

Installing and configuring the Office 365 module

Installation

The Microsoft 365 Web plugin is not installed by default on Esia platforms. You must first install the corresponding package. Connect using SSH with a root account on your Esia server. Type the following commands

copy

```
apt update
apt install esia-webp-office365
```

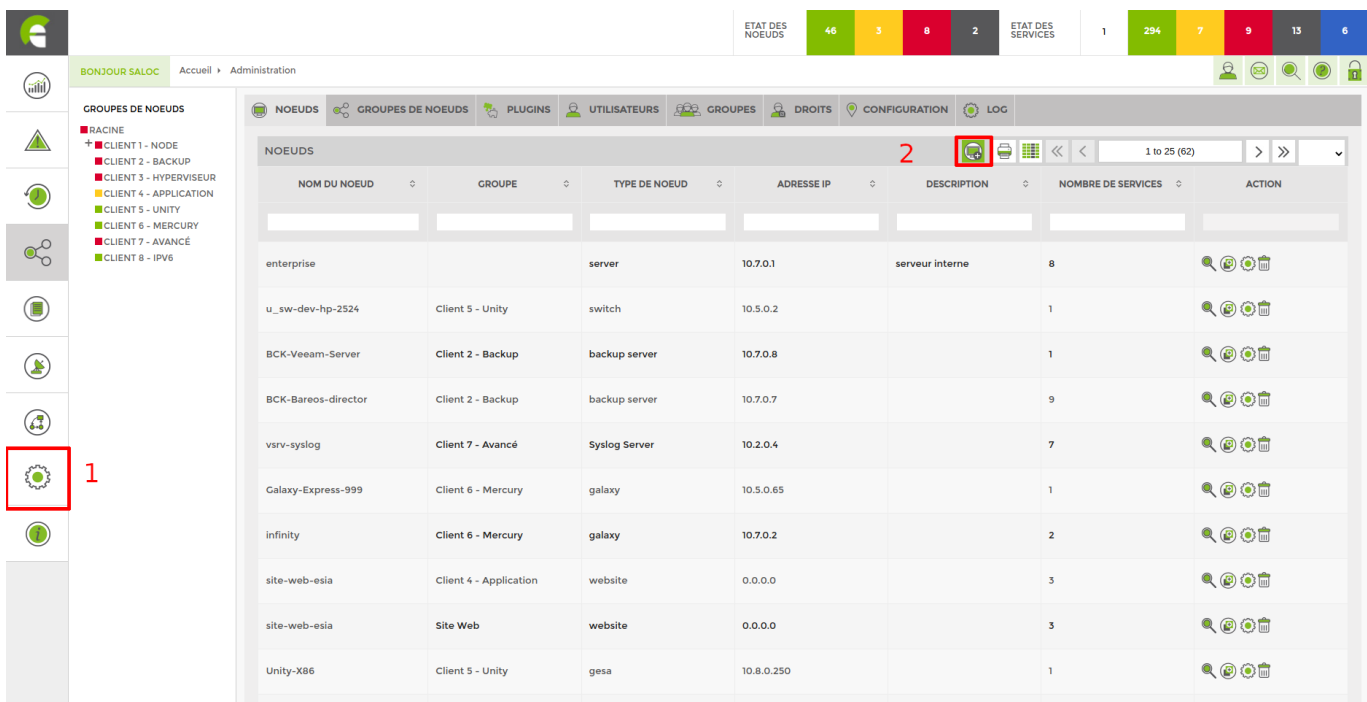
If it does not find the package, the Esia repository has not been added to your server. You can add it by following the corresponding part of the following tutorial: [Installing an Esia Galaxy server](#)

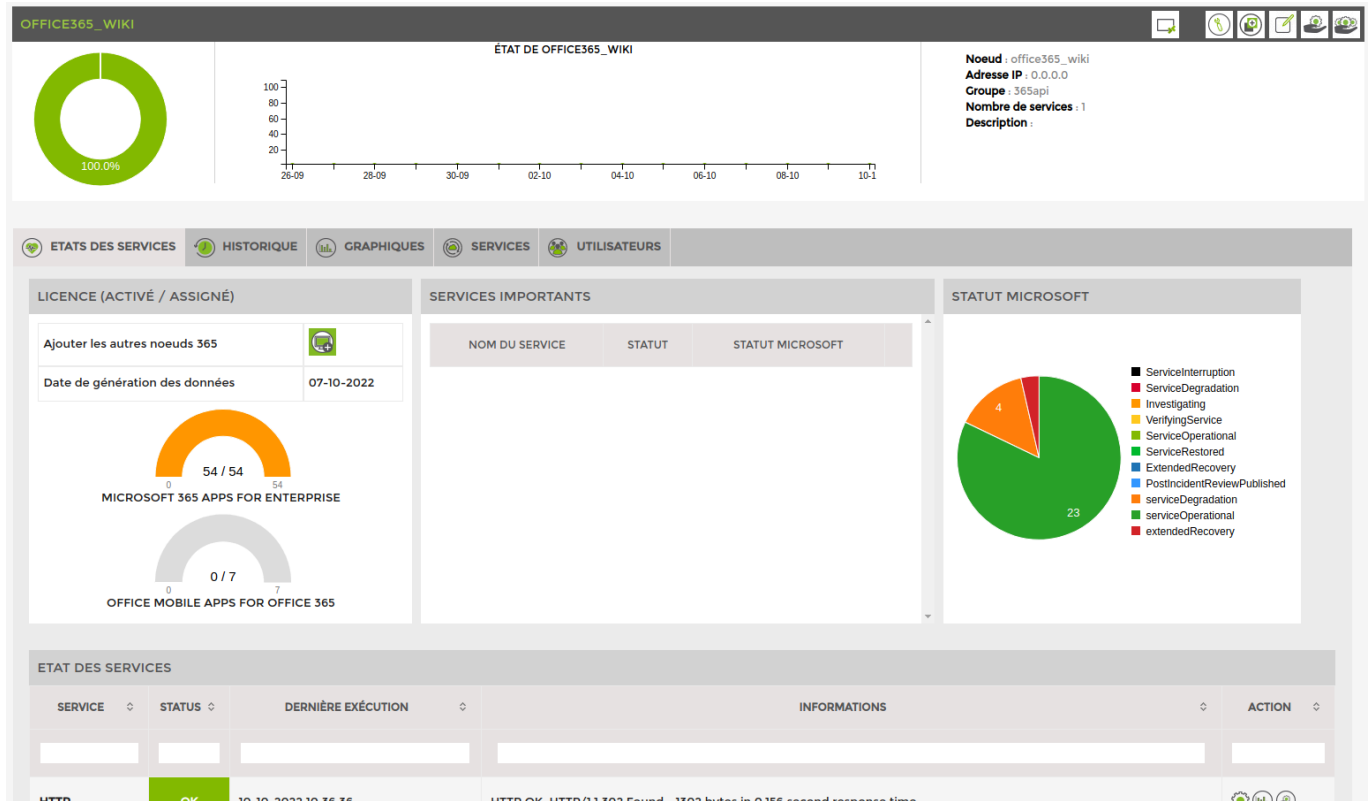
Once installed, go to the Esia administration WEB interface.

Configuration

Before configuring the node, you must authorise Esia to contact your Office 365 instance. You can follow the tutorial below: [Microsoft Office 365](#)

In the Esia administration interface, click on “Add Node”.





3 new services have been added and will monitor the status of Microsoft services.

Select the services you want to monitor. I've chosen to monitor Exchange, Teams and Sharepoint in this tutorial. Once you've done this, click on "Add service(s)".

<input type="checkbox"/>	NOM DU SERVICE	STATUT	STATUT MICROSOFT	DETAIL
<input checked="" type="checkbox"/>	Exchange Online	WARNING	serviceDegradation	
<input type="checkbox"/>	Identity Service	OK	serviceOperational	
<input type="checkbox"/>	Microsoft 365 suite	WARNING	serviceDegradation	
<input type="checkbox"/>	Skype for Business	OK	serviceOperational	
<input checked="" type="checkbox"/>	SharePoint Online	WARNING	serviceDegradation	
<input type="checkbox"/>	Dynamics 365 Apps	OK	serviceOperational	
<input type="checkbox"/>	Azure Information Protection	OK	serviceOperational	
<input type="checkbox"/>	Yammer Enterprise	OK	serviceOperational	
<input type="checkbox"/>	Mobile Device Management for Office 365	OK	serviceOperational	
<input type="checkbox"/>	Planner	OK	serviceOperational	
<input type="checkbox"/>	Sway	OK	serviceOperational	

Add the other office 365 nodes

There's more than just the basic Office 365 view available. You can also add the following views:

- Exchange
- Onedrive
- SharePoint
- Teams

To do this, click on "Add other 365 nodes".

NOM DU SERVICE	STATUT	STATUT MICROSOFT
Exchange Online	WARNING	serviceDegradation
Microsoft Teams is Status	WARNING	extendedRecovery
SharePoint Online	WARNING	serviceDegradation

The next page appears:

SERVICE: ONE DRIVE
 Nom du noeud
office365_wiki-One Drive

SERVICE: SHARE POINT
 Nom du noeud
office365_wiki-Share Point

SERVICE: EXCHANGE
 Nom du noeud
office365_wiki-Exchange

SERVICE: TEAMS
 Nom du noeud
office365_wiki-Teams

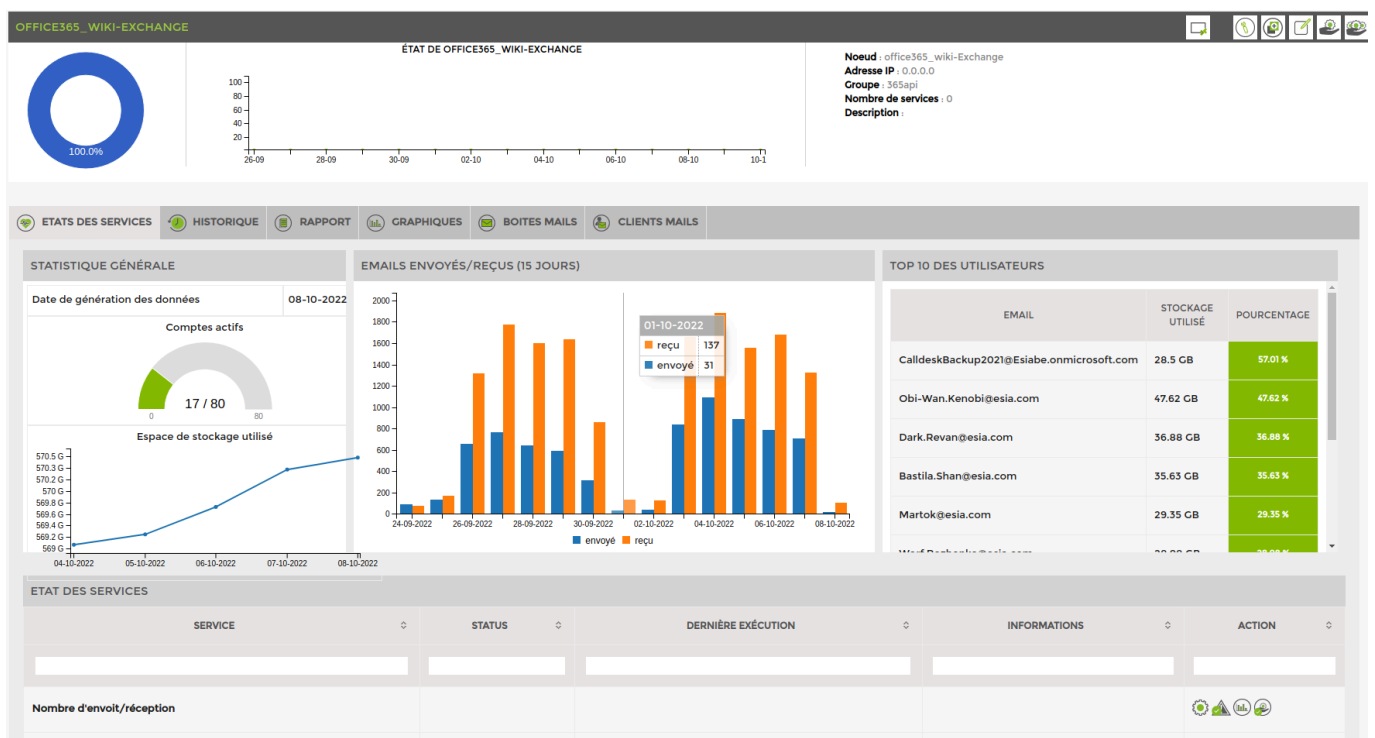
Select the nodes you want to add, and if necessary change their name and the group to which they will be added (by default: the same as your original Office 365 node).

Once you have done this, click on "Add" and close the window. The nodes will be automatically added with the following elements:

Exchange


Here is the available view and 2 services are automatically added:

- Mailbox usage: turns yellow or red if the mailbox has reached its quota or is blocked.
- Number of mails sent/received: test the number of mails sent/received daily by default the alert and critical values are 1500 and 2000 mails.

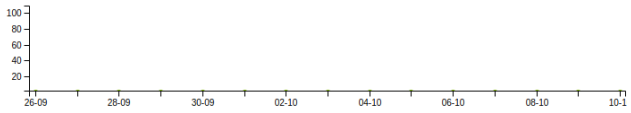


Onedrive

Here is the available view and 1 service is automatically added. It tests OneDrive's global storage space



ÉTAT DE OFFICE365_WIKI-ONE DRIVE



Noeud : office365_wiki-One Drive
Adresse IP : 0.0.0.0
Groupe : 365api
Nombre de services : 1
Description :

ÉTATS DES SERVICES |
 HISTORIQUE |
 RAPPORT |
 GRAPHIQUES |
 ACTIVITÉ SUR LES FICHIERS |
 UTILISATEURS

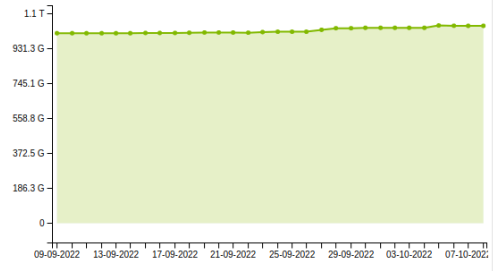
STATISTIQUE GÉNÉRALE

Date des données	08-10-2022
Nombre de fichier total	490 910
Nombre de fichier actif	98
Total utilisateur	61
Utilisateur actif	9

TOP 10: ESPACE UTILISÉ

Feanor Atthis	315.21 GB	31 %
Jack O'Neil	228.5 GB	22 %
Thomas Whitmore	108.99 GB	11 %
Obi-Wan Kenobi	97.21 GB	9 %
Martok	72.94 GB	7 %
Bastila Shan	50.28 GB	5 %
B'Elanna Torres	41.07 GB	4 %

ESPACE DE STOCKAGE UTILISÉ

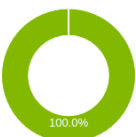


ÉTAT DES SERVICES

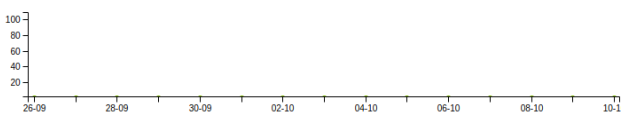
SERVICE	STATUS	DERNIÈRE EXÉCUTION	INFORMATIONS	ACTION
Espace de stockage	Critique	10-10-2022 11:59:39	CRITICAL: storage used 103% (1052.5GB) on 1024GB > 90	

Sharepoint

Here is the available view and 1 service is automatically added. It tests the global storage space of all Sharepoint sites.



ÉTAT DE OFFICE365_WIKI-SHARE POINT



Noeud : office365_wiki-Share Point
Adresse IP : 0.0.0.0
Groupe : 365api
Nombre de services : 1
Description :

ÉTATS DES SERVICES |
 HISTORIQUE |
 RAPPORT |
 GRAPHIQUES |
 ACTIVITÉ SUR LES FICHIERS |
 DÉTAIL DES SITES

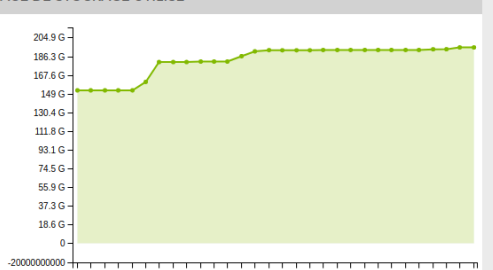
STATISTIQUE GÉNÉRALE

Date des données	10-10-2022
Nombre de fichier total	0
Nombre de fichier actif (1 jour)	null
Nombre de page vue (7 jours)	14
Fichier actifs (7 jours)	2307
Nombre de page visitée (7 jours)	8

TOP 10 DES PLUS GROS SITE

Propriétaires de Produits	139.63 GB
Propriétaires de webcom2you	48.85 GB
Propriétaires de Esia Group (Teams)	2.62 GB
Propriétaires de Prestataires	2.14 GB
Propriétaires de Commerciale	963.72 MB
Propriétaires de Admin_Compta	721.83 MB
Test Réseaux sociaux	56.46 MB

ESPACE DE STOCKAGE UTILISÉ

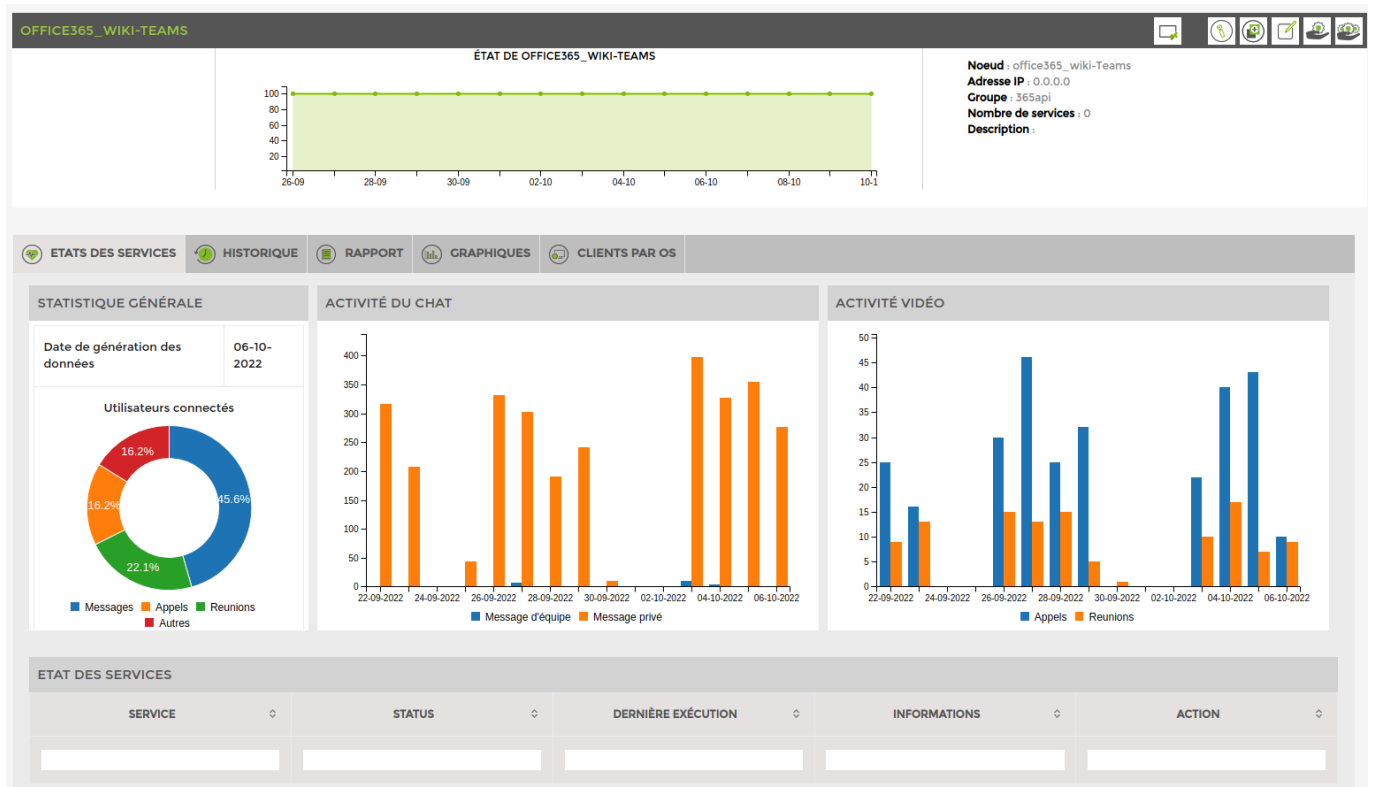


ÉTAT DES SERVICES

SERVICE	STATUS	DERNIÈRE EXÉCUTION	INFORMATIONS	ACTION
Espace de stockage	OK	10-10-2022 11:59:15	OK: storage used 19% (195.1GB) on 1TB < 80	

Teams

Here's the available view.



Defender

Requires a Svalinn license (Available from Esia version 3.5.2)

“Microsoft Graphics” API access rights :

- SecurityEvents.Read.All
- SecurityAlert.Read.All
- SecurityIncident.Read.All
- AuditLog.Read.All

[Check the tutorial on configuring permissions.](#)

Plugins

Plugins added on node creation :

- **Active alerts** (CHECK_API_M365_SECURITY_ALERT_ACTIVE) :

Status “alert” or “critical” depending on the number of active alerts.

- **Recent alerts** (CHECK_API_M365_SECURITY_ALERT_COUNT) :

Status “alert” or “critical” depending on the number of alerts (of all types, not just active ones) that have occurred over a period of time. Default is 1 day.

- **Active incidents** (CHECK_API_M365_SECURITY_INCIDENT_ACTIVE) :

Status “alert” or “critical” depending on the number of active incidents.

- **Recent incidents** (CHECK_API_M365_SECURITY_INCIDENT_COUNT) :

Status “alert” or “critical” depending on the number of incidents (of all types, not just active ones) that have occurred over a period of time. Default is 1 day.

- **Secure Score** (CHECK_API_M365_SECURITY_SECURESCORE) :

Status “alert” or “critical” depending on the SecureScore percentage value.

- **Valide authentication - MFA** (CHECK_API_M365_SECURITY_USERS_AUTH_COUNT) :

Status “alert” or “critical” depending on the number of users who have **not** configured valid multi-factor authentication.

Other plugins available :

- **Valide authentication - SSPR** (CHECK_API_M365_SECURITY_USERS_AUTH_COUNT) :

Status “alert” or “critical” depending on the number of users who have **not** configured valid self-service password reset (SSPR).

Add the plugin, then change the parameter “method=mfa” to “**method=sspr**”

Exemple : -A \$AUTH_FILE_OFFICE365 -t security -n usersAuthMethodCount -a **method=sspr** -w 1 -c 3

- **Valide authentication - PasswordLess**
(CHECK_API_M365_SECURITY_USERS_AUTH_COUNT) :

Status “alert” or “critical” depending on the number of users who have **not** configured valid password less.

Add the plugin, then change the parameter “method=mfa” to “**method=passwordless**”

Exemple : -A \$AUTH_FILE_OFFICE365 -t security -n usersAuthMethodCount -a **method=passwordless** -w 1 -c 3

For the **CHECK_API_M365_SECURITY_USERS_AUTH_COUNT** plugin (MFA, SSPR or PasswordLess), you can test a specific user type by adding the parameter `type=<$type>` (inside the `-a`). Here are the available types :

- **admin** ⇒ Only users who are administrators

Exemple : `-A $AUTH_FILE_OFFICE365 -t security -n usersAuthMethodCount -a method=mfa,type=admin -w 1 -c 3`

- **member** ⇒ Only users who are of type “Member” (See the “Type” column of the table in the “Authentication” tab) **and not administrators**

Exemple : `-A $AUTH_FILE_OFFICE365 -t security -n usersAuthMethodCount -a method=mfa,type=member -w 1 -c 3`

- **guest** ⇒ Guest users only

Exemple : `-A $AUTH_FILE_OFFICE365 -t security -n usersAuthMethodCount -a method=mfa,type=guest -w 1 -c 3`

Several types can be combined, for example all “Administrator” users and “Member” (non-admin) users, so everyone except guests : `-A $AUTH_FILE_OFFICE365 -t security -n usersAuthMethodCount -a method=mfa,type=admin:member -w 1 -c 3`

Views

Here is the main view of the node :

OFFICE-DEFENDER

5 DERNIÈRES NOTES

Aucune note

[Ajouter une note](#)

Noeud : office-Defender
 Adresse IP : 0.0.0.0
 Groupe : Web
 Nombre de services : 6
 Description :

ETATS DES SERVICES | HISTORIQUE | GRAPHIQUES | NOTES | SECURE SCORE | ALERTES | INCIDENTS | AUTHENTIFICATION

STATISTIQUES GÉNÉRALE

Secure Score: **49.34%**

3 Incidents actifs | 0 Incidents sur 1 jour(s)

8 Alertes actives | 0 Alertes sur 1 jour(s)

1085 Nombre d'utilisateurs | 886 MFA valides

125 SSPR valides | 6 PasswordLess valides

LES 5 DERNIERS INCIDENTS ACTIFS

Unfamiliar sign-in properties involving one user	Actif	Haute
Initial access incident involving one user	Actif	Haute
Multi-stage incident involving Initial access & Credential access involving one user	Actif	Haute

SECURE SCORE

ETAT DES SERVICES

SERVICE	STATUS	DERNIÈRE EXÉCUTION	INFORMATIONS	PRISE EN CHARGE	ACTION
Alertes actives	Critique	<1 minutes	CRITICAL: There are 8 active alert(s) remaining (> 6)		
Alertes récentes	OK	<3 minutes	OK: No alerts have been reported over the past 1 day(s)		
Incidents actifs	Alerte	<3 minutes	WARNING: There are 3 active incident(s) remaining (> 1)		
Incidents récents	OK	<0 minutes	OK: No incidents have been reported over the past 1 day(s)		
Secure Score	Critique	<3 minutes	CRITICAL: Secure Score is Vulnerable at 49.34% (< 50)		
Authentification valide - MFA	Alerte	<2 minutes	WARNING: 199 users do not have valid MFA (> 1)		

SecureScore tab :

ETATS DES SERVICES | HISTORIQUE | GRAPHIQUES | NOTES | SECURE SCORE | ALERTES | INCIDENTS | AUTHENTIFICATION

SECURE SCORE : 49.34%

PROFILS DE CONTRÔLE

RANG	ACTION RECOMMANDÉE	IMPACT	SCORE	CATÉGORIE	PRODUIT	TYPE D'ACTION	MENACES
223	Enable 'Microsoft Defender for Endpoint Plug-in for WSL'	0.46%	0/5	Device	MDATP	Config	Inconnu
222	Enable Microsoft Defender Antivirus real-time behavior monitoring for Linux	0.46%	0/5	Device	MDATP	Config	Inconnu
221	Turn on Microsoft Defender Antivirus Tamper Protection for Linux	0.74%	0/8	Device	MDATP	Config	Inconnu
220	Enable Microsoft Defender Antivirus real-time behavior monitoring in macOS	0.46%	0/5	Device	MDATP	Config	Inconnu
219	Turn on Tamper Protection for MacOS	0.74%	0/8	Device	MDATP	Config	Inconnu
218	Block rebooting machine in Safe Mode	0.85%	0/9	Device	MDATP	Config	Inconnu

Alerts tab :

ALERTES D'ACTIVITÉS									
ID INCIDENT	TITRE	PRODUIT	DÉTECTÉ PAR	CATÉGORIE	STATUS	SÉVÉRITÉ	DERNIÈRE MODIFICATION	MITRE	ACTION
122	Unfamiliar sign-in properties	AAD Identity Protection	azureAdIdentity-Protection	InitialAccess	Résolu	Haute	30-01-2026 06:40:28	TI078 TI078.004	
121	Unfamiliar sign-in properties	AAD Identity Protection	azureAdIdentity-Protection	InitialAccess	Résolu	Haute	30-01-2026 06:40:12	TI078 TI078.004	
120	Unfamiliar sign-in properties	AAD Identity Protection	azureAdIdentity-Protection	InitialAccess	Résolu	Haute	30-01-2026 06:39:57	TI078 TI078.004	
119	Unfamiliar sign-in properties	AAD Identity Protection	azureAdIdentity-Protection	InitialAccess	Résolu	Haute	30-01-2026 06:39:45	TI078 TI078.004	
118	Unfamiliar sign-in properties	AAD Identity Protection	azureAdIdentity-Protection	InitialAccess	Nouveau	Haute	21-01-2026 12:48:39	TI078 TI078.004	
117	Anonymous IP address	AAD Identity Protection	azureAdIdentity-Protection	InitialAccess	Résolu	Moyenne	05-12-2025 09:11:17	Aucun	

Incidents tab :

LISTE D'INCIDENTS									
ID INCIDENT	TITRE	STATUS	SÉVÉRITÉ	DATE DE CRÉATION	DERNIÈRE MODIFICATION	ASSIGNÉE À	NATURE DE L'ATTAQUE	CLASSIFICATION	ACTION
122	Unfamiliar sign-in properties involving one user	Résolu	Haute	30-01-2026 06:40:28	30-01-2026 06:40:28	Inconnu	unknown	unknown	
121	Unfamiliar sign-in properties involving one user	Résolu	Haute	30-01-2026 06:40:11	30-01-2026 06:40:11	Inconnu	unknown	unknown	
120	Unfamiliar sign-in properties involving one user	Résolu	Haute	30-01-2026 06:39:56	30-01-2026 06:39:56	Inconnu	unknown	unknown	
119	Unfamiliar sign-in properties involving one user	Résolu	Haute	30-01-2026 06:39:45	30-01-2026 06:39:45	Inconnu	unknown	unknown	
118	Unfamiliar sign-in properties involving one user	Actif	Haute	21-01-2026 12:48:38	21-01-2026 12:48:39	Inconnu	unknown	unknown	
117	Anonymous IP address involving one user	Résolu	Moyenne	05-12-2025 09:11:16	05-12-2025 09:11:16	Inconnu	unknown	unknown	

Authentification tab :

MÉTHODES D'AUTHEMIFICATION DES UTILISATEURS							
UTILISATEUR	ADMINISTRATEUR	TYPE	MFA	SSPR	PASSWORDLESS	MÉTHODES	ZÈME FACTEUR
[REDACTED]	Oui	Membre	Valide	Désactivé	Désactivé	email officePhone microsoftAuthenticatorPush softwareOneTimePasscode	voiceOffice
[REDACTED]	Non	Membre	Valide	Désactivé	Désactivé	mobilePhone	sms
[REDACTED]	Non	Membre	Valide	Désactivé	Désactivé	mobilePhone	sms
[REDACTED]	Non	Membre	Désactivé	Désactivé	Désactivé	Aucun	Aucun
[REDACTED]	Non	Membre	Valide	Désactivé	Désactivé	mobilePhone	sms
[REDACTED]	Non	Membre	Valide	Désactivé	Désactivé	mobilePhone	sms
[REDACTED]	Oui	Membre	Valide	Désactivé	Désactivé	mobilePhone microsoftAuthenticatorPush softwareOneTimePasscode	push

From: <https://wiki.esia-sa.com/> - **Esia Wiki**

Permanent link: https://wiki.esia-sa.com/en/interface/module_o365

Last update: **2026/04/13 14:04**

