

Vous pouvez tout voir depuis nos fenêtres

Soyez mieux informé. Une solution intégrée globale pour une gestion totale de la sécurité.

LA SOLUTION CAPTURE SECURITY CENTER DE SONICWALL EST SIMPLE

Avec son authentification unique (SSO) et son architecture sur un seul et même écran (SPOG), surveillez l'ensemble de votre écosystème de sécurité grâce à une solution de gestion évolutive.

Capture Security Center (CSC) vous offre tout ce dont vous avez besoin pour une gestion complète, accessible depuis une interface unique riche en fonctionnalités. Cette dernière permet d'avoir un œil sur tout, y compris l'analyse et le reporting pour la sécurité des réseaux, du sans fil, de la messagerie, des terminaux et du cloud, Risk Meters, ainsi que la gestion des actifs.

CSC est une solution SaaS qui vous offre une plus grande agilité grâce à une vue à 360° de l'ensemble de votre écosystème de sécurité SonicWall. Son intégration fonctionnelle offre une meilleure efficacité et une élasticité

opérationnelle avec une véritable interface SPOG. Prenez des décisions éclairées face à n'importe quelle menace, rapidement, en temps réel (depuis n'importe quel site et n'importe quel appareil connecté), avec des rapports détaillés et des analyses puissantes.

CSC soutient votre stratégie globale de cyberdéfense parce que sa conception est conforme aux exigences de niveau de service pour les centres de sécurité opérationnels (SOC). Il permet de bénéficier d'une gouvernance de la sécurité unifiée, du respect de la conformité et de nombreuses autres stratégies de gestion des risques, le tout à partir d'une seule application Web.



Capture Security Center est une véritable application SPOG qui fournit une solution de gestion globale intégrée. Cette solution est fournie avec la plupart des pare-feu et services dans le cloud de SonicWall.

CAPTURE SECURITY CENTER

Gestion unifiée, reporting et analyses dans le cloud pour la sécurité des réseaux, du sans fil, du switch, de la messagerie, des terminaux et du cloud

EN SAVOIR PLUS

Gestion, Rapports, Analyse, Capture Client, CAS-Shadow IT, CAS-SaaS Security, Sécurité de la messagerie, Sans fil, Licences, Droits

Gagnez en efficacité et en élasticité opérationnelle

Soyez plus efficace. Travaillez plus vite et plus intelligemment en fournissant moins d'efforts.

CAPTURE SECURITY CENTER EST PLUS EFFICACE

Gérez davantage avec une architecture SPOG. Accédez à tout ce qui se trouve dans votre infrastructure de sécurité et votre réseau, y compris l'architecture, les cybermenaces et les problèmes de conformité.

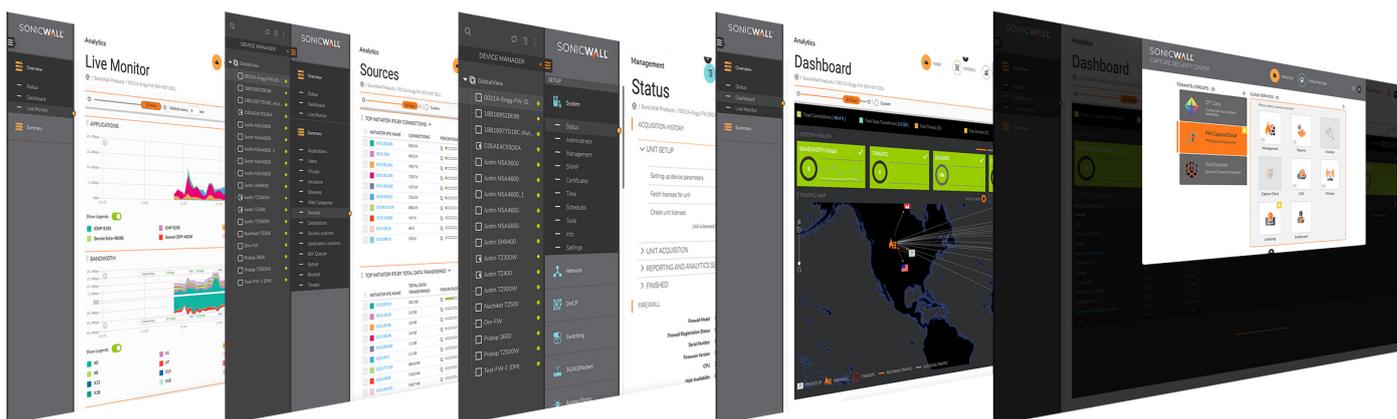
CSC est un outil de gestion de la productivité avec une évolutivité intégrée et une meilleure coordination de la gestion.

L'authentification unique concerne tous les aspects opérationnels de votre réseau, de la sécurité du cloud au terminal. Grâce à la conception native dans le cloud, vous avez tout ce dont vous avez besoin dans un cadre simple et commun. Chaque tâche est plus facile et plus efficace.

Réduisez le temps et les dépenses nécessaires à l'exécution des tâches quotidiennes. Éliminez les silos de sécurité inutiles et gagnez en efficacité grâce à la possibilité de « voir et cliquer » pour tous les flux de travail

vitaux. Obtenez les nouvelles capacités dès qu'elles sont disponibles.

Gérez l'intégralité de votre pile de sécurité SonicWall d'une manière centralisée. Identifiez les failles et les risques en matière de sécurité grâce à Risk Meters et aux analyses précises. Répondez plus rapidement grâce aux informations sur les menaces urgentes et aux renseignements sur la situation. Simplifiez le flux de gestion, réduisez les erreurs de configuration et les erreurs humaines, et déployez facilement des pare-feu, commutateurs et points d'accès distants dans les succursales grâce au déploiement sans intervention.



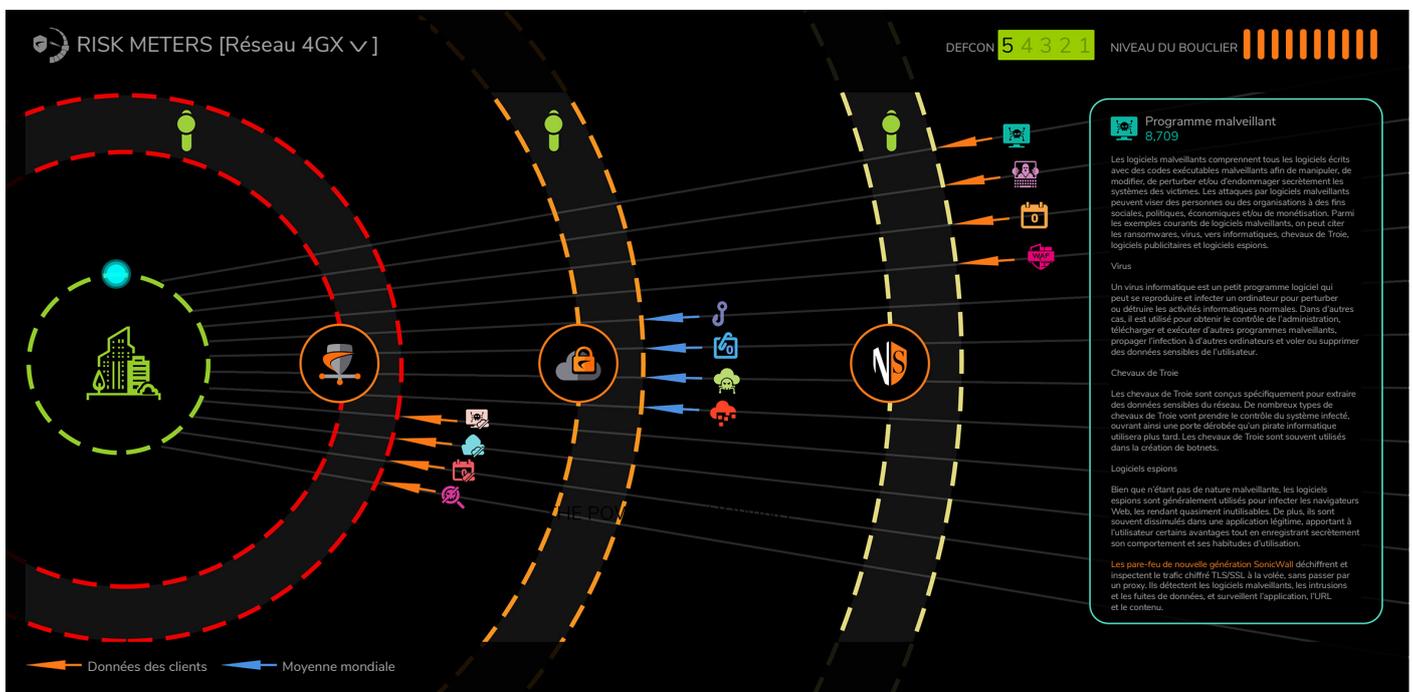
La conception native dans le cloud améliore l'efficacité et l'élasticité opérationnelle. Réduisez les silos de sécurité, augmentez la productivité de l'ensemble de l'environnement de sécurité, le tout à partir d'une seule application.

Renseignements synchronisés sur les cybermenaces pour l'ensemble de votre réseau

Soyez en sécurité. Étudiez vos risques et vos menaces, en temps réel et avec des données réelles.

CAPTURE SECURITY CENTER EST INTELLIGENT

Combinez des données personnalisées basées sur l'état actuel de vos équipements de sécurité avec les renseignements les plus récents sur les cyber-menaces. Défendez votre réseau en vous basant sur les données de risque réel, en temps réel.



Risk Meters affiche automatiquement les données sur les menaces et les scores de risque en se basant sur les données des menaces en direct par rapport à votre niveau actuel de protection. Identifiez les failles dans les couches défensives et prenez des décisions de sécurité en temps réel. Guidez les décisions sur la planification, les règles et la budgétisation de la sécurité en vous basant sur une notation logique.

Avec **SonicWall Risk Meters**, vous pouvez personnaliser votre évaluation de la sécurité en fonction des exigences spécifiques de votre infrastructure réseau. Étudiez les menaces qui pèsent sur votre réseau, projetées dans une analyse en temps réel étayée par des graphiques. Cette ressource

intégrée permet à vos équipes de sécurité de voir les vecteurs de menaces et d'identifier les mesures à prendre pour défendre votre réseau. Regardez les menaces converger sur votre réseau depuis le Web, le cloud, les applications, les terminaux, les appareils mobiles, les bases de données et l'IdO. Visualisez

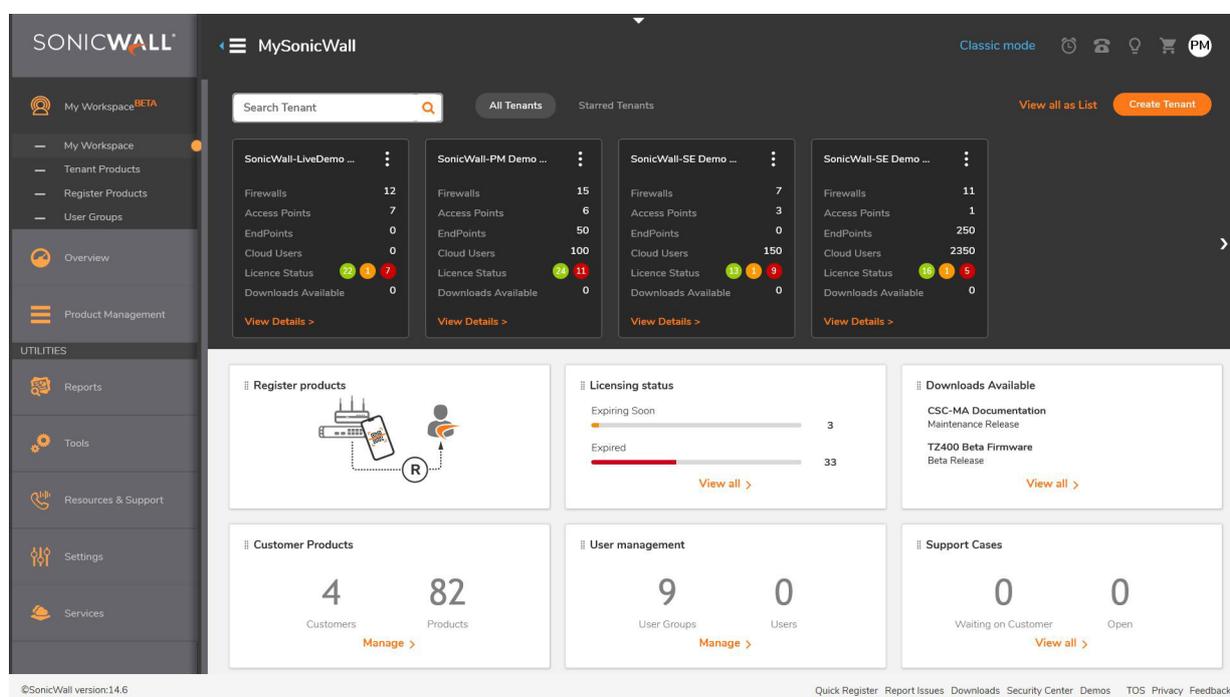
les failles potentielles de sécurité, identifiez les attaques entrantes, surveillez toutes les sources possibles, notamment les services tiers, et prenez des mesures défensives. Éliminez les attaques imprévues et renforcez la sécurité de votre réseau en fonction de ce qui se passe en temps réel.

Gérez la sécurité avec fluidité

Gardez le contrôle. Menez vos opérations de sécurité d'une manière centralisée.

CAPTURE SECURITY CENTER EST UNE SOLUTION COMPLÈTE

Bénéficiez de puissants points de vue « tout-en-un » sur vos environnements de sécurité pour simplifier les processus de gestion et de compte, accélérer la prise de décision, améliorer le support et corriger les failles de sécurité.



Accessible depuis la console cloud Capture Security Center, « My Workspace » de MySonicWall vous permet de mener vos opérations de sécurité complexes d'une manière à la fois plus simple et plus efficace. Ses flux de travail systématiques vous permettent d'intégrer, de configurer et de gérer facilement et rapidement plusieurs locataires sur les campus, dans les succursales ou les groupes

fonctionnels, d'effectuer des enregistrements de produits en masse, d'activer les licences et l'assistance, et de lancer des essais de produits à la demande.

Les flux de travail des locataires fournissent un accès instantané aux équipes chargées des opérations de sécurité dans toutes les entreprises, y compris un contrôle d'accès granulaire basé sur les rôles aux produits gérés par le Capture Security

Center. Un tableau de bord intuitif vous donne une visibilité instantanée et une connaissance des produits dont la licence a expiré ou des produits qui ont besoin de mises à jour logicielles ou du firmware. Engagez, collaborez et communiquez avec les locataires et facilitez, suivez et résolvez les problèmes et les cas d'assistance en utilisant un portail en libre-service intégré.

Récapitulatif des fonctionnalités CSC

Gestion

- Accès SPOG à la plupart des fonctions
- Plusieurs sessions simultanées d'utilisateurs
- Gestion centralisée de la sécurité et du réseau
- Tableau de bord universel
- Gestion des pare-feu
- Gestion des switches SonicWall
- Gestion sans fil
- Configuration centralisée de règles
- Définition de règles au niveau du groupe
- Réplication de règles depuis un appareil vers un seul appareil ou un groupe d'appareils
- Gestion et flux de travail des demandes de modifications
- Déploiement sans intervention
- Configurations pré-fournies et sans intervention des appareils
- Déploiement et configuration du VPN
- Surveillance et système d'alerte des appareils actifs
- Visualisation des applications et renseignements

- Prise en charge API, CLI et SNMP
- Gestion Capture Client
- Gestion Cloud App Security
- Gestion Hosted Email Security
- MySonicWall et MyWorkspace
- Risk Meters
- Security Center
- Cloud App Security – Shadow IT
- Gestion des licences
- Gestion basée sur les rôles (utilisateurs, groupes)
- Sauvegarde des fichiers de préférences pour les pare-feu

Surveillance

- Surveillance et système d'alerte des appareils
- Flux de données IPFIX en temps réel
- Surveillance et système d'alerte des périphériques actifs
- Gestion des relais SNMP
- Surveillance de l'état des VPN et pare-feu
- Risk Meters

Reporting

- Journalisation centralisée des pare-feu
- Rapports Syslog ou IPFIX
- Rapports PDF programmés personnalisés
- Rapport sur plusieurs menaces
- Rapport centré sur l'utilisateur
- Rapport sur l'utilisation des applications
- Rapport sur les botnets
- Rapport Geo IP
- Rapport sur les adresses MAC
- Rapport Capture ATP
- Rapport sur les points d'accès sans fil indésirables
- Rapport Cloud App Security (CAS)
- Rapport Capture Client
- Rapport sur les services et la bande passante par interface

Analyse

- Activités basées sur les utilisateurs
- Utilisation des applications
- Visibilité entre les produits avec Capture Client
- Visualisation dynamique en temps réel
- Fonctionnalités d'exploration approfondie et de pivotement

Licences et formules

Les services cloud sont disponibles dans les formules suivantes.

1. Gestion CSC, version basique (Lite)

Cette version convient mieux pour la sauvegarde/restauration des systèmes ou des préférences de pare-feu, ainsi que pour la mise à niveau du micrologiciel. Tout pare-feu avec un abonnement AGSS ou CGSS peut disposer de cette fonctionnalité de gestion de base pour faciliter l'administration des pare-feu.

2. Gestion CSC

Cette option d'abonnement payant active des fonctions de gestion complète, y compris l'automatisation des flux de travail et le déploiement sans intervention.

3. Gestion et reporting CSC

Cette option de licence est idéale pour les établissements plus grands disposant de nombreux pare-feu déployés dans des endroits géographiquement dispersés qui disposent d'une gestion inférieure au niveau du groupe ou basée sur le client. Il s'agit notamment de PME, d'entreprises distribuées, du secteur public et d'établissements d'enseignement avec de nombreux districts et campus, ainsi que de fournisseurs de services gérés (MSP).

Outre ses capacités de gestion complètes, cette option d'abonnement offre des fonctionnalités complètes de reporting pour effectuer des examens et des audits de performance réseau ou des contrôles de sécurité périodiques ou à la demande. Cela peut se faire à l'aide du tableau de bord interactif universel affiché à l'écran avec des tableaux et graphiques en direct, ou en dehors de l'écran avec des rapports exportés programmés.

4. Analyses CSC

Il s'agit d'un service complémentaire puissant pour toutes les options d'abonnement à Capture Security Center. Activer le service permet d'accéder pleinement aux outils et services de sécurité et d'analyse de l'application SonicWall Cloud App pour mener des analyses forensiques sur le réseau et rechercher des menaces à l'aide de fonctionnalités d'exploration approfondie et de pivotement. CSC Analytics comprend également 30 jours de stockage des journaux et 365 jours de reporting.

Modèles de pare-feu pris en charge

Capture Security Center est disponible pour les clients équipés des pare-feu SOHO-W, SOHO 250, SOHO 250W, TZ Series, NSA Series, NSa 2650-6650 et NSv Series. Pour les séries SuperMassive 9000 Series, NSa Series et NSsp 12400 à 12800, l'option d'abonnement à la gestion CSC est automatiquement activée dans le cadre de l'activation de son abonnement AGSS correspondant.

CAPTURE SECURITY CENTER

	Gestion	Reporting ⁴	Analyses ⁴
Pare-feu d'entrée de gamme	SOHO-W, SOHO 250, SOHO 250W TZ Series, NSv 10-100	SOHO-W, SOHO 250, SOHO 250W, TZ Series, NSv 10-100	SOHO-W, SOHO 250, SOHO 250W, TZ Series, NSv 10-100
Pare-feu de milieu de gamme	NSA Series, NSa Series, NSv 200-400	NSA Series, NSa Series, NSv 200-400	NSA Series, NSa Series, NSv 200-400
Pare-feu haut de gamme	SuperMassive 9000 series, NSsp 12000 series, NSa 9250-9650, NSv 800-1600	SuperMassive 9000 series, NSsp 12000 series, NSa 9250-9650, NSv 800-1600	SuperMassive 9000 series, NSsp 12000 series, NSa 9250-9650, NSv 800-1600

⁴La prise en charge du reporting et de l'analyse pour les pare-feu haut de gamme est disponible uniquement sur l'analyse On_prem.

	Fonctionnalités	Gestion CSC Lite	Gestion CSC	Gestion et reporting CSC	Analyses SaaS	Analyses sur site
Gestion	Sauvegarde/restauration – système pare-feu	Oui	Oui	Oui	Oui	Oui ²
	Sauvegarde/restauration – préférences pare-feu	Oui	Oui	Oui	Oui	Oui ²
	Mise à niveau firmware	Uniquement depuis le fichier local	Uniquement depuis le fichier local ou MySonicWall	Oui	Uniquement depuis le fichier local	Uniquement depuis le fichier local ³
	Planification des tâches	-	Oui	Oui	-	-
	Gestion des pare-feu de groupe	-	Oui	Oui	-	-
	Héritage – avancer/inverser	-	Oui	Oui	-	-
	Déploiement sans intervention ¹	-	Oui	Oui	-	-
	Téléchargements des signatures de pare-feu hors ligne	-	Oui	Oui	-	-
	Flux de travail	-	Oui	Oui	-	-
	Licences groupées – Recherche, partage, inventaire des codes d'activation utilisés	-	Oui	Oui	-	-
Reporting (Basé sur Netflow/IPFIX)	Planification de rapports, surveillance en direct, tableaux de bord récapitulatifs	-	-	Oui	Oui	Oui
	Télécharger les rapports : Applications, menaces, CFS, utilisateurs, trafic, source/ destination (reporting sur les flux sur 1 an)	-	-	Oui	Oui	Oui
Analyse (Basée sur Netflow/IPFIX)	Analyse forensique du réseau et détection des menaces à l'aide d'une exploration approfondie et de pivots	-	-	-	Oui	Oui
	Cloud App Security – Shadow IT	-	-	-	Oui	Non
	Conservation des données	-	-	-	Trafic sur 30 jours	1 an
Support technique		Cas Web uniquement	Support 24 h/24, 7 j/7	Support 24 h/24, 7 j/7	Support 24 h/24, 7 j/7	Support 24 h/24, 7 j/7

¹ Pris en charge pour SOHO-W avec le firmware 6.5.2+ ; TZ, NSA Series et NSa 2650-6650 avec le firmware 6.5.1.1+. Non pris en charge pour les SOHO ou NSv Series.

² Requiert le service AGSS/CGSS ou tout service Capture Security Center payant.

³ Requiert une licence d'assistance 24 h/24, 7 j/7.

Informations de commande

Produit	Référence
Logiciel de gestion SonicWall Capture Security Center pour TZ Series, SOHO-W, SOHO 250, SOHO 250W, NSv 10 à 100 1 an	01-SSC-3664
Logiciel de gestion SonicWall Capture Security Center pour TZ Series, SOHO-W, SOHO 250, SOHO 250W NSv 10 à 100 2 ans	01-SSC-9151
Logiciel de gestion SonicWall Capture Security Center pour TZ Series, SOHO-W, SOHO 250, SOHO 250W NSv 10 à 100 3 ans	01-SSC-9152
Logiciel de gestion SonicWall Capture Security Center pour NSA 2600 à 6600, NSa 2650 à 6650 et NSv 200 à 400 1 an	01-SSC-3665
Logiciel de gestion SonicWall Capture Security Center pour NSA 2600 à 6600, NSa 2650 à 6650 et NSv 200 à 400 2 ans	01-SSC-9214
Logiciel de gestion SonicWall Capture Security Center pour NSA 2600 à 6600, NSa 2650 à 6650 et NSv 200 à 400 3 ans	01-SSC-9215
Logiciel de gestion et de reporting SonicWall Capture Security Center pour TZ Series, SOHO-W, SOHO 250, SOHO250W, NSv 10 à 100 1 an	01-SSC-3435
Logiciel de gestion et de reporting SonicWall Capture Security Center pour TZ Series, SOHO-W, SOHO 250, SOHO250W, NSv 10 à 100 2 ans	01-SSC-9148
Logiciel de gestion et de reporting SonicWall Capture Security Center pour TZ Series, SOHO-W, SOHO 250, SOHO250W, NSv 10 à 100 3 ans	01-SSC-9149
Logiciel de gestion et de reporting SonicWall Capture Security Center pour NSA 2600 à 6600, NSa 2650 à 6650 et NSv 200 à 400 1 an	01-SSC-3879
Logiciel de gestion et de reporting SonicWall Capture Security Center pour NSA 2600 à 6600, NSa 2650 à 6650 et NSv 200 à 400 2 ans	01-SSC-9154
Logiciel de gestion et de reporting SonicWall Capture Security Center pour NSA 2600 à 6600, NSa 2650 à 6650 et NSv 200 à 400 3 ans	01-SSC-9202
Logiciel d'analyse SonicWall Capture Security Center pour SOHO-W, SOHO 250, SOHO250W, TZ Series, NSv 10 à 100 1 an	02-SSC-0171
Logiciel d'analyse SonicWall Capture Security Center pour NSA 2600 à 6600, NSa 2650 à 6650 et NSv 200 à 400 1 an	02-SSC-0391

Navigateurs Internet

- Microsoft® Internet Explorer 11.0 ou supérieur (ne pas utiliser le mode de compatibilité)
- Mozilla Firefox 37.0 ou version ultérieure
- Google Chrome 42.0 ou version ultérieure
- Safari (dernière version)

Appliances SonicWall prises en charge par Capture Security Center

- Appliances de sécurité réseau SonicWall : SuperMassive E10000 et 9000 Series, E-Class NSA, NSsp Series, NSa Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- Appliances virtuelles de sécurité réseau SonicWall : NSv Series
- Sécurité des terminaux SonicWall – Capture Client
- Sécurité du cloud SonicWall – Cloud App Security (CAS)
- SonicWall Email Security
- SonicWall Web Application Firewall
- SonicWall Secure Mobile Access : SMA 100 Series

À propos de SonicWall

SonicWall offre une Boundless Cybersecurity pour l'ère de l'hyper-distribution et une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. En connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant de véritables économies, SonicWall comble le fossé commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour en savoir plus, rendez-vous sur www.sonicwall.com.