers 
Storage accounts 
Virtual networks 
contoso ems932138 - App registrations 
contoso ems932138 
Ove rview 
Quick start 
Users and groups 
Enterprise applications 
Devices (Preview) 
App registrations 
Application proxy 
Licenses 
Azure AD Connect 
Domain names 
App registrations 
New application registration 
Endpoints Troubleshoot 
To view and manage your registrations for converged applications, please visit the Microsoft Application 
Console. 
Search by name or App/d 
DISPLAY NAME 
Twitter 
BrowserStack 
Linkedin 
APPLICATION TYPE 
Web app / API 
Web app / API 
Web app / API 
Web app / API 
All apps 
APPLICATION ID 
f5fdfb60-85db-4c5g-95b7-64bd... 
dcOfb1e6-OßO-4C42-87d5-db97... 
82db6ebe-2157-4325-aOc5-36a... 
26cd8e81-93ad-4bge-ogc3-658f... 
Azure Active Directory 
Monitor 
Advisor 
Security Center 
O Billing 
Help + support 
More services > 
ability (MOM and MAM) 
Password reset 
Company branding 
User settings 
Properties 
Notifications settings 
SECURITY 
Conditional access 
Users flagged for risk 

Give an App Name, pick an Application type of **Native**, and a Redirect URI of <https://securescoreapi> will do and click **Create**.

Machine generated alternative text:
Microsoft Azure 
Dashboard 
All resources 
(O) Resource groups 
App Services 
Function Apps 
SQL databases 
Azure Cosmos DB 
Virtual machines 
Load balancers 
Storage accounts 
Virtual networks 
contoso ems932138 - App registrations 
> 
Create 
Azure Active Directory 
Monitor 
Advisor 
Security Center 
O Billing 
Help + support 
More services > 
Create 
* Name O 
Secu reScoreAPIDemo 
Application type O 
Native 
* Redirect URI O 
https://securescoreapi 
Create 

Select your app..

Machine generated alternative text:
Microsoft Azure 
Dashboard 
All resources 
(O) Resource groups 
App Services 
Function Apps 
SQL databases 
Azure Cosmos DB 
Virtual machines 
Load balancers 
Storage accounts 
Virtual networks 
contoso ems932138 - App registrations 
contoso ems932138 
Azure 
Ove rview 
Quick start 
Users and groups 
Enterprise applications 
Devices (Preview) 
App registrations 
Application proxy 
Licenses 
Azure AD Connect 
Domain names 
App registrations 
New application registration 
Endpoints Troubleshoot 
To view and manage your registrations for converged applications, please visit the Microsoft Application 
Console. 
Search by name or App/d 
DISPLAY NAME 
Twitter 
BrowserStack 
Linkedin 
Secure ScoreAPIDemo 
APPLICATION TYPE 
Web app / API 
Web app / API 
Web app / API 
Web app / API 
Web app / API 
All apps 
APPLICATION ID 
f5fdfb60-85db-4c5g-95b7-64bd... 
dcOfb1e6-OßO-4C42-87d5-db97... 
82db6ebe-2157-4325-aOc5-36a... 
26cd8e81-93ad-4bge-ogc3-658f... 
3b7age53-7Cc5-40bg-a961-d01f... 
Azure Active Directory 
Mobility (MOM and MAM) 
Password reset 
Company branding 

Now let's grant some permissions. Click on **Required permissions** and select Microsoft Graph API and then select ***Read all usage reports*** permissions to your application.

Machine generated alternative text:
Settings 
Required permissions 
+ Add Grant Perm issions 
Windows Azure Active Directory 
Required permissions 
Add API access 
Enable Access 
p Search resources 
Add API access 
Select an API 
Microsoft Graph 
Select permissions 
O role, I scope 
Done 
O 
X 
APPLICATION PERMIm 
DELEGATED PERMISm 
Enable Access 
NeaC all groups 
Read and write all users' full profiles 
Read all users' full profiles 
Read all users' basic profiles 
Read and write access to user profile 
Sign in and read user profile 
Read user and shared mail 
Read and write user and shared mail 
Send mail on behalf of others 
Read user and shared calendars 
Read and write user and shared calendars 
Read user and shared contacts 
Read and write user and shared contacts 
Read user and shared tasks 
Read and write user and shared tasks 
Edit or delete items in all site collections 
Read all usage reports 
Have full access to the application's folder (preview) 
Read and write files that the user selects (preview) 
Read files that the user selects (preview) 
Select 
admin@EMS932138.o... 
CONTOSO EMS932138 
Yes 
Yes 
Yes 
Yes 

Click **Select**, **Done** and then **Grant Permissions**

Machine generated alternative text:
rescoreAPlDemo 
Settings 
Required permissions 
Required permissions 
+ Add Grant Perm issions 
Do you want to grant the permissions below for SecureScoreAPlDemo for all 
accounts in current directory? This action will update any existing permissions this 
application already has to match what is listed below. 

Take note of the Application Id and the Redirect Uri of your app - you will need them in the script.

Now that you have fulfilled all the pre-requisites, you are ready to pull the data!

All sample code and documentation about the Secure Score API can be found here: <https://github.com/OfficeDev/O365-Cloud-Sec-Tooling>

**Get Secure Score with Interactive Logon**: <https://github.com/OfficeDev/O365-Cloud-Sec-Tooling/blob/master/Securescore/GetSecureScoreFromAPI-ADAL.ps1>

This script will install a local ADAL library from GIT, then do a local prompt for credentials. If your global admin account requires MFA, this implementation will respect that. You will need to populate your Client ID and Redirect URL from above in the function called "Get-AuthenticationResult". The script currently dumps out the last 9 days of Secure Score results to the console. You can edit (a local copy of) the script to do anything else you like, including converting to CSV, or integrating into a different data store.

* Add your clientId (Application Id) and redirectUri to the getsecurescorefromapi-adal.ps1 script.
* Run the powershell script - ./getsecurescorefromapi-adal.ps1
* Your securescore in the report should match what you see in the UI securescore.office.com

Machine generated alternative text:
EXPLORER 
OPEN EDITORS 
Welcome 
Secure Score Demo API.ps1 Secure.. 
GetSecureScoreFromAPl-ADAL.ps... 
G) READMEmd Securescore 
0365-CLOUD-SEC-TOOUNG 
Securescore 
ConfigForSecureScoreAPl.json 
DEPRECATED-LEGACYSecureScoreC.. 
GetSecureScoreAPl-S2S.ps1 
GetSecureScoreFromAPl -ADALps1 
G) READMEmd 
Secure Score Demo API.ps1 
securescore_get.md 
0 READMEmd 
DO Welcome 
1 reference 
Secure Score Demo API.ps1 
> GetSecureScoreFromAPl-ADALps1 X 
@ READMEmd 
34 
35 
36 
38 
39 
41 
42 
43 
44 
45 
46 
47 
48 
51 
function Get-AuthenticationResu1t($tenant = 
#your client id 
"common", $env= "prod") { 
$clientld 
"cd735e86-b123-4b0f-9914-3ca69afcb897" 
#your app redirect Uri 
$redirectUri 
"https : / / securescoreapi " 
$resourceAppIdURI 
"https : / (graph . microsoft . com/" 
$authority 
"https://login.windows.net/" + $tenant 
$authContext = New-Object "Microsoft. IdentityMode1.C1ients.ActiveDirectory.AuthenticationContext" -ArgumentList $authority,$false 
$authResu1t - 
$ authContext . AcquireToken ( $ resourceAppIdURI, 
$clientld, 
$redirectUri, [Microsoft. IdentityMode1. Clients. ActiveDirectory . PromptBeh 
return $authResu1t 
1 reference 
function Connect-AAD ($tenant = 
PROCESS { 
$global : aadGPoShAuthResu1t 
$global :aadGPoShEnv = $env 
" common " 
$null 
$en'& "prod" , 
$graphVer="beta") { 
$global : aadGPoShGraphVer 
$graphVer 
$global :aadGPoShGraphUr1 - 
"https://graph . microsoft . com/" 
PROBLEMS 
OUTPUT 
DEBUG CONSOLE 
: 24 
: 47 
: 43 
TERMINAL 
licensedUserCount 
activeUserCount 
secureScore 
maxSecureScore 
accountScore 
dataScore 
deviceScore 
enabledServices 
controlScores 
. {HasExchange, HasLync, HasSharePoint, HasOD4B.. 
. {@{referenceId=AdminMFA; score=1Ø; maxScore=5Ø; 
controlDetai1s=}, @{referenceId=UserMFA; score=2; 
2: PowerShell Integrated 
maxScore=3Ø; controlDetai1s=} 
score=2Ø; maxScore=2Ø; 
@{referenceId=A1tInfoIncomp1ete; score—I; maxScore=1; controlDetai1s=}, @{referenceId=DLPEnab1ed; 
controlDetai1s=} ... } 
averageSecureScore 
: 42.60029 
averageMaxSecureScore • 
. 422.946747 
averageAccountScore 
: 22.05521 
averageDataScore 
: 18.8462429 
averageDevi ceScore 
: 1.6988349 
PS C:\Users\mipancir\Documents\Dev\Git\0365-C10ud-Sec-T001ing\securescore> 



Machine generated alternative text:
Your Secure Score Summary 
Your Secure Score is: 
Of 364 
Take action to see how you can improve your score 
today 
SEP 13 
2017 
5:00 PM 
90 
For more information about your Secure Score 
go to: Score Analyzer. 

That’s it - they match! For more info check out the rest of the code in the repo and this blog article that this lab is ~~copied from~~ inspired by - <https://blogs.technet.microsoft.com/office365security/using-the-office-365-secure-score-api/>