Systancia

the human face of the workplace

SYSTANCIA CLEANROOM 4.5
Release Note

#Cybersecurity #Virtualization #AI

www.**systancia**.com

Ref. :	FR_Systancia-Cleanroom_4.5_RN_rev.1.01
Version :	1.01
Produit :	Systancia Cleanroom
Date :	2023-08-31

Objet :

Ce document présente les évolutions techniques et fonctionnelles de la version 4.5 de Systancia Cleanroom.

TABLE DES MATIERES

1. Principales nouveautés de Systancia Cleanroom 4.5

Les principales nouvelles fonctionnalités incluses dans la version 4.5 du produit Systancia Cleanroom sont présentées ci-après.

1.1 Support de Debian 11

Systancia Cleanroom 4.5 ne supporte plus Debian 10 mais seulement Debian 11 pour l'installation des serveurs.

1.2 Compatibilité avec des environnements respectant le silotage AD (« AD tiering »)

Systancia Cleanroom Session 4.5 apporte des évolutions lui permettant de s'intégrer à un environnement respectant les principes du silotage AD (« AD tiering »). Pour toutes informations complémentaires sur le silotage AD, Systancia propose un ebook pour apporter des détails sur l'architecture silotage AD, et la réponse apportée avec Systancia Cleanroom Session :

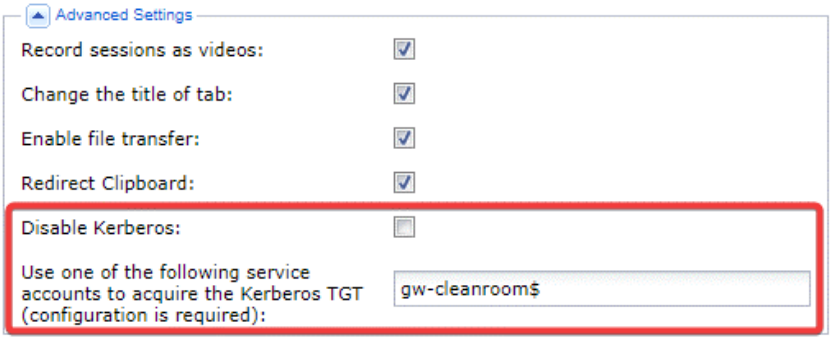
https://marketing.systancia.com/acton/media/33519/ebook-pam-silotage-ad

1.2.1 Support de l'authentification Kerberos pour les applications RDP et HTML5 RDP

Systancia Cleanroom 4.5 apporte le support de l'authentification Kerberos pour les applications RDP et HTML5 RDP en mode sans agent.

Un compte ordinateur de l'AD peut maintenant être paramétré sur le Passerelle Cleanroom. Ce compte est utilisé pour récupérer un ticket Kerberos nécessaire au processus d'authentification vers un serveur RDP.

L'option se situe dans les paramètres avancés :

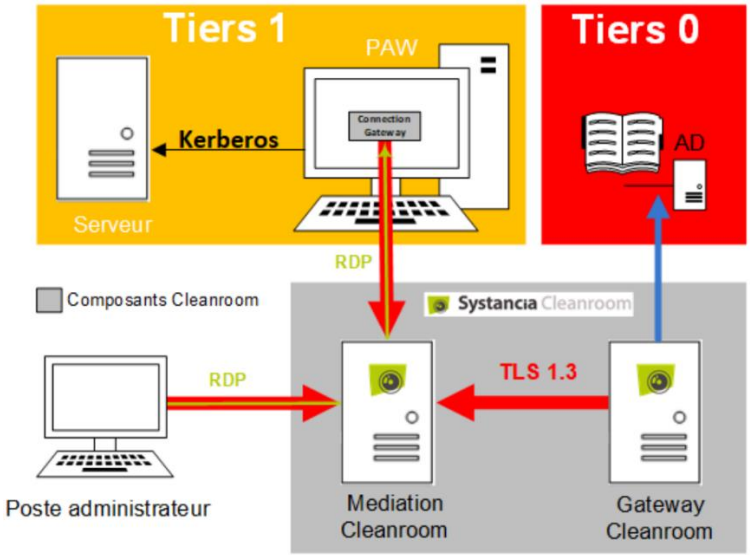


Cette fonctionnalité n'est pas dédiée à un environnement où le silotage AD a été appliqué, il peut très bien s'adapter à un besoin de connexion à un serveur RDP avec un compte appartenant au groupe « Protected Users » qui impose l'utilisation de Kerberos pour l'authentification de l'utilisateur.

1.2.2 Support de la connexion à des postes PAW

La connexion à un poste PAW (Privileged Access Workstations), qui est un poste dédié à l'administration d'un tiers, impose un renforcement accru de sa sécurité. Il n'est normalement pas autorisé d'exposer des ports en écoute sur cette machine au reste du réseau pour garantir sa non-compromission.

Pour que Systancia Cleanroom Session puisse se connecter à un poste PAW, nous ajoutons un nouveau composant : la Passerelle Cleanroom pour Windows. Il s'agit d'une Passerelle Cleanroom, dont la connexion est toujours à l'initiative de la Passerelle vers la Mediation, qui permet à Systancia Cleanroom Session de pouvoir avoir accès au poste PAW après le montage d'un tunnel TLS. L'accès au poste PAW débloque la possibilité de s'y connecter en RDP avec une écoute par le service RDP restreint à la boucle locale (localhost), de ce fait, aucune machine externe autre que Systancia Cleanroom Session n'aura la capacité de s'y connecter en RDP.



L'administrateur devra indiquer, au niveau de son application RDP ou HTML5 RDP, le nom de la passerelle par laquelle Systancia Cleanroom Session aura accès au poste PAW :

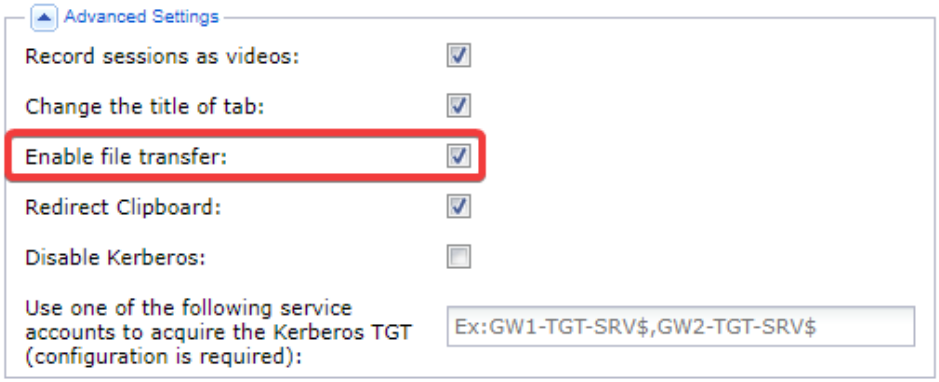
1.3 Support de l'authentification multifacteur sur la console Systancia Cleanroom

Systancia Cleanroom 4.5 apporte le support de l'authentification multifacteur pour la console d'administration. La console d'administration supporte les mêmes authentifications multifacteurs que le portail Cloud Systancia Cleanroom, c'est-à-dire :

- Authentification avec un jeton OTP
- Authentification avec un jeton TOTP
- Authentification avec un jeton RADIUS
- Authentification avec périphérique FIDO2
- Authentification depuis un domaine SAML

1.4 Configuration de l'autorisation du transfert de fichiers pour les applications HTML5 RDP

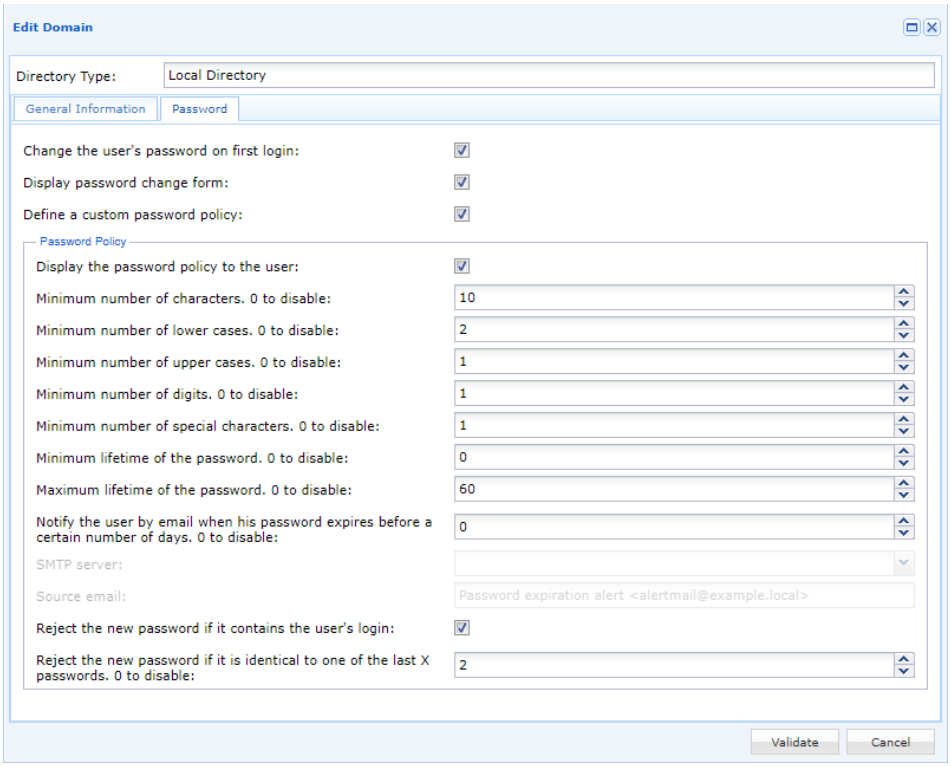
Avec Systancia Cleanroom 4.5, il est maintenant possible d'autoriser ou non le transfert de fichiers pour les applications HTML5 RDP. Le paramètre se situe dans les paramètres avancés de l'application :



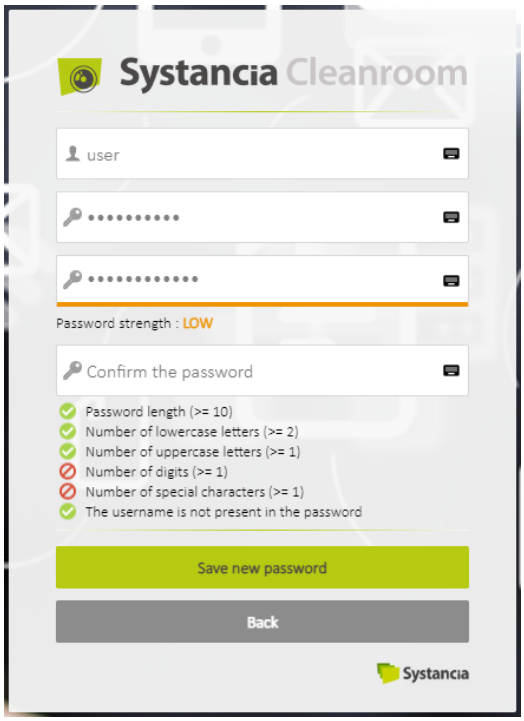
A noter que la mise à jour de Systancia Cleanroom 4.4 vers 4.5 basculera toutes les applications avec ce paramètre désactivé, la création de nouvelles applications n'activera pas non plus cette option par défaut.

1.5 Paramétrage d'une politique de mot de passe pour les comptes locaux

Systancia Cleanroom 4.5 apporte la possibilité de définir une politique de mot de passe pour tout domaine local via un nouvel onglet de paramétrage :



Si la configuration réalisée par l'administrateur le permet, l'utilisateur pourra avoir un retour sur les éléments devant figurer dans son mot de passe :



1.6 Enrôlement des TOTP à l'aide de QRcode

Il n'est plus nécessaire de devoir paramétrer les smartphones des utilisateurs afin de leur ajouter la clef TOTP qui était soit stockée dans un attribut utilisateur ou soit stockée dans le produit mais envoyée par mail. Maintenant un QRcode à scanner avec l'application de TOTP est affiché lors de la première connexion de l'utilisateur :

L'utilisateur devra ensuite valider son code afin que le produit ne lui affiche plus de QRcode.

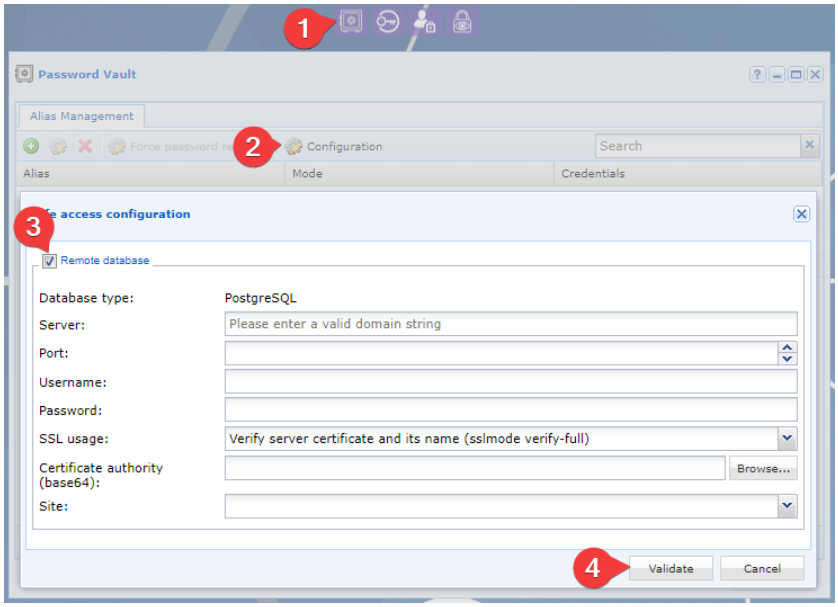
Cette fonctionnalité n'est disponible uniquement que pour les clefs TOTP stockées par le produit, elle est donc incompatible avec l'option de récupération de la clef dans un attribut LDAP.

1.7 Déport du coffre-fort Systancia Cleanroom vers une base de données présente dans le LAN

Systancia Cleanroom 4.5 ajoute la possibilité de déporter le stockage du coffre-fort de la Mediation vers une base de données PostgreSQL présente dans le LAN et atteignable via une Passerelle.

Afin de configurer ce déport il faut :

1. Ouvrir le coffre-fort
2. Cliquer sur « Configuration »
3. Activer l'accès à la BDD distante
4. Paramétrer l'accès à la BDD et valider les modifications



1.8 Cleanroom ACM

Cleanroom Application Credentials Manager permet à des scripts ou des processus de récupérer des identifiants du coffre-fort Systancia Cleanroom. Pour ce faire un agent doit être déployé afin d'assurer la liaison entre le serveur avec son script ou application et Systancia Cleanroom :

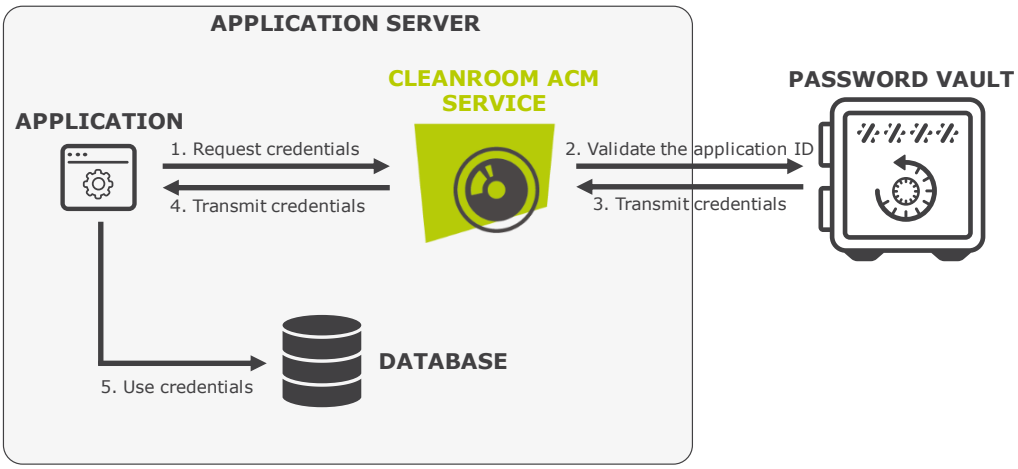


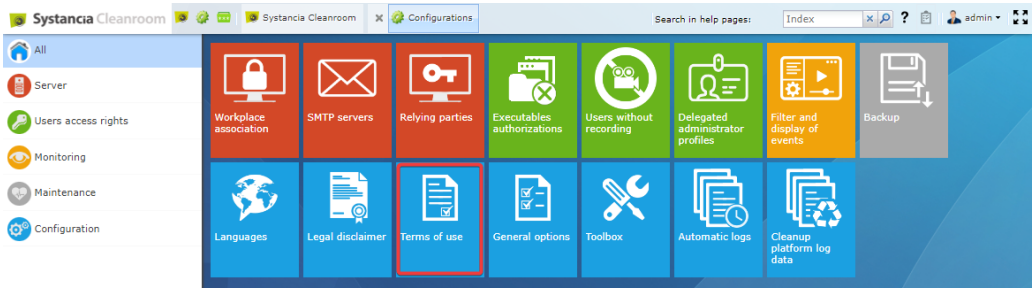
Figure - Authentication process from an application to a database

L'administrateur Cleanroom peut finement gérer les autorisations pour la récupération des identifiants par les différents scripts (restrictions sur les process, restrictions temporelles ou sur les alias pouvant être récupérés).

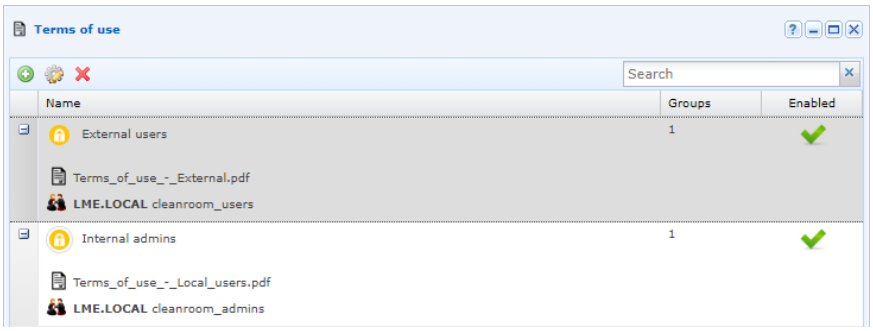
Pour activer la fonctionnalité il est nécessaire de contacter Systancia.

1.9 Paramétrage de chartes utilisateur pour l'utilisation du produit

Les administrateurs ont maintenant la possibilité de paramétrer une ou plusieurs chartes d'utilisation de la plateforme à faire valider par leurs utilisateurs. Une nouvelle tuile sur le plan de travail « Configurations » a été ajoutée : « Chartes d'utilisation ».

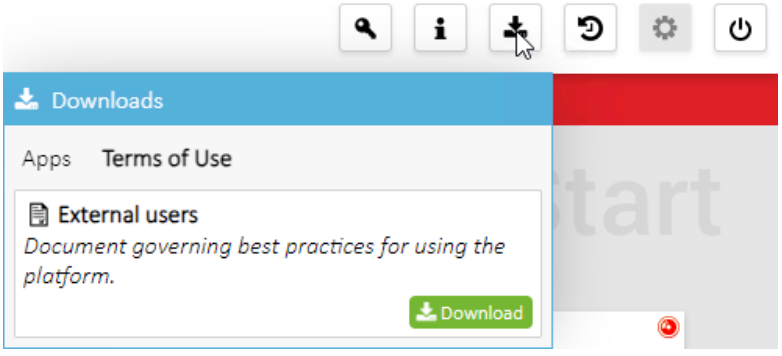


A partir de ce menu, l'administrateur pourra affecter une charte à un groupe d'utilisateurs. Un utilisateur pouvant se voir affecter différentes chartes.



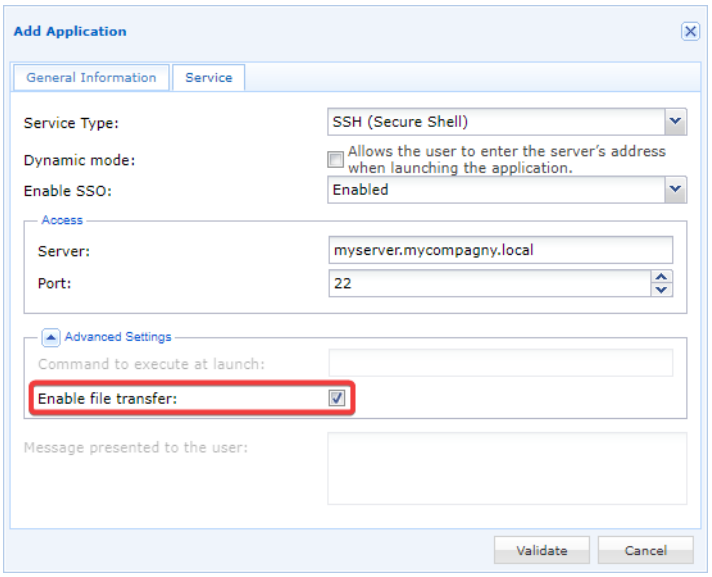
Lors de la première connexion de l'utilisateur, il devra valider les chartes pour pouvoir accéder au portail Cloud.

Toutes modifications d'une charte entrainent le besoin d'être revalidée par l'ensemble des utilisateurs. De plus les utilisateurs peuvent à tout moment retélécharger la charte via le menu de téléchargements.



1.10 Transfert de fichiers avec une application SSH

Les applications SSH ajoutent dans les paramètres avancés une option permettant de commuter l'application pour une utilisation de type transfert de fichiers. Toutes applications ayant ce paramètre activé ne lanceront plus l'utilitaire Putty mais l'utilitaire FileZilla pour initier une connexion SFTP.



Les actions d'ouverture de fichiers ou de répertoires tout comme les suppressions sont toutes tracées au niveau de l'archive générée.

A noter que l'accès SFTP en direct (connexion vers la Passerelle Cleanroom) est supporté.

2. Mises à jour/évolutions intégrées

Ci-dessous vous trouvez le récapitulatif des mises à jours/évolutions intégrées à la nouvelle version de Systancia Cleanroom :

2.1 Sécurité

IPC inclus : 45616, 44701, 45619, 43536, 42166, 41803, 39209

- Réduction des informations collectables sur la liste des domaines via interception et modifications de requêtes Web.
- Ajout d'un nouvel onglet sur les domaines locaux dédié aux mots de passe avec la possibilité de définir une politique de mot de passe spécifique.
- Les actions de déploiement/suppression de l'agent d'enregistrement depuis la console d'administration ne laissent plus de traces des identifiants en cas d'échec de l'action.
- Restriction des accès de la base locale Zope et arrêt du stockage temporaire des informations de sessions.
- La configuration d'un certificat sur une interface Web configure correctement la chaîne de certification des autorités de certification (sous réserve que la PKI créée contienne toutes les informations).
- Amélioration du cloisonnement des utilisateurs vis-à-vis des sessions Systancia Cleanroom Desk.
- La console d'administration supporte l'ensemble des authentifications multifacteurs supportées par le portail Cloud, soit : l'ensemble des jetons d'authentification, les périphériques FIDO2, l'authentification SAML et l'authentification à un domaine LDAP avec RADIUS.

2.2 Clients Systancia Cleanroom

IPC inclus : 45460, 39790, 44035, 42706, 42507, 36223, 31852, 42110, 40164, 39698

- Support du lancement d'applications en ligne de commande avec le client Cleanroom Desktop
- Ajout d'une nouvelle clef de registre pour désactiver le contrôle de la révocation du certificat par le client Cleanroom Desktop :

  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Systancia\Cleanroom\Agent]

  "disablecertificaterevocation"=dword:00000001
- Modification de la récupération de la configuration proxy : vérifie en premier la configuration présente dans HKEY_CURRENT_USER avant HKEY_LOCAL_MACHINE
- La configuration proxy du système n'est plus ignorée si le proxy est défini sur 127.0.0.1 ou 127.0.0.2
- Le client Gate pour MacOS est signé et reconnu par Apple
- Correction de l'affichage de deux icônes dans la systray pour Ubuntu 21.10
- Ajout de logs complémentaires dans le cas de l'échec de validation de la règle Windows Security Center

2.3 Composants Mediation

IPC inclus : 45179, 44528, 43887, 42241, 42459, 40140

- Le changement de mode n'occasionne plus la bascule en mode failover pour un cluster loadbalancing.
- Suppression du service cleanroom-vault pour le remplacer par un timer systemd du même nom. Ce timer a la charge de contrôler les alias qui doivent avoir une rotation du mot de passe et initie cette action si nécessaire.
- Gestion de l'envoi de courriel vers un serveur SMTP long à répondre. Le timeout maximal de 45 secondes est défini pour l'établissement de la connexion au serveur SMTP.
- Augmentation de la verbosité des logs des rotations de mot de passe avec la configuration du fichier /var/log/ipdiva/cleanroom-vault.log et le passage en DEBUG.
- Correction des défauts de connexion lorsque la connexion réalisée au routeur SSL est associée à un fichier dont le descripteur est supérieur à 1024
- Adresse de broadcast forcée sur celle de la VIP par le watchdog lorsque son masque de sous-réseau est /32

2.4 Composants Passerelle

IPC inclus : 43519, 40189, 42767, 41638, 42187, 42201, 40379

- Déplacement forcé des archives dans le répertoire de stockage à long terme si la Passerelle n'a pas pu l'initier pour cause d'erreur du service d'enregistrement.
- Fiabilisation de la rotation de mot de passe Linux lorsque le serveur cible est long à répondre.
- Réduction de la volumétrie de logs en cas de non-montage du répertoire pour le transfert de fichiers HTML5 SSH.
- Fiabilisation des connexions TLS à l'agent d'enregistrement lorsqu'une autre connexion ferme sa connexion réseau à ce dernier.
- La modification des mots de passe utilisateur utilise une connexion SMB avec le compte de lecture du domaine et plus une connexion anonyme. La rotation du mot de passe est gérée en LDAPS pour les domaines LDAP dont les connexions au serveur LDAP/AD sont en LDAPS.
- La modification des mots de passe est réalisée de manière séquentielle s'il y a plusieurs serveurs LDAP de paramétré et s'arrête dès lors que la modification a réussi sur l'un des serveurs.
- Fiabilisation du mécanisme de suppression automatique des archives lorsqu'une archive possède un nom vide.

2.5 Portail Cloud

IPC inclus : 39654, 44488, 43359, 43521, 43959, 43374, 41918, 41839

- Ajout d'une barre de défilement lorsqu'un nombre de domaines important utilise tout l'espace vertical disponible.
- Amélioration du temps nécessaire pour le contrôle des conditions d'accès.
- Extension du support des caractères pour les mots de passe aux caractères UTF-8.
- La connexion des utilisateurs peut maintenant être soumise à l'acceptation d'une ou plusieurs chartes par l'utilisateur.
- Le QRCode généré pour enregistrer une clef TOTP n'est validé qu'après la saisie du code actuel par l'utilisateur.
- Les authentifications en échec sur le portail Cloud mutualisé Gate/Cleanroom n'impacte plus les statistiques Gate.
- Le message d'invitation à la saisie du code TOTP a été révisé pour donner l'information à l'utilisateur d'aller chercher le code sur son application TOTP.
- Lorsque l'utilisateur s'authentifie sur le formulaire en cascade, le processus d'authentification s'arrête s'il n'a pas réussi à passer un MFA sur l'un des domaines.

2.6 SAML

IPC inclus : 45633, 41816, 41362

- Support de l'architecture cluster.
- Ajout d'une option permettant la synchronisation à la demande des groupes AzureAD avec Systancia Cleanroom. Pour avoir accès à la fonctionnalité il est nécessaire de basculer le type de fournisseur d'identité à Azure.
- Les groupes SAML possède un nouvel attribut « external id » qui est utilisé pour indiquer le nom du groupe tel que retourné par l'IDP tandis que l'attribut « name » est un nom d'usage spécifique à Systancia Cleanroom.

2.7 Console d'administration

IPC inclus : 46116, 45293, 43167, 43224, 42196, 43085, 42217, 39375, 34366, 42532, 42228, 25535, 40742

- Blocage de la création de nouvelles Passerelles avec un nom non conforme
- Amélioration du temps d'affichage des contrats d'accès lorsque de nombreuses ressources sont disponibles
- Ajout du support de changement de mot de passe avec une authentification en cascade. L'option est à activer dans les options générales.
- Ajout dans les configurations des administrateurs délégués des menus « Politique de mot de passe » ; « Comptes supervisés » et « Bureaux VDI standard et étendus ».
- Les barres de défilement n'apparaissent plus, sauf si nécessaire, lorsqu'un zoom est paramétré par une valeur ne correspondant pas à un multiple entier (110% ou 125% par exemple).

- Les caractères « u » et « \ » ne sont plus interdit pour la création de déclencheurs de lancement de processus au niveau des alertes.
- Ajout d'une option sur le menu listant les Passerelles afin de pouvoir télécharger le certificat racine de l'AC du service d'enregistrement.
- Modification de la règle OS pour que la détection de Windows 10 devienne une détection de Windows 10/11.
- Ajout d'une nouvelle fonctionnalité nommée Cleanroom ACM (Application Credentials Manager).
- Exécution en tâche de fond du déploiement ou de la désinstallation de l'agent d'enregistrement pour ne pas atteindre le timeout du navigateur en cas de lenteurs importantes dans l'opération.
- La recherche des applications n'est plus impactée par la présence de tags dans certaines applications.
- Ajout d'une nouvelle catégorie d'applications par défaut nommée « DEFAUT ».
- Le tri des utilisateurs par groupe est maintenant possible.

2.7.1 Domaine d'authentification

IPC inclus : 43738, 39636, 42140, 41053

- Ajout d'une option sur les domaines LDAP pour indiquer le certificat de l'AC des serveurs LDAPS.
- L'activation ou désactivation de l'option RADIUS est maintenant possible pour un domaine LDAP déjà créé.
- Support de la configuration de plusieurs jetons sur un domaine, les utilisateurs auront le choix du jeton qu'ils souhaitent utiliser.
- La modification de la configuration d'un utilisateur n'entraine plus le besoin pour l'utilisateur de modifier son mot de passe à la prochaine connexion si le paramètre de changement de mot de passe à la première connexion est actif.

2.7.2 Centre de contrôle

IPC inclus : 43952, 42587, 20682, 40866, 40560

- La génération des miniatures des archives RDP avec agent contrôle le démarrage effectif de l'enregistrement pour éviter les erreurs de génération.
- L'accès au centre de contrôle reste possible lorsque la Mediation Slave et une passerelle sont indisponibles.
- Ajout d'un indicateur, à activer dans les options générales, permettant de donner un indice d'utilisation des applications RDP et HTML5 RDP avec utilisation de l'agent.
- Le chargement des miniatures dans le centre de contrôle n'est plus bloquant, l'accès à ce menu ne provoque plus de déconnexion lorsque la bande passante est faible.
- Les marqueurs sur la timeline des archives sont correctement affichés même en cas de lenteurs pour le chargement de la vidéo.

2.7.3 Workflow

IPC inclus : 46095, 45827

- Les workflows issus de domaines SAML apparaissent correctement dans la liste des workflows en attente.
- Optimisation du temps d'affichage des workflows.

2.7.4 Coffre-fort

IPC inclus : 41458, 40314, 42343

- Déblocage de la possibilité de saisir un login LDAP au format UPN : « user@domain ».
- Ajout du paramétrage du déport du coffre-fort Systancia Cleanroom vers une BDD PostgreSQL accessible via une Passerelle Cleanroom.
- La modification des alias LDAP est possible à tout instant.

2.8 Console system

IPC inclus : 44593, 43836, 43242, 40674, 41399

- La connexion à une BDD PostgreSQL pour les organisations offre le choix du niveau de contrôle et d'exigence du certificat présenté par la BDD.
- L'affichage des hôtes virtuels au niveau d'une interface Web n'est plus limité à 15.
- Ajout d'une nouvelle tuile pour permettre le paramétrage de la sélection des organisations par les utilisateurs, soit en mode liste (fonctionnement historique) ou soit avec un champ libre.
- Mise à jour automatique du fichier djangosettings.ini pour ajouter tous les noms des hôtes virtuels Web ou Reverse Proxy créés ou supprimés.
- Ajout d'une nouvelle configuration pour l'association d'organisations Gate/Cleanroom : paramétrer l'indépendance de la gestion des licences. Si l'indépendance est paramétrée alors une licence de produit concerné ne sera déduite qu'à partir du premier lancement d'application dudit produit.

2.9 MFA

IPC inclus : 43457, 42784, 41770, 42127, 40417, 39751

- Affichage d'un QRCode à l'utilisateur pour permettre l'enregistrement de sa clef TOTP.
- Ajout de paramètre site sur le jeton SMS Orange HTTP.
- La modification de n'importe quel paramètre de l'OTP SMS HTTP OVH provoquait la désactivation du passage à travers un site.
- Insensibilité à la casse pour l'affectation d'une clef TOTP à un utilisateur.
- Ajout du support d'envoi d'OTP SMS avec CleverSMS avec un mail de format « NUMERO_TELEPHONE@mm.clreversaas.fr » ou bien en précisant vers quel domaine le courriel doit être envoyé (utile lors de l'utilisation d'un relais local).
- Support du mode PUSH pour les jetons RADIUS.

2.10 Applications Web et Reverse Proxy

IPC inclus : 44847, 42262, 41761, 41403, 41300, 41227, 41058, 40487, 39985

- Déblocage de la restriction sur les périphériques mobiles pour les ressources Web et Reverse Proxy.
- Le mode SSO par préchargement de formulaire - il est maintenant possible d'identifier les champs identifiant, mot de passe et jeton CSRF avec des sélecteurs. Le sélecteur CSS est utilisable avec le préfixe « css: » ; par exemple pour rechercher un champ ayant comme ID « LOGIN_user » le sélecteur suivant pourra être utilisé : « css:#LOGIN_user ». Le seconde sélecteur est un sélecteur basé sur les regex dont son utilisation est préfixée par « re: » ; par exemple pour rechercher un champ dont le nom est terminé par une série de chiffres aléatoires tel que « LOGIN_pwd[54616] », le regex suivant pourra être utilisé : « re:LOGIN_pwd\[\d*\] ».
- Ajout de la configuration des cookies lors de l'utilisation du SSO par pré-authentification et ajout d'une nouvelle fonction « %uriencoded(texte_à_encoder)% ». Elle permet d'encoder un texte en remplaçant certains caractères spéciaux peu courant par des chaines de substitution UTF-8.
- Modification de la gestion du cookie de session utilisé pour l'enregistrement afin de s'adapter aux modifications de fonctionnement des navigateurs.
- Ajout dans la configuration du SSO par pré-authentification de l'affichage de la requête finale redirigeant l'utilisateur sur la page après passage du formulaire ainsi qu'un ajout de nouvelles fonctions : « %sha256()% » et « %rsaoep()% ».
- Ajout des fonctions pour le SSO par pré-authentification suivantes :
    - %,% : séparateur de paramètres d'une fonction
    - %rsa()% : fonction de chiffrage RSA. Nécessite deux paramètres, la clef publique et la donnée à chiffrer
    - %hmacmd5()% : fonction de chiffrage HMAC(MD5), nécessite deux paramètres, la donnée à chiffrer et la clef de chiffrement
    - %md5% : fonction de chiffrage MD5, nécessite un argument, la donnée à chiffrer
    - %reqresult()% : permet d'utiliser le résultat d'une requête précédemment envoyée. Nécessite un paramètre et possède un paramètre optionnel : le numéro d'ordre de la requête dont on veut récupérer le résultat, et en optionnel, le nom de la clé à utiliser si le résultat de la requête contenait plusieurs paramètres.
- Ajout de la possibilité de déclarer des variables locales ou de session avec le SSO par pré-authentification.
- Les messages d'avant ouverture d'application n'utilisent plus le système de notification de l'OS mais affiche un pop-up sur le portail dont l'utilisateur doit valider sa lecture avant lancement de l'application. Cela permet de contrer le blocage des notifications par le navigateur.
- Amélioration de l'enregistrement vidéo pour les sites Web utilisant de nombreuses iframe sans attribut de taille.

2.10.1 Application Web

IPC inclus : 43440, 41753, 40938, 42946, 42955, 42922, 41562, 42406, 42116, 41943, 42086, 42085, 42084, 42115, 42130, 41751, 40574, 40568, 41622, 41030, 41049, 41434, 41514, 41521, 40332, 40259, 37795, 39634, 33852

- Gestion des pages annonçant plusieurs feuilles de style avec un attribut title.
- Améliorations générales du fonctionnement de l'application.
- La restriction réseau via plage IP est de nouveau permise.
- Améliorations générales du fonctionnement des applicaitions Web pour son moteur de parsing et réécriture d'URL
- Amélioration du temps d'affichage des pages Web pour les versions antérieures à Firefox 105
- Amélioration du temps d'affichage des pages Web pour les navigateurs à base chromium

2.10.2 Application Reverse Proxy

IPC inclus : 39954

- Ajout de l'ensemble des modes de SSO supportés par l'application Web soit : Classique ; Préchargement de formulaire et Pré-authentification.

2.11 Applications HTML5

IPC inclus : 46036, 45733, 42083, 39665, 43761, 43706, 42048, 41347

- Modification du mécanisme de capture du clavier pour éviter une consommation excessive de RAM sur les postes client Windows après l'ouverture du menu d'informations
- Ajout d'une nouvelle option dans les paramètres avancés afin de modifier le titre de l'onglet HTML5 par le nom de l'application
- Support du clavier français belge
- Le presse-papier remplace les caractères espaces insécables par un caractère espace régulier au lieu de « \xc2\xa0 »
- Autorisation de transfert de fichiers d'une taille supérieure à 2Go
- Optimisation de l'usage de la RAM lors d'un transfert de fichier
- L'utilisation exclusive de ressources HTML5 n'entraîne plus la déconnexion de l'utilisateur sur l'inactivité
- Amélioration de la gestion de la saisie avec auto-complétion des claviers des smartphones

2.11.1 Application HTML5 RDP

IPC inclus : 45817, 43640, 40446

- Ajout d'une nouvelle option dans les paramétrages avancés permettant d'autoriser ou non le transfert de fichiers HTML5.
- Modification des archives pour les applications HTML5 RDP en mode sans agent : l'enregistrement des frappes clavier entoure d'une balise la saisie de touches spéciales. Par exemple l'enfoncement de la touche contrôle gauche apparaissait comme ceci « Control_L » avec Systancia Cleanroom 4.4 et est maintenant affichée « <Control_L> ».
- Accélération des ouvertures des applications en mode sans agent avec la méthode de redimensionnement « zoom ».

2.11.2 Application HTML5 SSH

IPC inclus : 42698, 44395, 39960, 41853, 39673

- Ajout d'un paramètre dans le fichier /etc/guacamole/guacd.conf afin de forcer la suppression de caractère. Il s'agit du paramètre « force_backspace_erasing » qui peut être à « yes » ou « no » (valeur par défaut) sous une section « [ssh] ». Lorsqu'il est actif tout appui sur la touche retour arrière provoquera la suppression du caractère à l'écran de l'utilisateur, même si le retour SSH de la suppression du caractère n'est pas reçu par la Passerelle HTML5.
- Support étendu de machines pour le transfert de fichiers, les prérequis étant le support de SFTP et le bon fonctionnement d'une commande « mkdir -m ».
- Ajout du paramétrage de la touche backspace au niveau de l'application : envoi de la combinaison ctrl+h ou ctrl+?.
- Ajout de la combinaison de touches « Shift+Backspace » afin d'envoyer le caractère backspace qui n'a pas été configuré dans l'application (ctrl+? au lieu de ctrl+h et vice versa).
- Le copier-coller multilignes entre le poste local et le serveur distant ne duplique plus les sauts de lignes.

2.11.3 Application SSH

IPC inclus : 38651, 40132, 39959

- Ajout d'un paramètre avancé autorisant le transfert de fichiers SFTP. L'activation de cette option modifie le fonctionnement de l'application SSH : ce n'est plus un client Putty qui sera ouvert pour l'utilisateur mais un client FileZilla.
- Support des connexions SSH vers un serveur Windows (valable aussi pour les applications HTML5 SSH).
- Envoi de la configuration tty du putty local vers le serveur distant.

2.12 Application VNC

IPC inclus : 44844

- Ajout de logs de débogages activable dans le fichier /etc/ipdiva/cleanroom/xrdprecord.ini de la Passerelle.

2.13 API

IPC inclus : 46166, 44932

- Support de la modification d'applications via API en se basant sur leur ID et non leur nom
- Ajout de nouvelles fonctions d'API pour la manipulation des alias du coffre-fort

2.14 Agent d'enregistrement

IPC inclus : 45880, 42873, 42210

- Prise en compte du cas où aucun certificat n'est disponible pour l'enregistrement direct afin d'éviter l'arrêt du processus.
- La fermeture de la session par l'agent a été revue pour éviter d'obtenir le message d'erreur MSTSC indiquant que la session a été interrompue. Le délai de fermeture forcée de la session par l'agent étant paramétrable via la valeur de registre SessionEndTimeout défini à 10 secondes par défaut.
- Gestion d'écrans multiples avec des mises à l'échelle différentes.

2.15 Accès directs

IPC inclus : 39830, 39831, 39832

- Ajout de l'accès direct RDP sans agent (connexion RDP vers la Passerelle Cleanroom).
- Ajout de l'accès direct RDP sans agent (connexion RDP vers la Passerelle Cleanroom) avec utilisation d'une application RDP. Cela permet entre autres d'utiliser le coffre-fort Systancia Cleanroom.
- Ajout de l'accès direct SSH permettant de lancer une application SSH sans passage par un menu.

2.16 Systancia Cleanroom Desk

IPC inclus : 43397, 42844, 42718, 42344, 41996, 41981

- Restriction de la suppression de clone lorsqu'il est en cours d'utilisation.
- Plus d'une page de règles de pare-feu peuvent être utilisées.
- Réduction de l'impact des latences de Workplace sur la console unifiée.
- Création de deux nouvelles applications dans les contrats d'accès, sous la catégorie Workplace, afin de paramétrer quels utilisateurs peuvent accéder au portail fusionné ou quels utilisateurs doivent utiliser le portail Workplace par un Reverse Proxy.
- Gestion de la reprise de session des bureaux via le bandeau On Air.
- Possibilité d'ouvrir plusieurs sessions Systancia Cleanroom Desk pour un même utilisateur.

2.17 Redirection des logs avec rsyslog

ICP inclus : 42128

- Le log d'ouverture d'application Web contient maintenant l'adresse IP de l'utilisateur.

2.18 Profil de notification

IPC inclus : 39458

- Les alertes emails de déclenchement d'enregistrement direct n'indiquent plus un nom d'utilisateur suivi d'un arobase mais seulement le nom d'utilisateur.

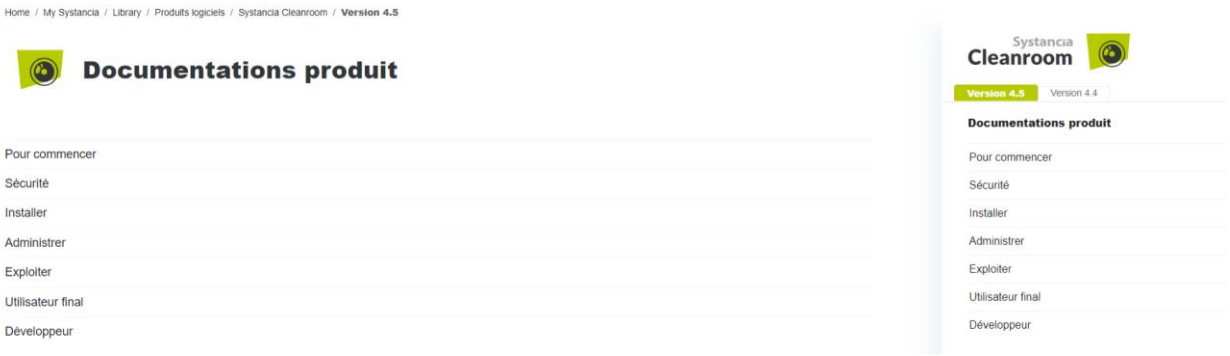
3. Informations techniques

3.1 Où télécharger la version 4.5 ?

Les fichiers d'installation de Systancia Cleanroom 4.5 sont disponibles sur le portail Systancia dans la Marketplace

3.2 Comment installer la version 4.5 ?

Les guides d'installation et de mise à jour de Systancia Cleanroom 4.5 sont disponibles sur le portail Systancia dans Library



SYSTANCIA

Actipolis 3, Bât C11

3, rue Paul Henri Spaak

68 390 SAUSHEIM

France

Téléphone : 03 89 33 58 20

Fax : 03 89 33 58 21

site web : https://www.systancia.com