

Installation & Configuration du module Office 365

Installation

Le Web plugin Microsoft 365 n'est pas installé par défaut sur les plateformes Esia. Il faut commencer par installer le paquet correspondant. Connecter vous en SSH avec un compte root sur votre serveur Esia. Taper les commandes suivantes

copy

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

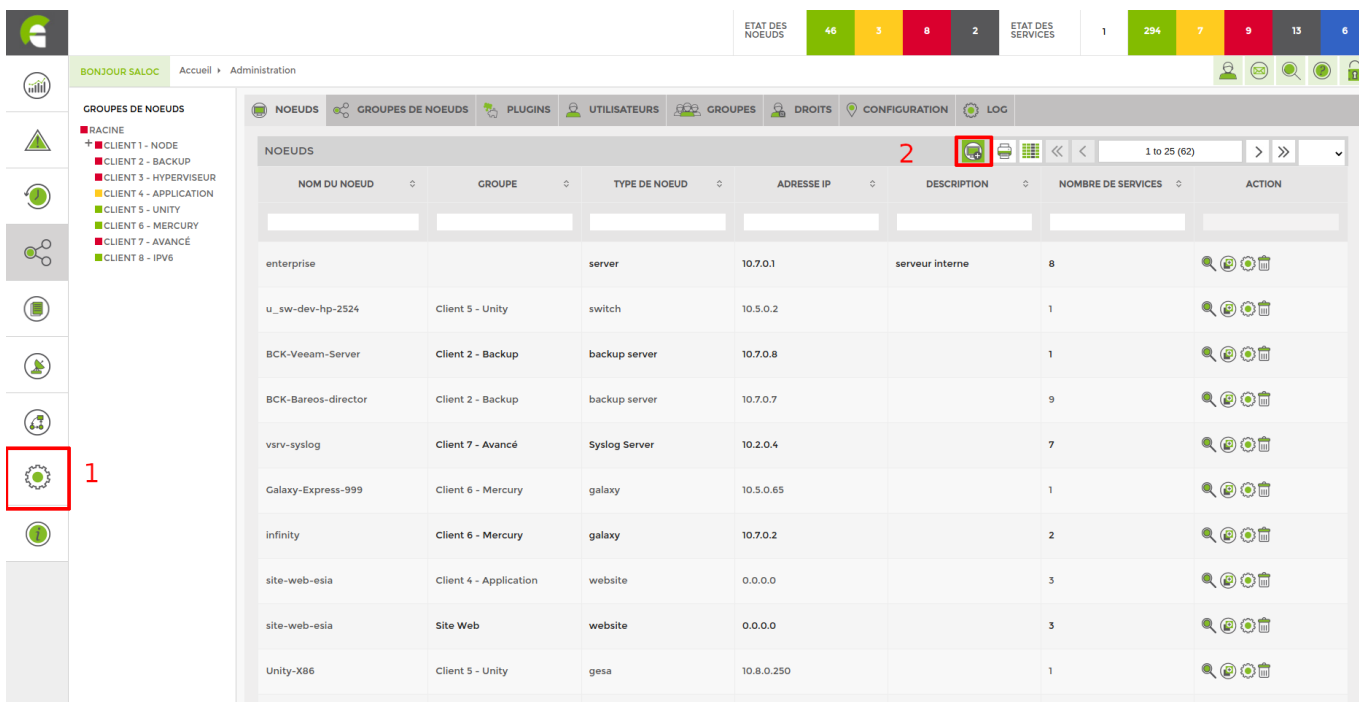
S'il ne trouve pas le paquet, c'est que le dépôt Esia n'est pas rajouter sur votre serveur. Vous pouvez le rajouter en suivant la partie correspondante dans le tuto suivant : [Installer un serveur Esia Galaxy](#)

Une fois installé aller dans l'interface WEB d'administration d'Esia.

Configuration

Avant de configurer le noeud, il faut autoriser Esia à contacter votre instance Office 365, vous pouvez suivre le tuto suivant: [Microsoft Office 365](#)

Dans l'interface d'administration d'Esia, cliquez sur "Ajouter Nœud".



Rentrez un nom pour votre nœud, et sélectionnez “Microsoft 365” en type de nœuds. N'oubliez pas de mettre votre nœuds dans un groupe. Pour terminer, cliquez sur “Ajouter”.

The screenshot shows a web form titled "AJOUTER UN NOEUD". It is divided into two main sections: "INFORMATIONS GÉNÉRALES" and "INFORMATIONS SNMP".

- INFORMATIONS GÉNÉRALES:**
 - Nom du nœud:** office365_wiki
 - Type de nœud:** Microsoft 365
 - Groupe:** 365api
 - Adresse IP:** 0.0.0.0
 - Connecté derrière la Unity:** none
 - Description:** (empty text area)
- INFORMATIONS SNMP:**
 - Version SNMP:** none

An "Ajouter" button is located at the bottom right of the form.

Il faut maintenant renseigner les 3 paramètres spécifiés (Tenant ID, Client ID et la clé). Cliquez ensuite sur “Sauver”.

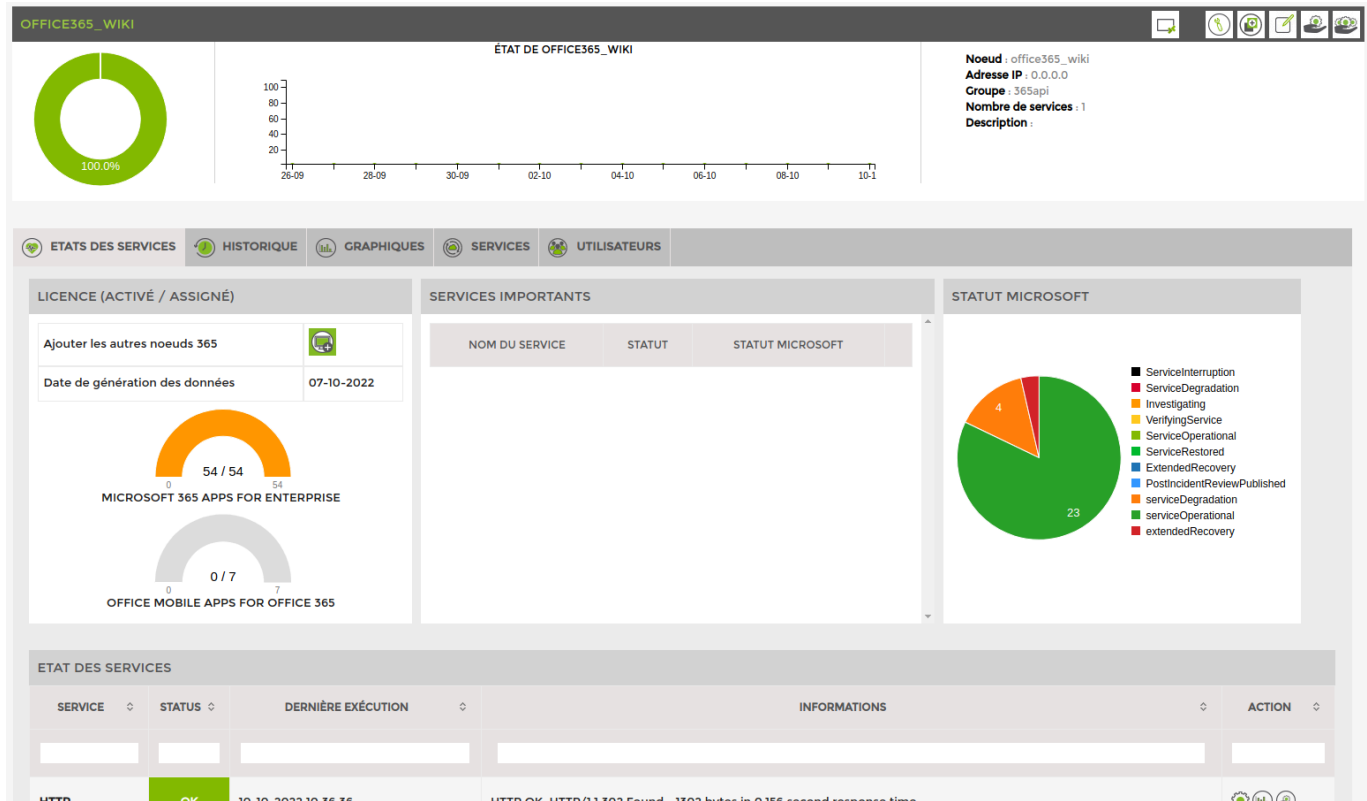
The screenshot shows the "CONFIGURATION CLIENT ID" section of the "AJOUTER UN NOEUD" form.

- Type d'affichage:** Office 365
- Tenant ID:** 787dd77f-11b0-428a-828f-6187c1d70000
- ID Client:** e5367991-728c-4401-b277-6187c1d70000
- Clé:** 61c1-2870a-828a8d9g-42870a-828a8d9g

Buttons for "Retour" and "Sauver" are located at the bottom left of this section.

Vous pouvez fermer la fenêtre, vous constatez qu'un service et un nœud ont été rajoutés. Une fois le groupe apparu, vous pouvez cliquer sur le nœud et vous arrivez sur cette page.

La partie centrale est vide, car, il n'y a actuellement aucun service important superviser. Pour en ajouter, cliquez sur l'onglet “Services”.



3 nouveaux services sont ajoutés et remonteront l'état des services Microsoft.

Sélectionnez les services que vous souhaitez superviser. J'ai choisi de superviser Exchange, Teams et Sharepoint dans ce tutoriel. Une fois cela fait, cliquez sur "Ajouter service(s)".

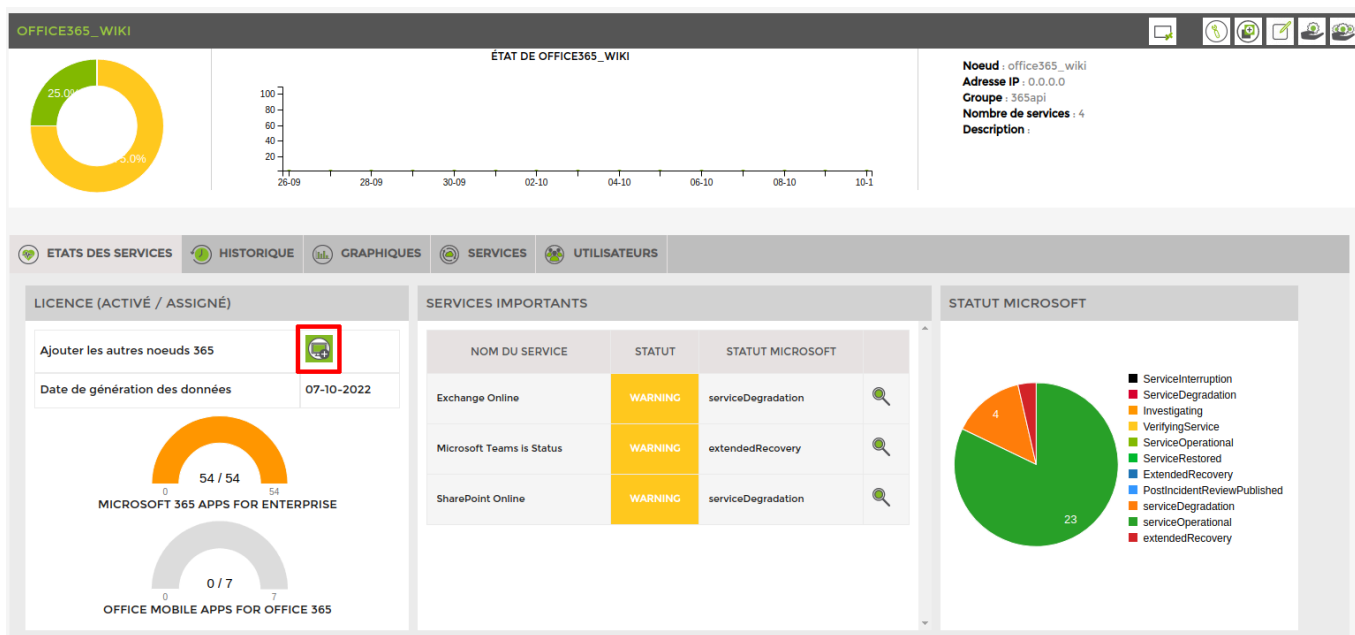
<input type="checkbox"/>	NOM DU SERVICE	STATUT	STATUT MICROSOFT	DETAIL
<input checked="" type="checkbox"/>	Exchange Online	WARNING	serviceDegradation	
<input type="checkbox"/>	Identity Service	OK	serviceOperational	
<input type="checkbox"/>	Microsoft 365 suite	WARNING	serviceDegradation	
<input type="checkbox"/>	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	

Ajouter les autres nœuds office 365

Il n'y a pas que la vue basique d'Office 365 de disponible. Vous pouvez ajouter également les vues suivantes:

- Exchange
- Onedrive
- SharePoint
- Teams

Pour cela cliquez sur "Ajouter les autres nœuds 365".



La page suivante apparaît:

AJOUTER LES AUTRES NOEUDS 365

Vous pouvez ajouter les noeuds supplémentaires 365 et obtenir de nouvelle capacité de supervision propre au différent services. Il vous suffit de cocher les cases.

GRUPE POUR LES NOUVEAUX NOEUD

Groupe
365api X

Sélectionner tout

SERVICE 365 DISPONIBLE

<input checked="" type="checkbox"/> SERVICE: ONE DRIVE Nom du noeud office365_wiki-One Drive	<input checked="" type="checkbox"/> SERVICE: SHARE POINT Nom du noeud office365_wiki-Share Point	<input checked="" type="checkbox"/> SERVICE: EXCHANGE Nom du noeud office365_wiki-Exchange
<input checked="" type="checkbox"/> SERVICE: TEAMS Nom du noeud office365_wiki-Teams		

Ajouter

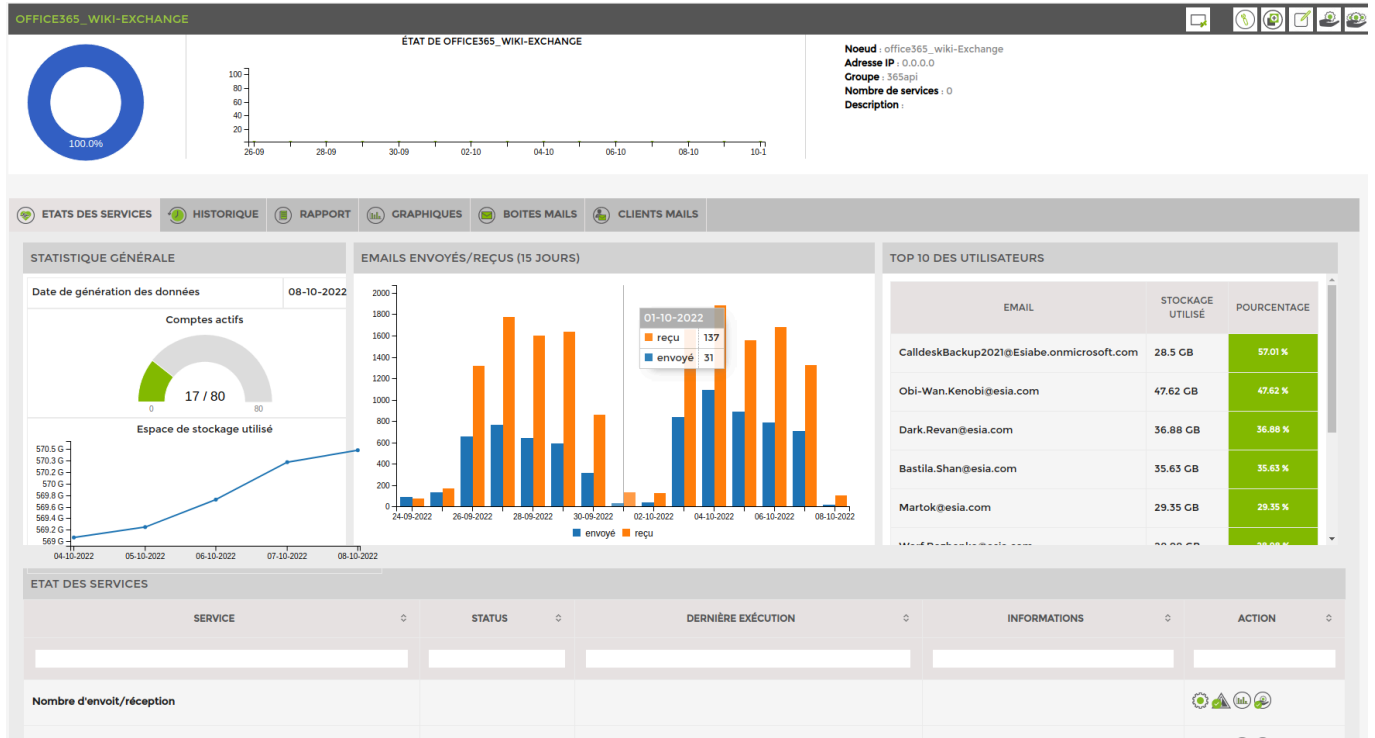
Sélectionnez les nœuds à rajouter, modifier au besoin leur nom ainsi que le groupe dans lesquelles les nœuds seront ajoutés (par défaut: le même que votre nœud office 365 d'origine).

Une fois cela fait cliquer sur "Ajouter" et fermez la fenêtre. Les nœuds seront automatiquement ajoutés avec les éléments suivantes :

Exchange

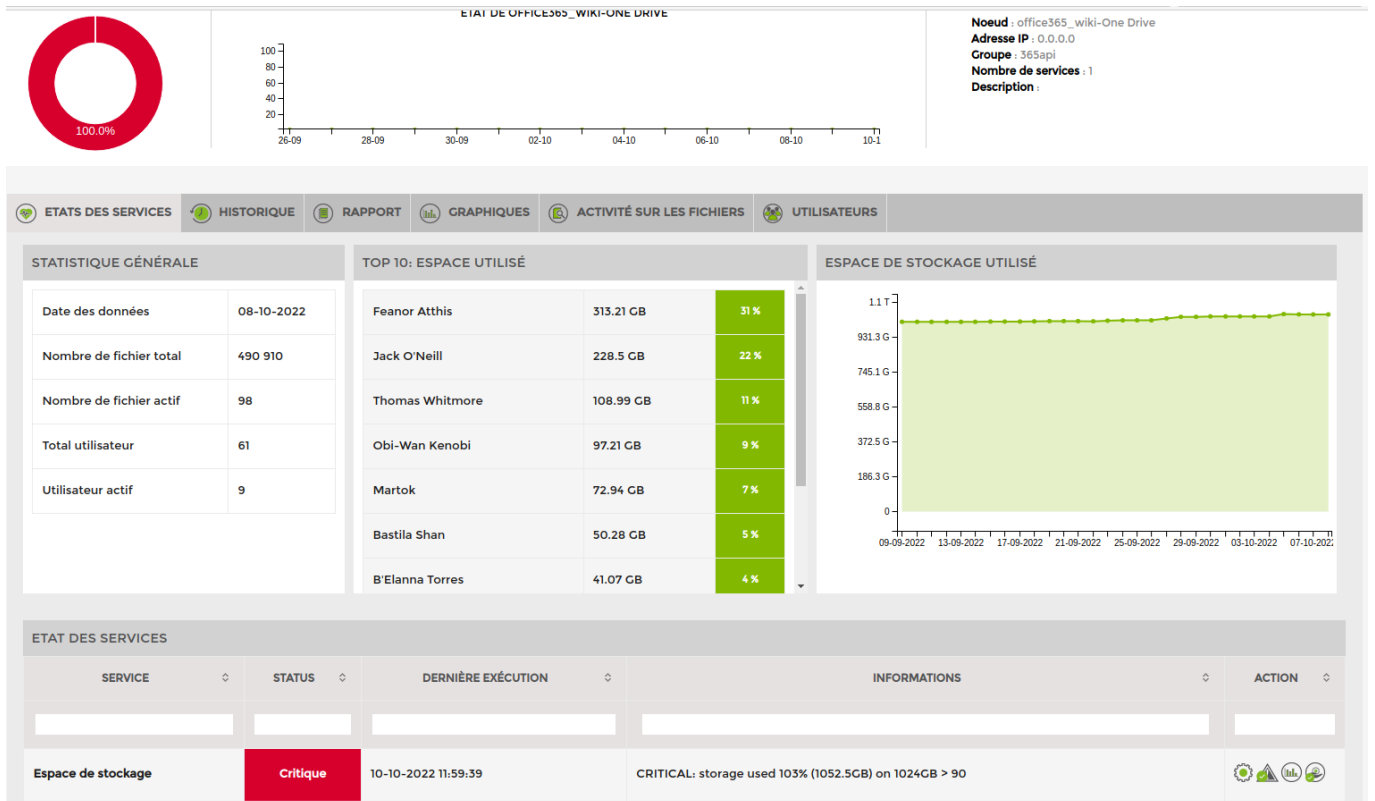
Voici la vue disponible et 2 services sont automatiquement ajoutés :

- Utilisation des boites mail : passe en jaune ou rouge si la boite a atteint le quota ou est bloquée
- Nombre d'envois/réception : tester le nombre de mails envoyer/reçu quotidien par défaut les valeurs d'alerte et de critique sont de 1500 et 2000 mails.



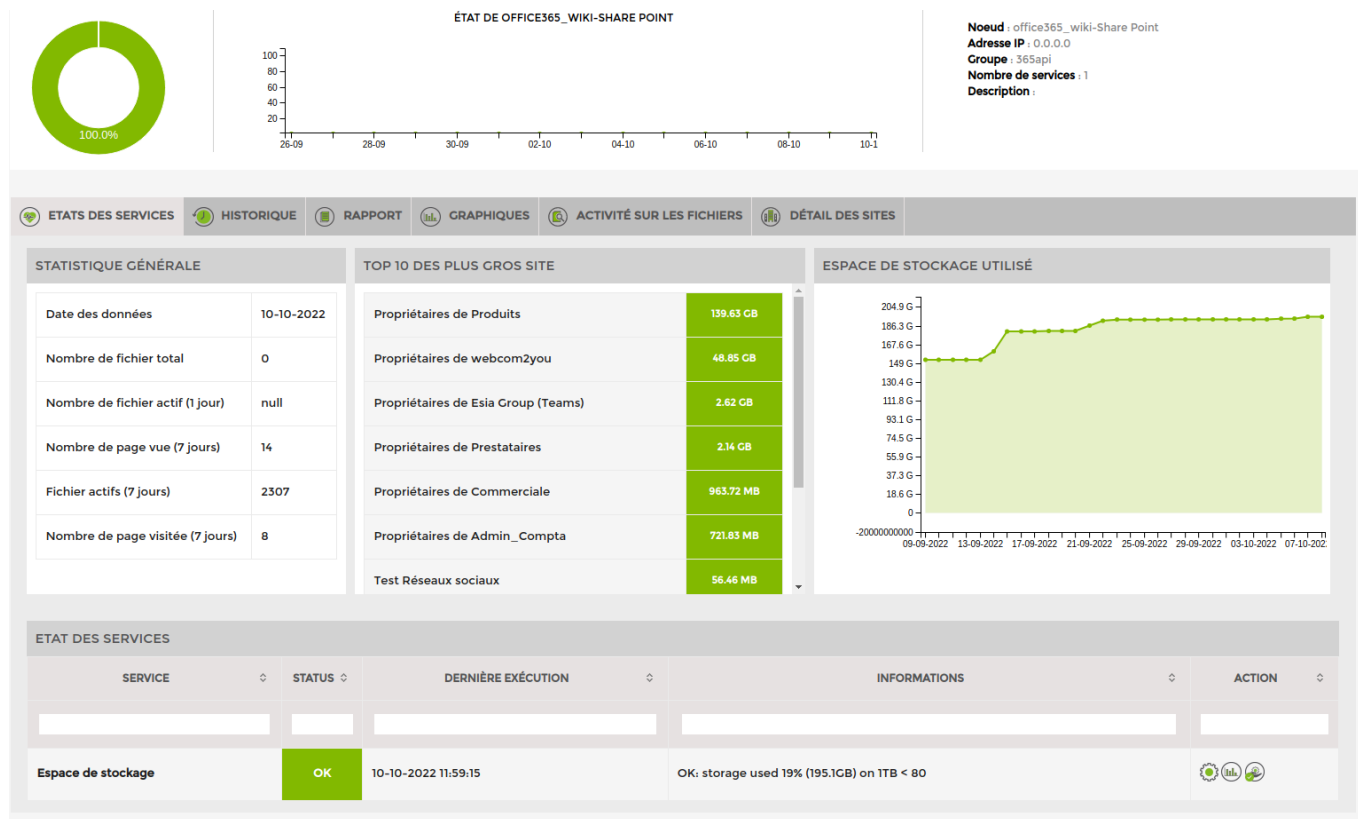
Onedrive

Voici la vue disponible et 1 service est automatiquement ajouté. Il test l'espace de stockage globale de OneDrive



Sharepoint

Voici la vue disponible et 1 service est automatiquement ajouté. Il test l'espace de stockage globale de tout les site Sharepoint



Teams

Voici la vue disponible.



Defender

Nécessite une licence Svalinn (Disponible à partir de la version d'Esia 3.5.2)

Droits d'accès API « Microsoft Graphique » :

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

[Voir le tuto de configuration des autorisations](#)

Plugins

Plugins ajoutés à la création du noeud :

- **Alertes actives** (CHECK_API_M365_SECURITY_ALERT_ACTIVE) :

Passe en statut « alerte » ou « critique » en fonction du nombre d'alertes actives.

- **Alertes récentes** (CHECK_API_M365_SECURITY_ALERT_COUNT) :

Passe en statut « alerte » ou « critique » en fonction du nombre d'alertes (de tous types, pas uniquement actives) survenues sur une période de temps. Par défaut sur 1 jour.

- **Incidents actifs** (CHECK_API_M365_SECURITY_INCIDENT_ACTIVE) :

Passe en statut « alerte » ou « critique » en fonction du nombre d'incidents actifs.

- **Incidents récents** (CHECK_API_M365_SECURITY_INCIDENT_COUNT) :

Passe en statut « alerte » ou « critique » en fonction du nombre d'incidents (de tous types, pas uniquement actifs) survenus sur une période de temps. Par défaut sur 1 jour.

- **Secure Score** (CHECK_API_M365_SECURITY_SECURESCORE) :

Passe en statut « alerte » ou « critique » en fonction de la valeur en pourcentage du SecureScore.

- **Authentification valide - MFA** (CHECK_API_M365_SECURITY_USERS_AUTH_COUNT) :

Passe en statut « alerte » ou « critique » en fonction du nombre d'utilisateurs qui n'ont **pas** configuré une authentification multifacteur valide.

Autres plugins disponibles :

- **Authentification valide - SSPR** (CHECK_API_M365_SECURITY_USERS_AUTH_COUNT) :

Passe en statut « alerte » ou « critique » en fonction du nombre d'utilisateurs qui n'ont **pas** configuré une méthode de réinitialisation de mot de passe en libre service (SSPR) valide.

Ajouter le plugin, puis modifier dans le paramètre "method=mfa" en "**method=sspr**"

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

- **Authentification valide - PasswordLess** (CHECK_API_M365_SECURITY_USERS_AUTH_COUNT) :

Passe en statut « alerte » ou « critique » en fonction du nombre d'utilisateurs qui n'ont **pas** configuré une méthode d'authentification sans mot de passe (PasswordLess) valide.

Ajouter le plugin, puis modifier dans le paramètre "method=mfa" en "**method=passwordless**"

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

Pour le plugin **CHECK_API_M365_SECURITY_USERS_AUTH_COUNT** (MFA, SSPR ou PasswordLess), on peut tester un type d'utilisateur spécifique. En ajoutant le paramètre type=<\$type> (dans le -a). Voici les types disponibles :

- **admin** ⇒ Uniquement les utilisateurs qui sont administrateurs

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

- **member** ⇒ Uniquement les utilisateurs qui sont de type "Membre" (Voir la colonne "Type" du tableau dans l'onglet "Authentification") **et pas administrateurs**

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

- **guest** ⇒ Uniquement les utilisateurs invités

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

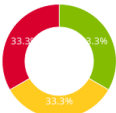
On peut combiner plusieurs types, par exemple tous les utilisateurs « Administrateurs » et les utilisateurs « Membres » (non admin), donc tout le monde sauf les invités : -A \$AUTH_FILE_OFFICE365

-t security -n usersAuthMethodCount -a method=mfa,type=admin:member -w 1 -c 3

Vues

Voici la vue principale du nœud :

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 :

STATISTIQUES GÉNÉRALE

Secure Score 49.34 %

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

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

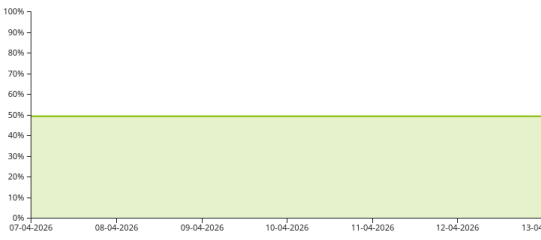
1085 Nombre d'utilisateurs / 886 MFA valides

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

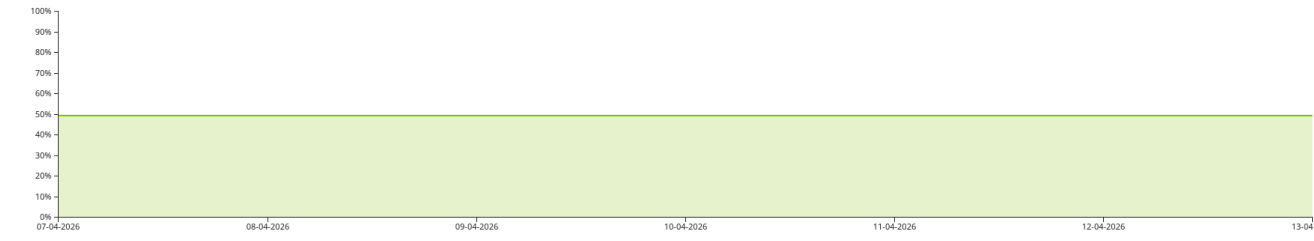
SECURE SCORE



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)		
Authentication valide - MFA	Alerte	<2 minutes	WARNING: 199 users do not have valid MFA (> 1)		

Onglet SecureScore :

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	0.83%	0/9	Device	MDATP	Config	Inconnu

Onglet Alertes :

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	

Onglet 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	

Onglet Authentification :

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/interface/module_o365

Last update: **2026/04/13 13:25**



