

Quoi de neuf dans UserLock ?

Quoi de neuf dans UserLock 5.5 ?.....	2
1.Nouvelle fonctionnalité Economiseur d'écran	2
2.Nouvelle fonctionnalité d'Inactivité des sessions.....	2
3.Nouvelle fonctionnalité Arrêt des machines.....	2
4.Nouvelle fonctionnalité : Stratégie de groupe.....	3
5.Améliorations et optimisations	3
Quoi de neuf dans UserLock 5 ?.....	4
1.Nouvelle interface	4
1.1.CONSOLE WINDOWS	4
1.2.WEB CONSOLE.....	9
2.Rapports	10
2.1.GENERAL.....	10
2.2.COMMENT PLANIFIER UN RAPPORT ET SON ENVOI AUTOMATIQUE PAR EMAIL.....	11
2.3.NOUVEAU MODE POUR LE RAPPORT STATISTIQUES DES SESSIONS	17
3.Sessions RAS	18
3.1.SESSIONS VPN AVEC UN SERVEUR RRAS.....	19
3.2.SESSIONS RADIUS AVEC IAS	19
3.3.CONFIGURER DES RESTRICTIONS POUR LES SESSIONS RAS	20

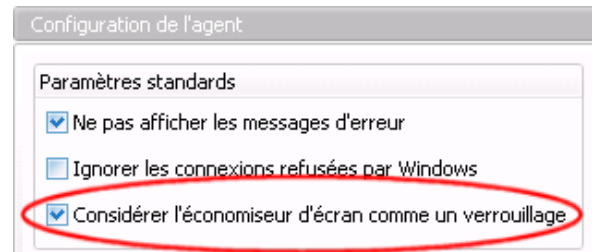
For additional information, please contact IS Decisions at one of the following:

Quoi de neuf dans UserLock 5.5 ?

1. Nouvelle fonctionnalité Economiseur d'écran

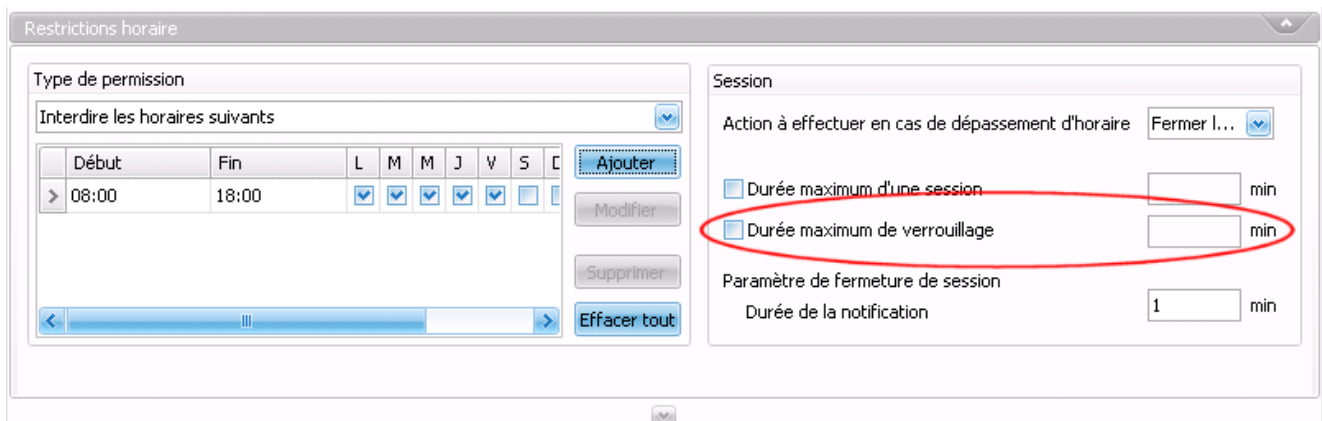
Il est désormais possible de considérer le démarrage d'un économiseur d'écran protégé par mot de passe comme un verrouillage de session.

Cochez l'option « *Considérer l'économiseur d'écran comme un verrouillage* » dans les propriétés de *Distribution de l'agent*.



2. Nouvelle fonctionnalité d'Inactivité des sessions

Il est maintenant possible de fermer une session après un certain temps de verrouillage. Combiné à la précédente fonctionnalité « *Considérer l'économiseur d'écran comme un verrouillage* » UserLock peut donc fermer automatiquement les sessions après un certain temps d'inactivité.

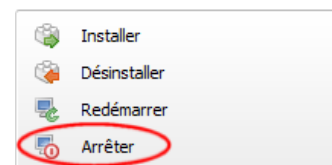


Dans le *Compte protégé* concerné, cocher « *Durée maximum de verrouillage* » et spécifier un délai en minutes.

3. Nouvelle fonctionnalité Arrêt des machines

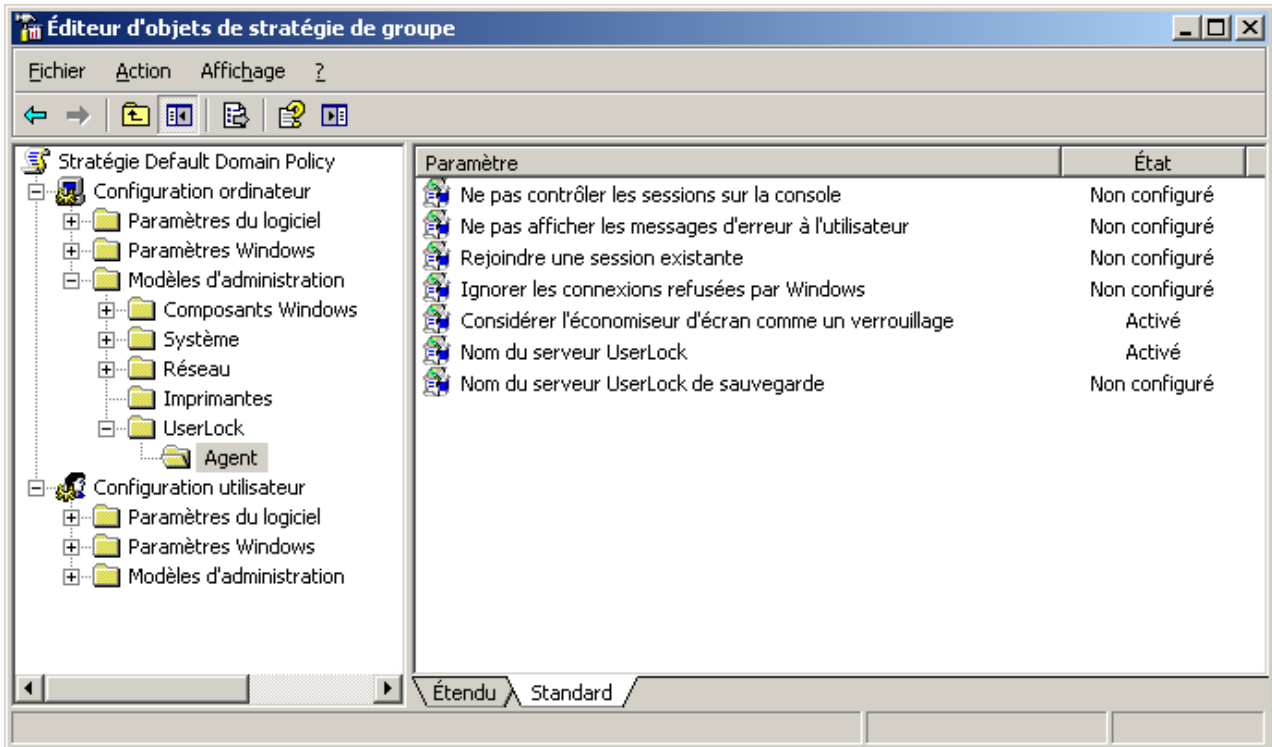
Il est maintenant possible de lancer un arrêt des machines à distance.

Cette commande est disponible dans *Distribution de l'agent*, dans la fenêtre *Actions* ou par le menu contextuel.



4. Nouvelle fonctionnalité : Stratégie de groupe

Un fichier de type *.adm* est maintenant disponible dans le répertoire d'installation de UserLock. Il permet de déployer les paramètres de l'agent à l'aide des *Stratégies de groupe*. C'est le complément idéal au déploiement de l'agent avec le *package MSI* par les *Stratégies de groupe*.



5. Améliorations et optimisations

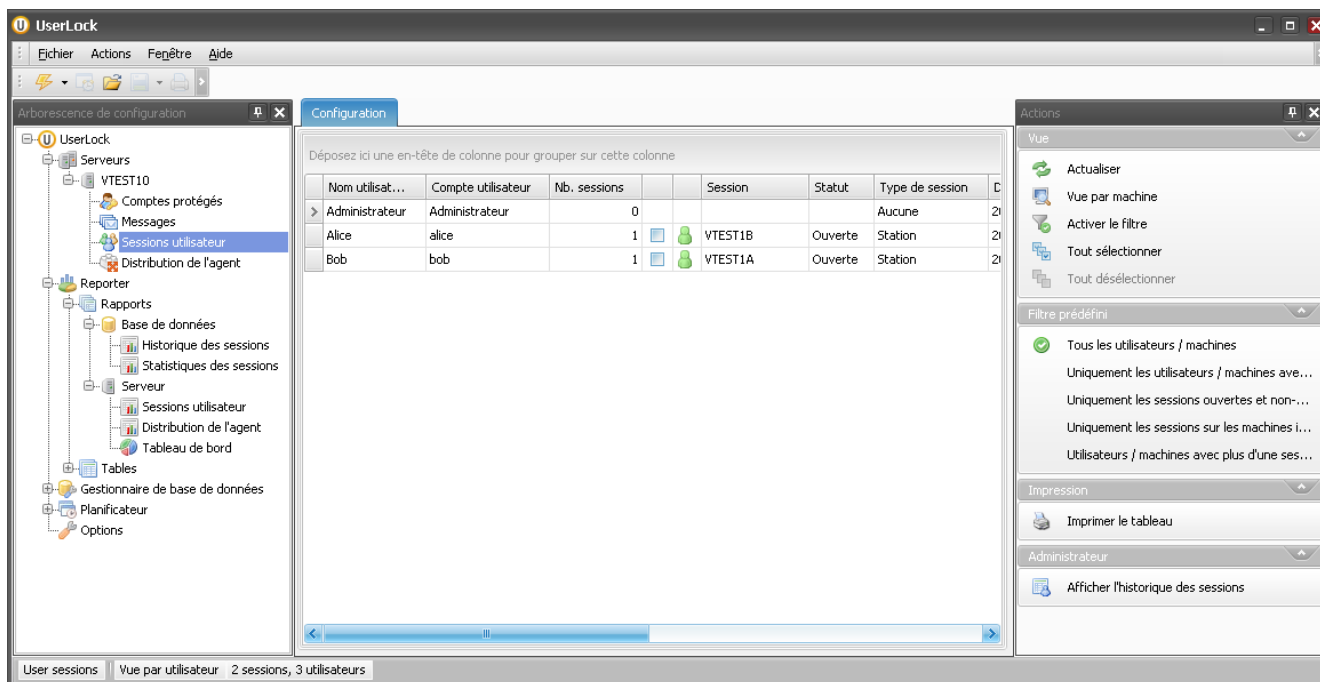
- Possibilité d'utiliser un grand nombre de *Comptes protégés* (jusqu'à 10.000).
- La requête du rapport d'*Historique des sessions* a été optimisée pour que le rapport s'affiche plus rapidement.
- Le rapport d'*Historique des sessions* peut désormais afficher les Sessions refusées par UserLock et les Sessions refusées par Windows de façon indépendante.

For additional information, please contact IS Decisions at one of the following:

Quoi de neuf dans UserLock 5 ?

1. Nouvelle Interface

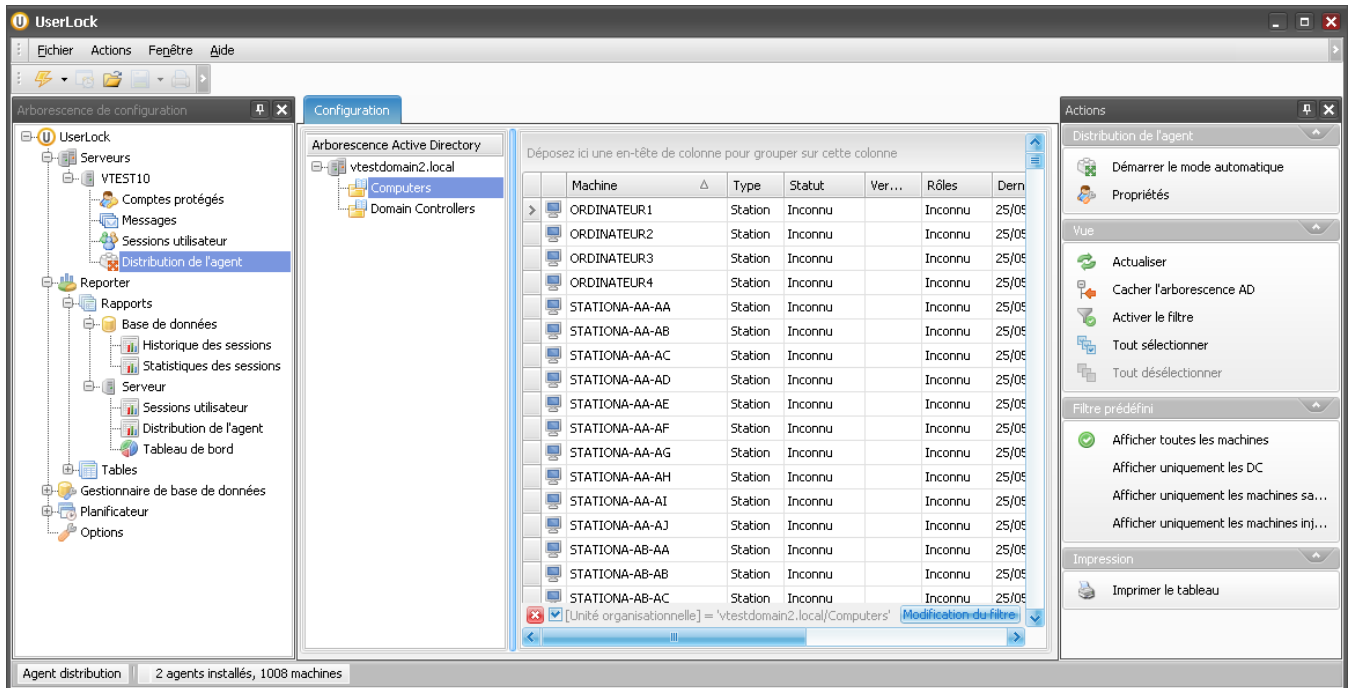
1.1. Console Windows



- Une nouvelle interface à onglets.
- Un **tableau de bord** permettant d'afficher des graphiques de statistiques.
- Les rapports sont affichés dans un nouvel onglet au lieu d'une nouvelle fenêtre.
- Un nouvel éditeur de propriétés : Les propriétés de chaque objet sont maintenant affichées dans un nouvel onglet au lieu d'une nouvelle fenêtre.
- Le *Reporter* est maintenant intégré dans la console.
- Le *Nettoyeur de base de données* est maintenant intégré dans la console.
- Le *Planificateur* est maintenant intégré dans la console.
- **La génération de rapports peut maintenant être planifiée très facilement** sans utilisation de lignes de commande. Les rapports peuvent également être envoyés automatiquement par email (Cf. *Rapports*).
- Les actions du menu contextuel sont aussi accessibles par la **fenêtre d'Actions**.

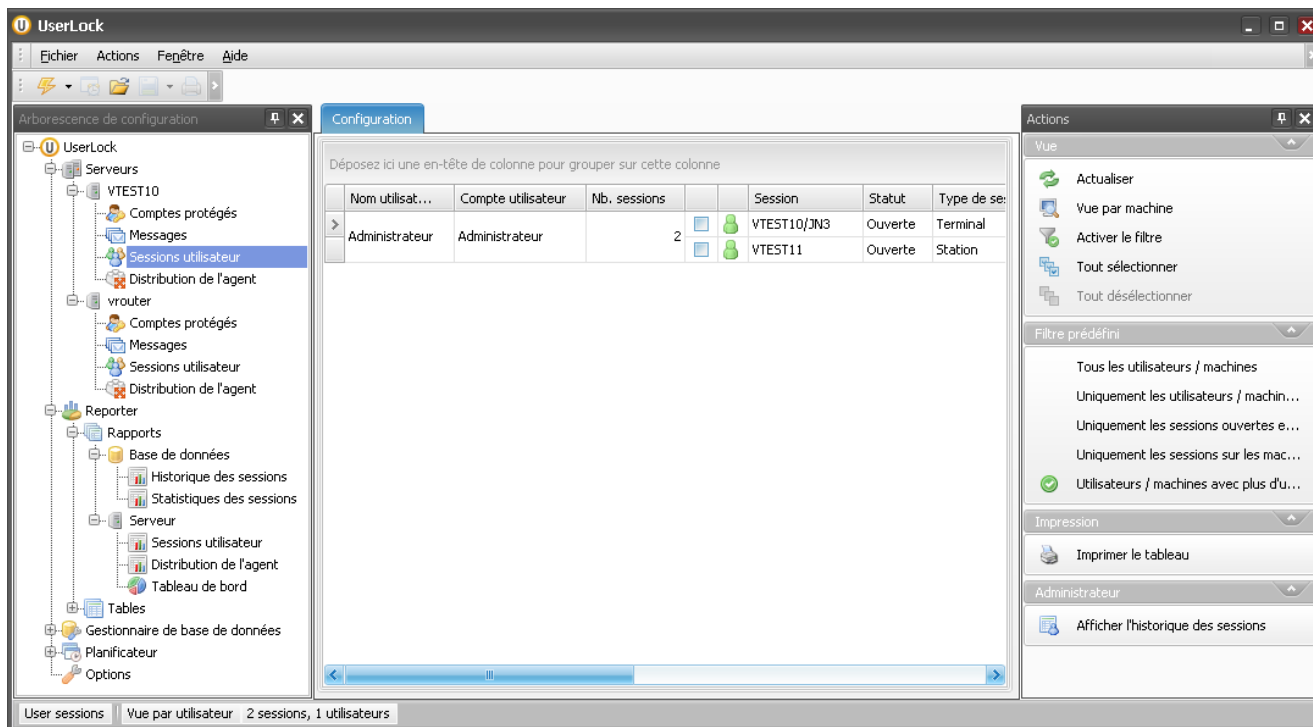
For additional information, please contact IS Decisions at one of the following:

- **L'arborescence Active Directory** peut être affichée dans la section *Distribution de l'agent* et *Sessions utilisateur* dans le mode *Vue par machines*.



For additional information, please contact IS Decisions at one of the following:

- Un **nouveau filtre prédéfini** a été ajouté et permet de ne visualiser que les utilisateurs ou machines avec plus d'une session.



For additional information, please contact IS Decisions at one of the following:

- Le filtre automatisé fait son apparition pour trouver rapidement des utilisateurs ou des machines (Cliquer sur *Activer le filtre automatique* dans la fenêtre d'Actions).

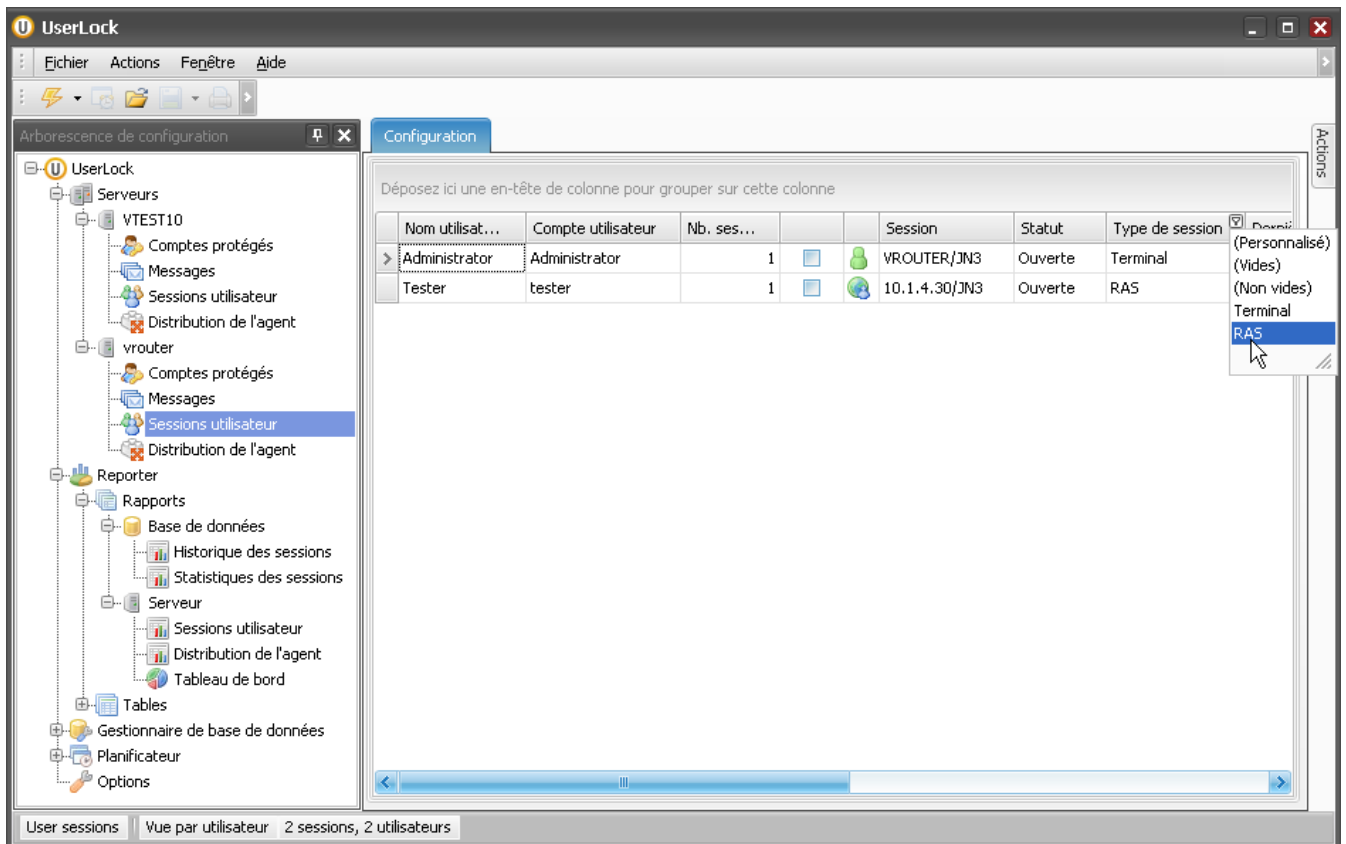
The screenshot shows the UserLock application window. On the left is a configuration tree with 'Sessions utilisateur' selected. The main area is a 'Configuration' window containing a table of user sessions. A filter is applied to the 'Nom utilisateur' column, showing only the user 'Bob'.

Nom utilisat...	Compte utilisateur	Nb. sessions	Session	Statut	Type de session	D
Bob	bob	1	VTEST1A	Ouverte	Station	20

At the bottom of the configuration window, the filter is displayed as: [Nom utilisateur] Comme 'B%' with a 'Modification du filtre' button.

For additional information, please contact IS Decisions at one of the following:

- **Le filtre rapide** : Vous pouvez maintenant cliquer sur une icône dans coin haut à droite de chaque colonne pour afficher une liste de toutes les valeurs présente dans la colonne cible. Sélectionner une valeur pour filtrer la vue en fonction de celle-ci sur la colonne cible.

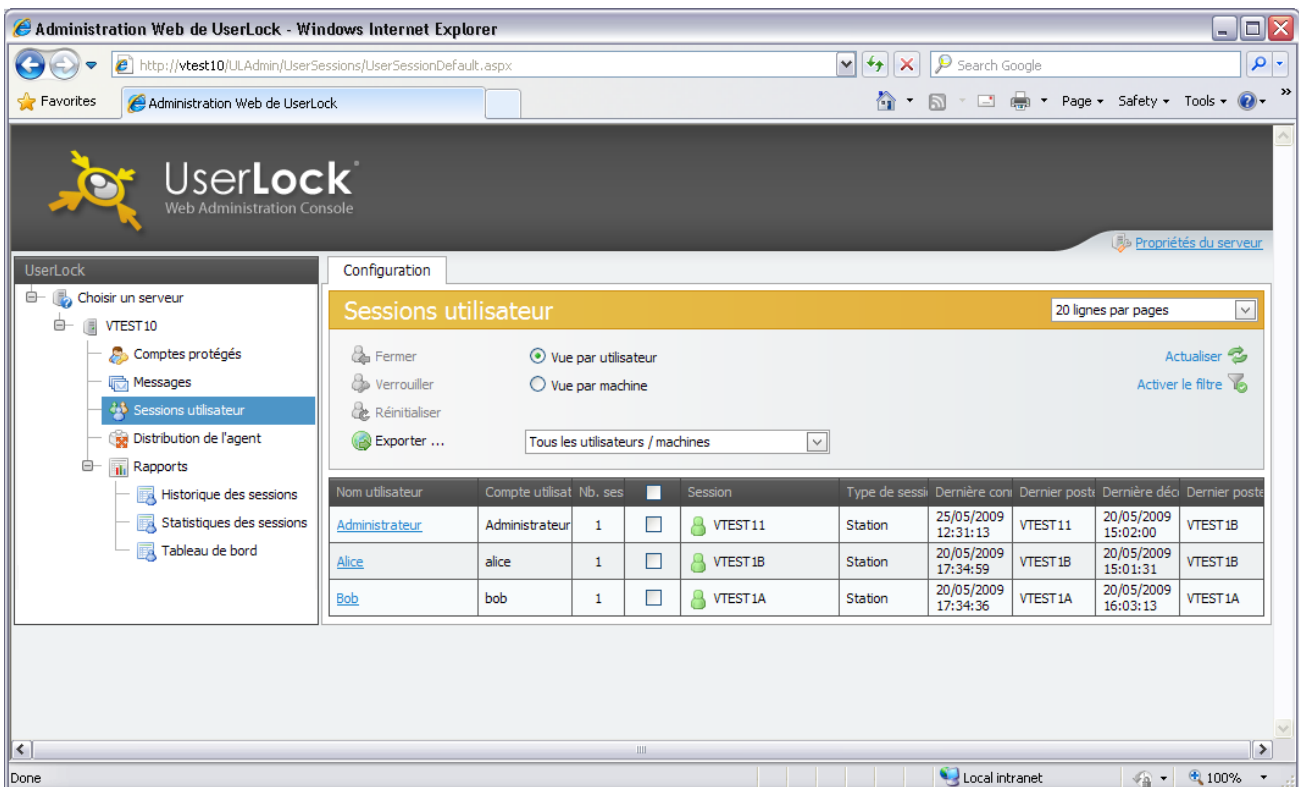


- Vous pouvez aussi configurer un **filtre avancé**. Cliquer-droit sur une l'entête d'une colonne puis sur *Editeur de filtre*.



1.2. Web console

- Une nouvelle interface à onglets.
- Un **tableau de bord** permettant d'afficher des graphiques de statistiques.
- **La possibilité de trier les utilisateurs et les machines** en fonction d'une ligne spécifique. Il suffit de cliquer sur l'entête de la ligne.
- **Le filtre automatisé** fait son apparition pour trouver rapidement des utilisateurs ou des machines dans la console.
- **L'arborescence Active Directory** peut être affichée dans la section *Distribution de l'agent* et *Sessions utilisateur* dans le mode *Vue par machines*.
- La gestion des droits UserLock est maintenant accessible dans la console Web à travers les *Propriétés du serveur*.
- La vue par *Sessions utilisateur* affiche maintenant le nom complet de l'utilisateur et le nom du compte.



The screenshot shows the UserLock Web Administration Console interface. The left sidebar contains a tree view with categories like 'Comptes protégés', 'Messages', 'Sessions utilisateur', 'Distribution de l'agent', 'Rapports', 'Historique des sessions', 'Statistiques des sessions', and 'Tableau de bord'. The main content area is titled 'Sessions utilisateur' and includes configuration options for 'Vue par utilisateur' (selected) and 'Vue par machine'. Below the configuration is a table of active sessions.

Nom utilisateur	Compte utilisat	Nb. ses		Session	Type de sessi	Dernière con	Dernier post	Dernière déo	Dernier poste
Administrateur	Administrateur	1	<input type="checkbox"/>	VTEST11	Station	25/05/2009 12:31:13	VTEST11	20/05/2009 15:02:00	VTEST1B
Alice	alice	1	<input type="checkbox"/>	VTEST1B	Station	20/05/2009 17:34:59	VTEST1B	20/05/2009 15:01:31	VTEST1B
Bob	bob	1	<input type="checkbox"/>	VTEST1A	Station	20/05/2009 17:34:36	VTEST1A	20/05/2009 16:03:13	VTEST1A

For additional information, please contact IS Decisions at one of the following:

2. Rapports

2.1. Général

- Pour afficher un rapport, sélectionner le dans l'arborescence du menu *Rapports*, configurer le selon vos critères puis lancer sa génération en cliquant sur le bouton *Exécution* présent dans la barre d'outils.
- Les rapports UserLock utilise maintenant un nouveau moteur de rapport et bénéficie d'une nouvelle présentation graphique.

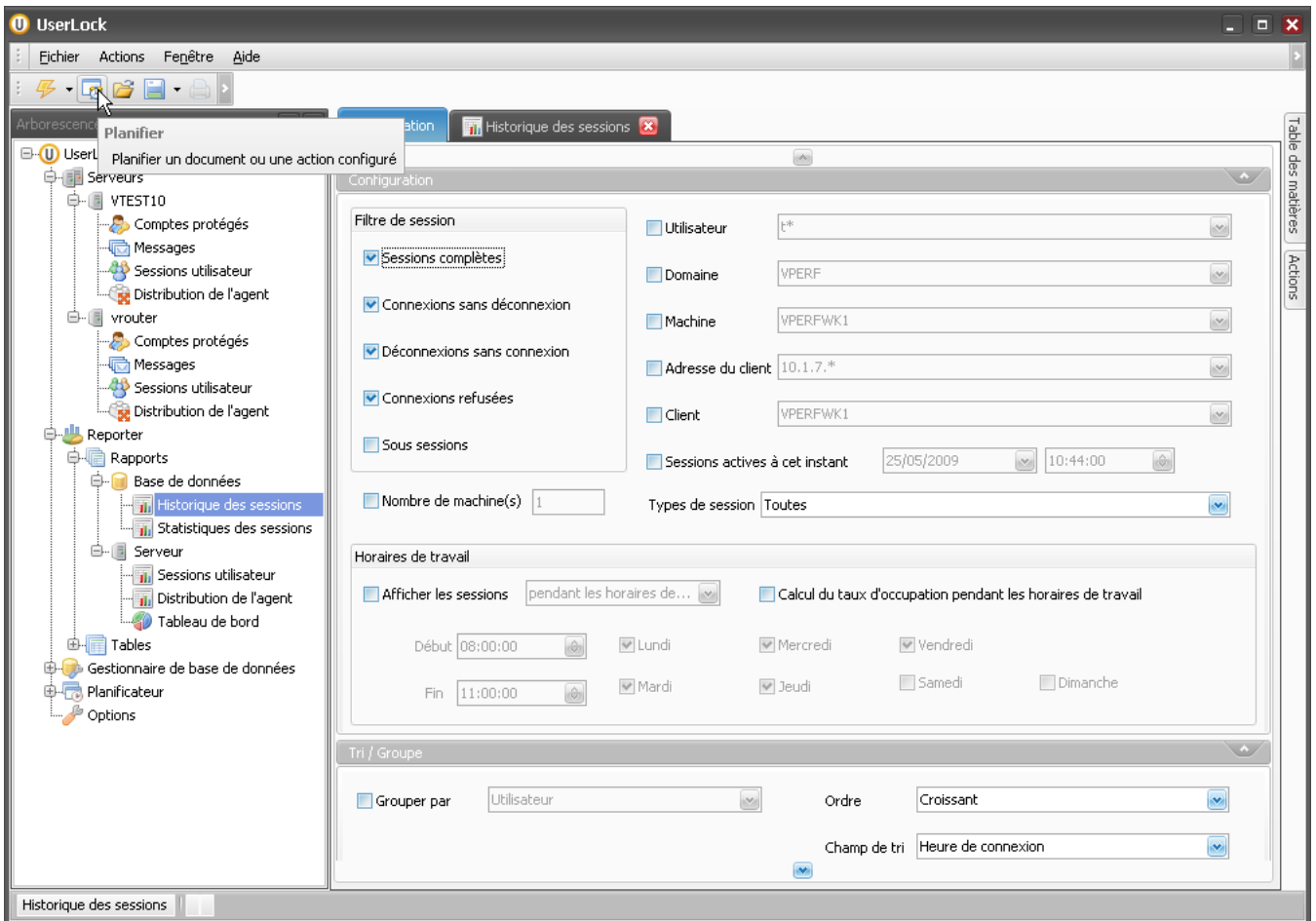
The screenshot shows the UserLock application window. The left sidebar contains a configuration tree with categories like 'Serveurs', 'Reporter', and 'Rapports'. The main window displays the 'Historique des sessions' report for the date 25/05/2009. The report includes configuration settings such as 'Sessions complètes', 'Connexions sans déconnexion', and 'Types de session: Toutes'. It also shows a table of session events with columns for connection and disconnection times, user names, domains, and machines.

Heure de connexion	Heure de déconnexion	Utilisateur	Domaine	Mach
10/04/2009 09:12:10	08/05/2009 13:06:16	User1	MyDomain	Workstation1
27/04/2009 09:20:16	06/05/2009 16:01:23	User5	MyDomain	Workstation5
04/05/2009 18:58:22	06/05/2009 10:19:36	User7	MyDomain	Workstation7
04/05/2009 19:00:45	06/05/2009 10:19:18	User7	MyDomain	10.1.1.1
06/05/2009 08:11:29	06/05/2009 16:46:51	User3	MyDomain	Workstation3
06/05/2009 09:17:42	06/05/2009 17:27:27	User9	MyDomain	Workstation9
06/05/2009 09:19:45	06/05/2009 17:28:11	User1	MyDomain	Workstation1
06/05/2009 09:31:09	06/05/2009 18:25:09	User6	MyDomain	Workstation6
06/05/2009 09:31:34	06/05/2009 17:29:25	User8	MyDomain	Workstation8
06/05/2009 09:39:57	06/05/2009 16:04:14	User2	MyDomain	Workstation2

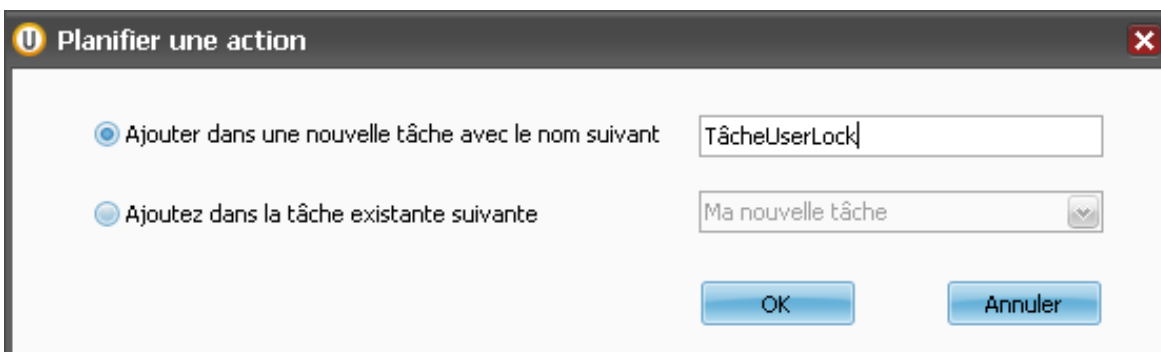
For additional information, please contact IS Decisions at one of the following:

2.2. Comment planifier un rapport et son envoi automatique par email

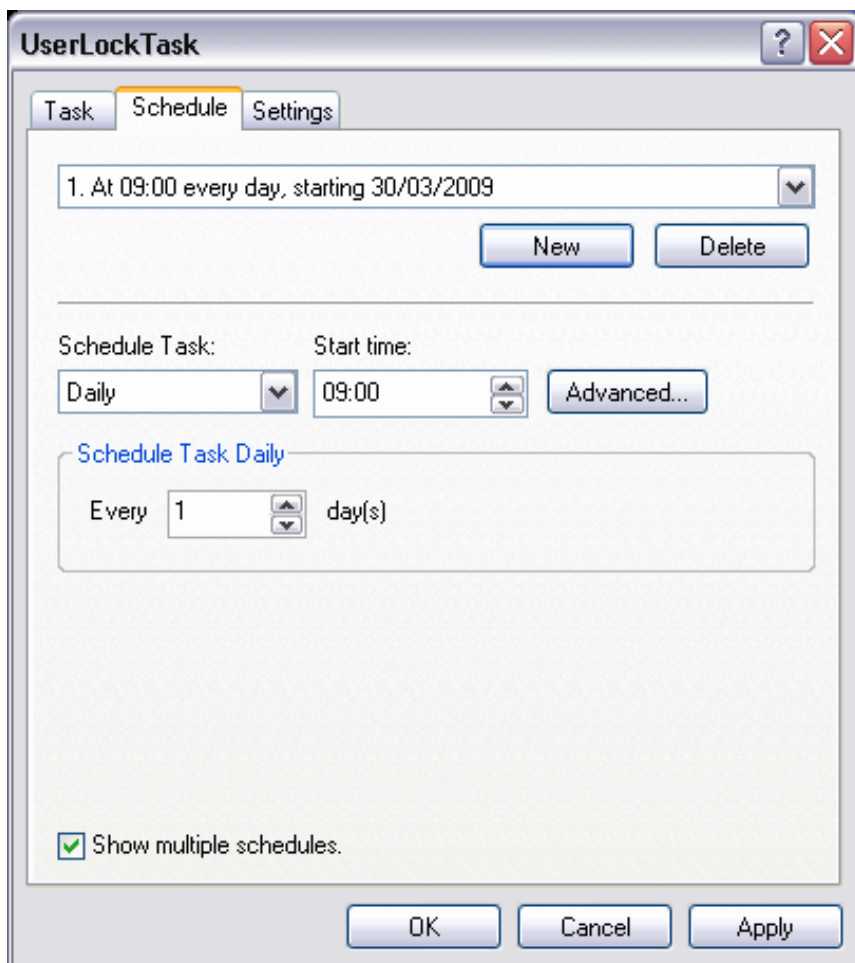
Configurer le rapport et cliquer sur le bouton *Planifier* :



Saisir un nom pour la nouvelle tâche :

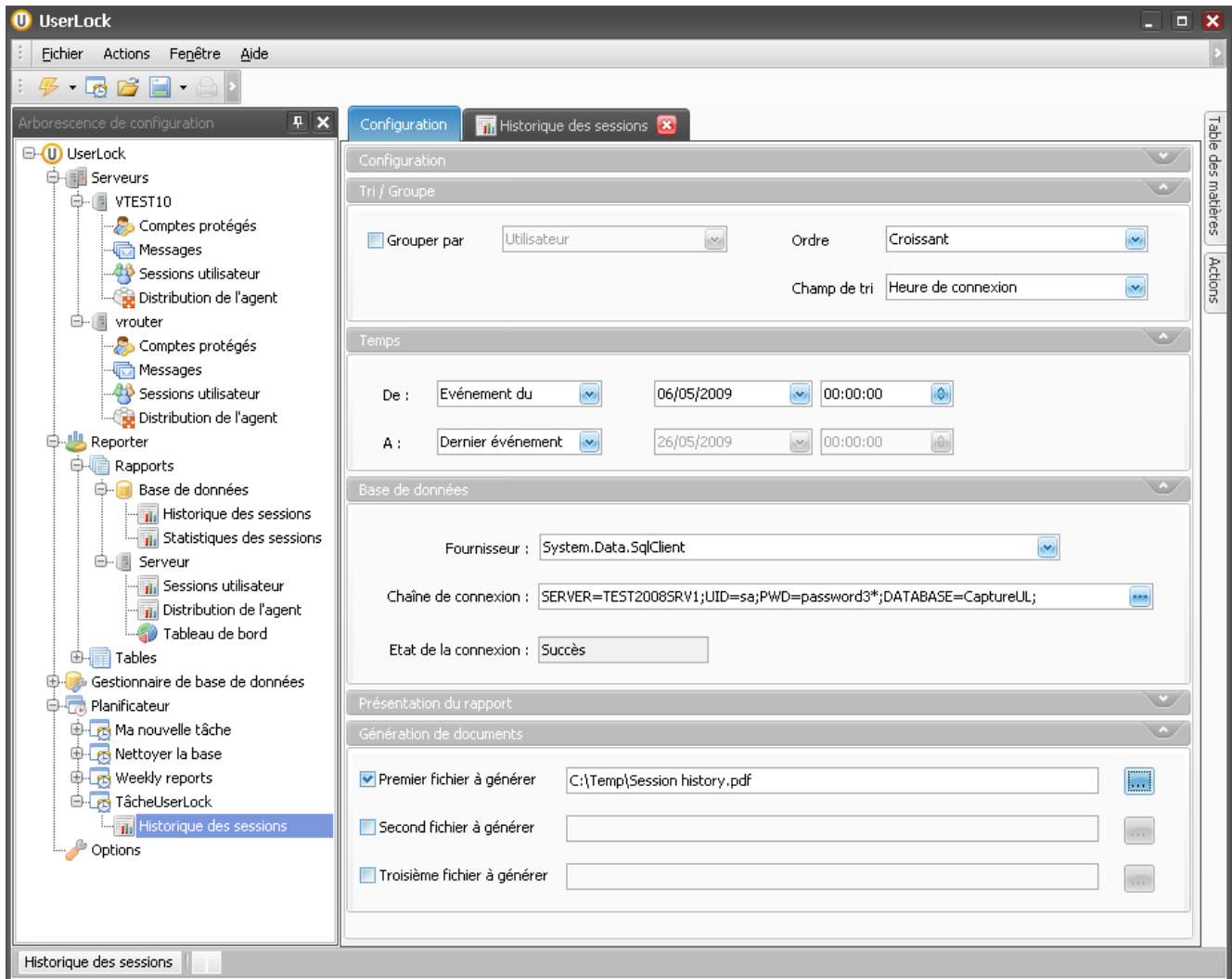


Configurer l'onglet *Planification* :



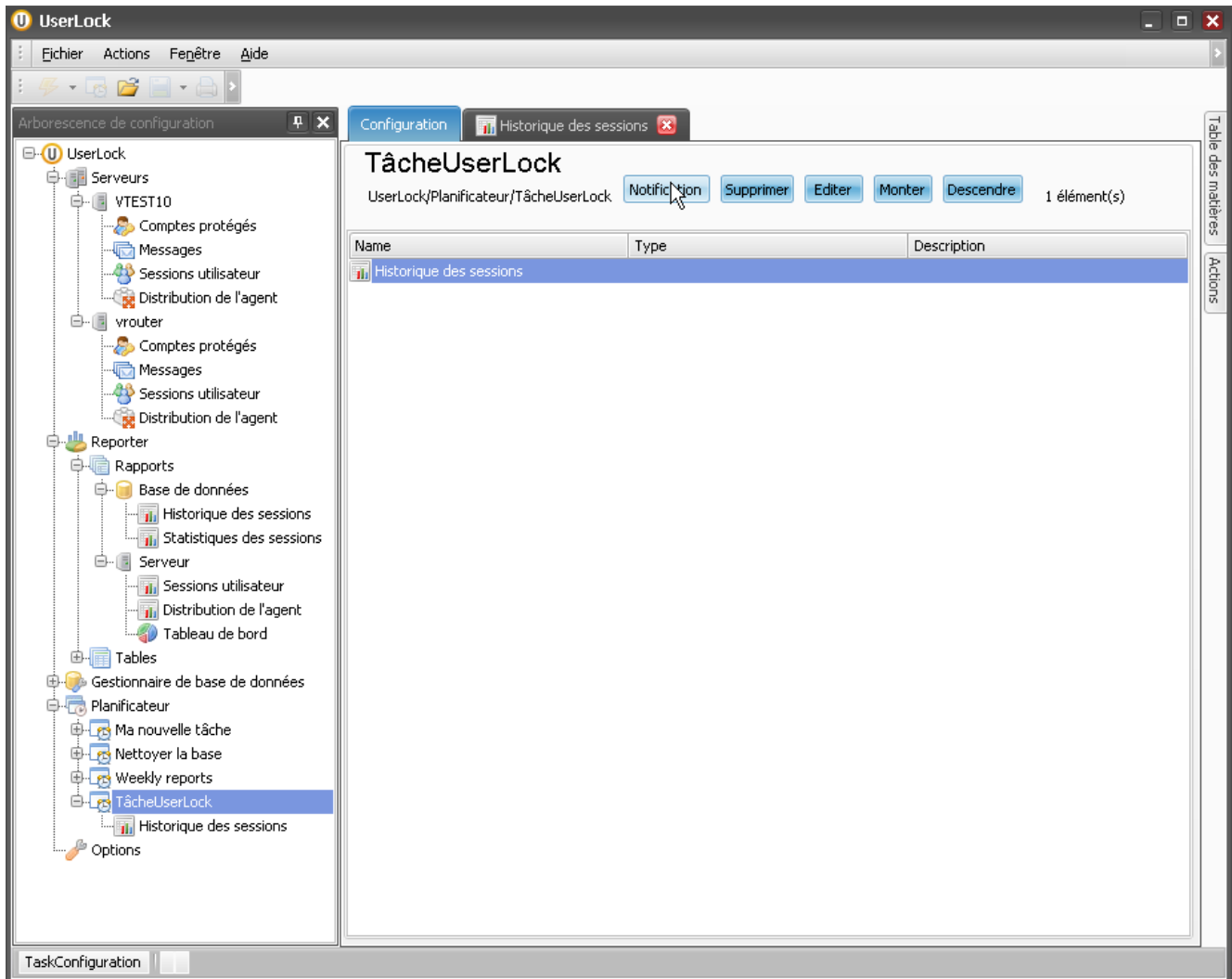
For additional information, please contact IS Decisions at one of the following:

La tâche est ajoutée dans le *Planificateur*. Il est nécessaire de configurer le fichier pour générer le rapport :



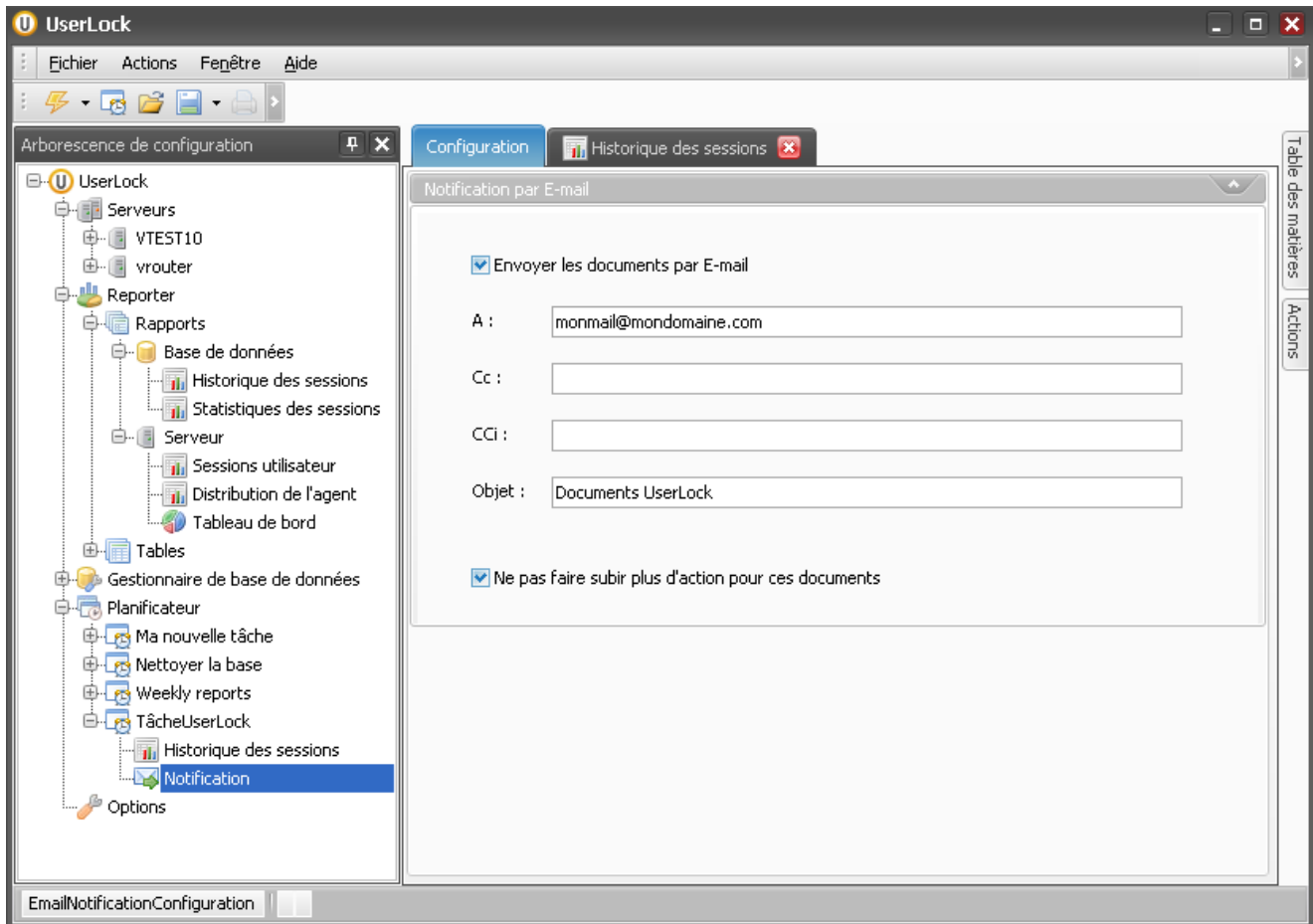
For additional information, please contact IS Decisions at one of the following:

Ajouter une *Action de notification* pour l'envoi du rapport par email :



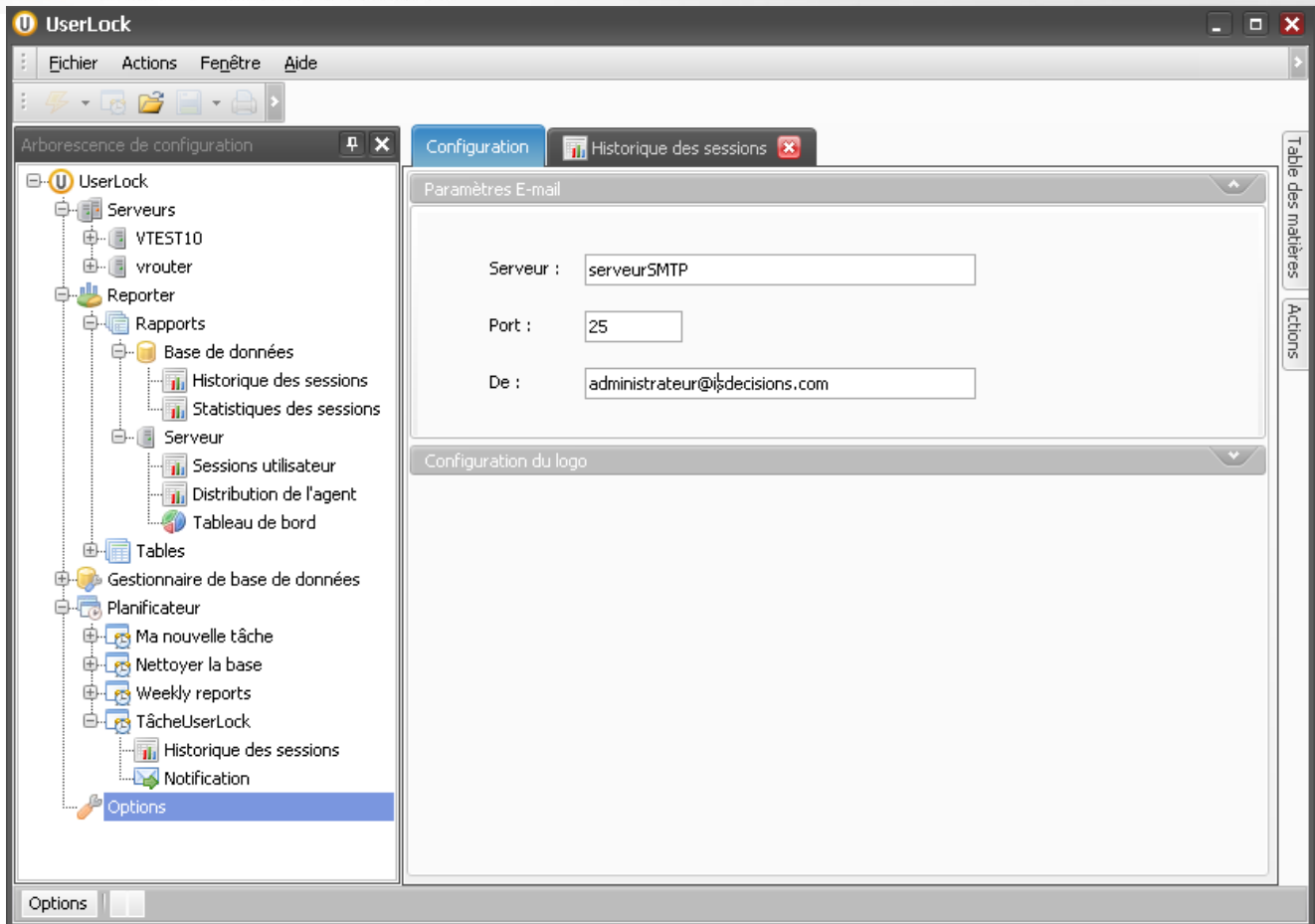
For additional information, please contact IS Decisions at one of the following:

Configurer la *Notification* :



Configurer les paramètres SMTP de la console UserLock (*différents et indépendants des paramètres SMTP du serveur UserLock*) :

For additional information, please contact IS Decisions at one of the following:



Le rapport est maintenant planifié. Il ne reste plus qu'à patienter jusqu'à la prochaine exécution de la tâche pour obtenir automatiquement ce rapport dans votre boîte email.

For additional information, please contact IS Decisions at one of the following:

2.3. Nouveau mode pour le rapport Statistiques des sessions

Dans les versions précédentes de UserLock, le rapport *Statistiques des sessions* permettait d'afficher les statistiques en fonction des utilisateurs. Il est maintenant possible de générer aussi les statistiques en fonction des machines.

The screenshot shows the UserLock interface with the 'Statistiques des sessions' report open. The report is configured to view data by machine. The table below shows the session statistics for various machines.

Machine	Domaine	Nombre de sessions	Temps total en session	Temps moyen par session	Temps moyen par jour ouvrable	Temps moyen p semaine
Server3	MyDomain	7	00:25:29	00:03:38	00:02:50	00:14:57
Server4	MyDomain	2	184:10:51	92:05:25	20:34:55	102:50:50
Server5	MyDomain	10	03:03:11	00:18:19	00:20:28	01:42:28
Workstation1	MyDomain	8	54:34:14	06:49:16	06:05:53	30:29:04
Workstation17	MyDomain	1	00:03:36	00:03:36	00:00:24	00:00:24
Workstation2	MyDomain	7	44:06:24	06:18:03	04:55:43	24:36:03
Workstation3	MyDomain	7	63:14:35	09:02:05	07:04:02	35:20:02
Workstation4	MyDomain	9	62:26:29	06:56:16	06:58:39	34:53:03
Workstation5	MyDomain	3	218:21:16	72:47:05	24:24:03	122:00:03
Workstation6	MyDomain	6	57:16:44	09:32:47	06:24:03	32:00:03
Workstation7	MyDomain	6	165:04:17	27:30:42	18:26:47	92:11:03
Workstation8	MyDomain	7	49:38:41	07:05:31	05:32:51	27:44:03
Workstation9	MyDomain	5	40:20:15	08:04:03	04:30:27	22:32:03

For additional information, please contact IS Decisions at one of the following:

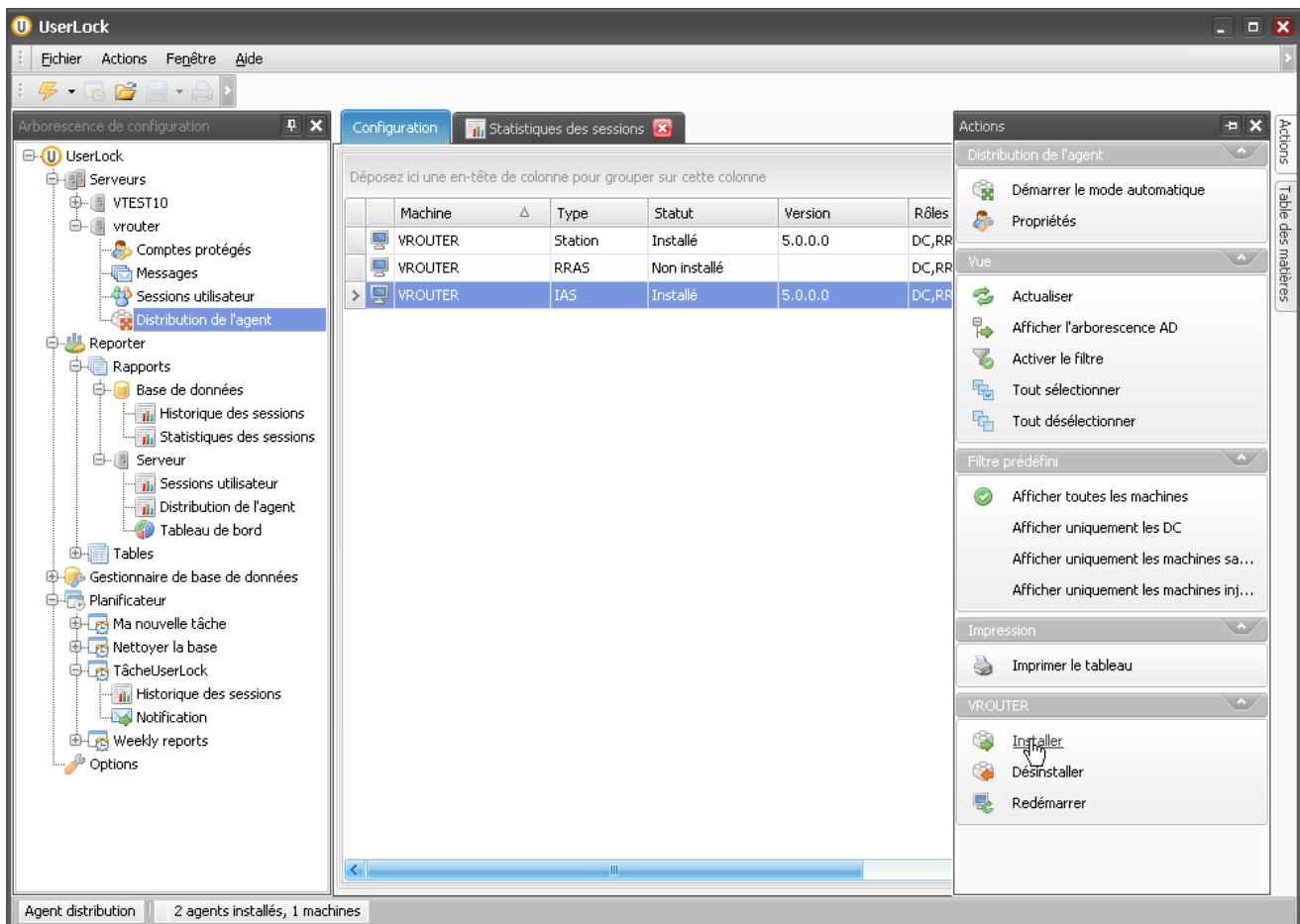
3. Sessions RAS

UserLock 5 peut protéger les sessions RAS gérées par des serveurs RRAS Microsoft (Service de Routage et Accès Distant) ou par tout routeur matériel configuré pour authentifier les utilisateurs à l'aide du protocole RADIUS sur un serveur IAS Microsoft (Service d'Authentification Internet)

Une ligne supplémentaire apparaîtra pour chaque serveur RRAS et chaque serveur IAS dans la section *Distribution de l'agent* de la console UserLock. Cliquer sur *Installer* après avoir sélectionné la ligne correspondante pour déployer l'agent. Après avoir installé l'agent, il sera nécessaire de redémarrer le service RRAS et/ou le service IAS. Si les deux services sont présents sur le serveur, il est nécessaire d'arrêter les deux services ; une fois que les deux services se retrouvent dans l'état arrêté en même temps, il est possible de les redémarrer. Sur Windows 2008 server, il sera nécessaire de redémarrer le serveur.

Une fois l'agent actif, les sessions RAS sont affichées dans la console UserLock et dissociées à l'aide d'une icône différente (Cf. Capture d'écran du filtre rapide).

Il est possible de filtrer la vue *Sessions Utilisateur* pour n'afficher que les sessions RAS (Cf. Capture d'écran du filtre rapide).



The screenshot shows the UserLock console interface. On the left is a configuration tree with 'Distribution de l'agent' selected. The main area displays a table of machines:

Machine	Type	Statut	Version	Rôles
VROUTER	Station	Installé	5.0.0.0	DC,RR
VROUTER	RRAS	Non installé		DC,RR
VROUTER	IAS	Installé	5.0.0.0	DC,RR

On the right, the 'Actions' panel is open, showing options for 'Distribution de l'agent' (Démarrer le mode automatique, Propriétés), 'Vue' (Actualiser, Afficher l'arborescence AD, Activer le filtre, Tout sélectionner, Tout désélectionner), 'Filtre prédéfini' (Afficher toutes les machines, Afficher uniquement les DC, etc.), 'Impression' (Imprimer le tableau), and 'VROUTER' (Installer, Désinstaller, Redémarrer).

For additional information, please contact IS Decisions at one of the following:

3.1. Sessions VPN avec un serveur RRAS

Il existe une limitation technologique lorsque UserLock protège les sessions VPN gérées à l'aide du service RRAS : l'adresse IP du client n'est pas fournie. Il n'est donc pas possible dans ce cas de mettre en place des restrictions d'adresses IP ou de tranches d'adresses IP

Pour contourner cette limitation, Il est possible de lier le service RRAS avec le service IAS en utilisant le protocole RADIUS (comme dans le cas d'un routeur matériel), et de déployer l'agent IAS au lieu de l'agent RRAS.

3.2. Sessions Radius avec IAS

Il n'y pas pour l'instant de Liste de compatibilité matériel pour les routeurs VPN ou les points d'accès Wifi fonctionnant correctement avec UserLock 5.

- Sessions VPN avec un routeur matériel

Les routeurs matériels doivent être configurés pour utiliser une **authentification RADIUS et la technologie RADIUS Accounting** (Gestion de comptes RADIUS) sur un serveur IAS.

Le protocole RADIUS autorisant le client RADIUS (serveur VPN) n'a pas de champ standard pour communiquer le nom de la machine cliente. Il ne sera donc pas possible de mettre en place des restrictions par nom de machine.

L'adresse IP du client VPN pourra être disponible sur certains serveurs VPN matériels, ce qui permettra d'utiliser les restrictions d'adresses IP ou de tranches d'adresses IP. Mais tous les types de matériels ne fournissent pas cette information. Il est donc nécessaire de vérifier au préalable si l'adresse IP du client VPN est bien disponible et affichée dans le rapport *Historique de sessions* avant de mettre en place ces règles de restrictions IP pour les sessions VPN.

- Protéger un point d'accès Wifi avec authentification

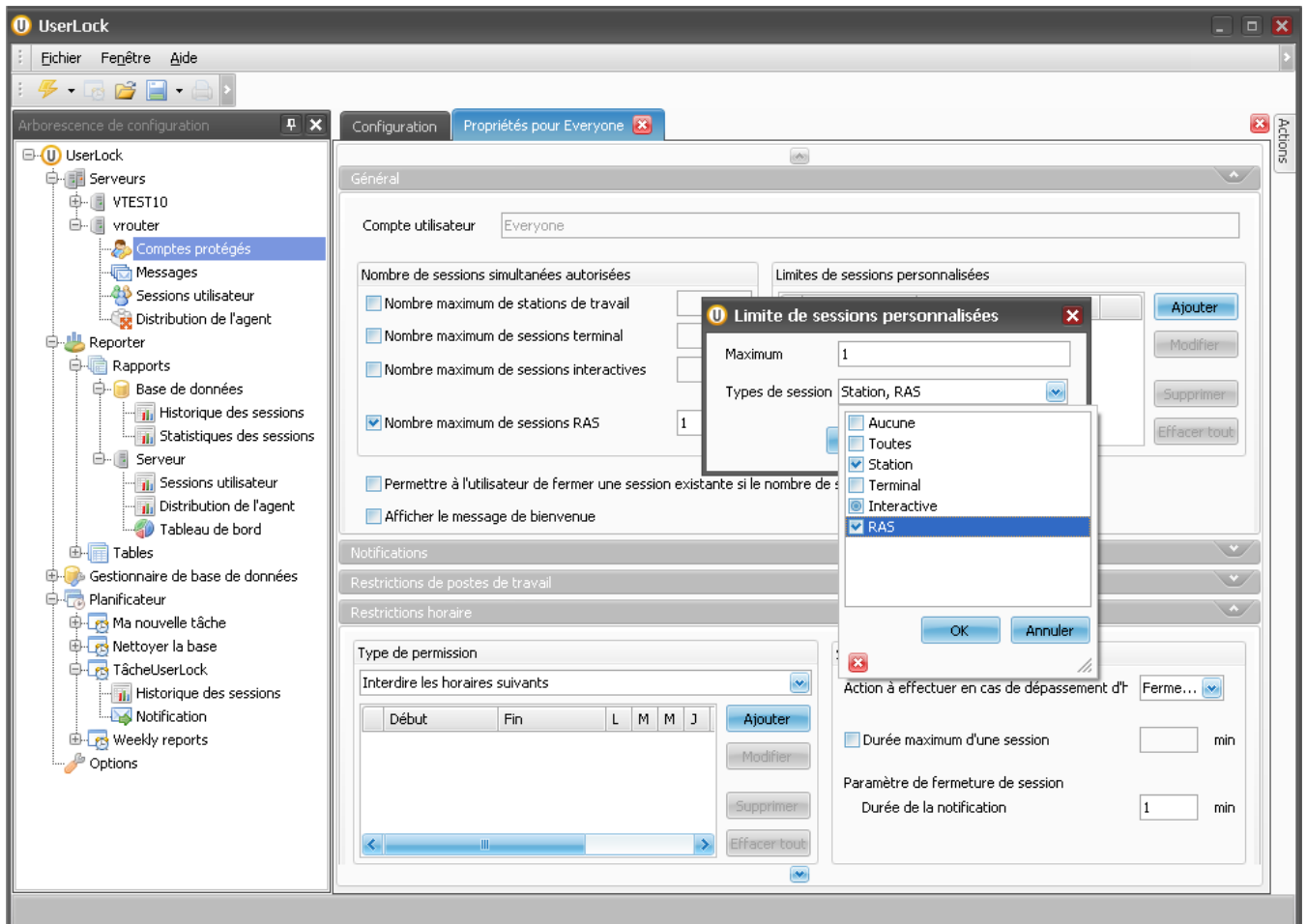
Cette protection est possible si votre point d'accès Wifi gère l'authentification des utilisateurs à l'aide du protocole RADIUS. Cependant, ce type de matériel doit respecter les règles standards qui suivent.

Votre matériel doit pouvoir authentifier vos utilisateurs à l'aide du protocole **RADIUS et de la technologie RADIUS Accounting** (Gestion de compte RADIUS).

Un événement Accounting doit être envoyé au serveur RADIUS lors de chaque de déconnexion de session Wifi de son point d'accès, même lorsque celle-ci est brutale. Certains points d'accès Wifi compatible RADIUS ne respectent pas cette règle standard.

Si le client Wifi est membre du domaine, le compte de machine peut être utilisé pour l'authentification. Dans ce cas, les sessions sous ce type d'authentification machine ne seront pas prises en compte par UserLock.

3.3. Configurer des restrictions pour les sessions RAS



- Limiter le nombre de sessions RAS simultanées

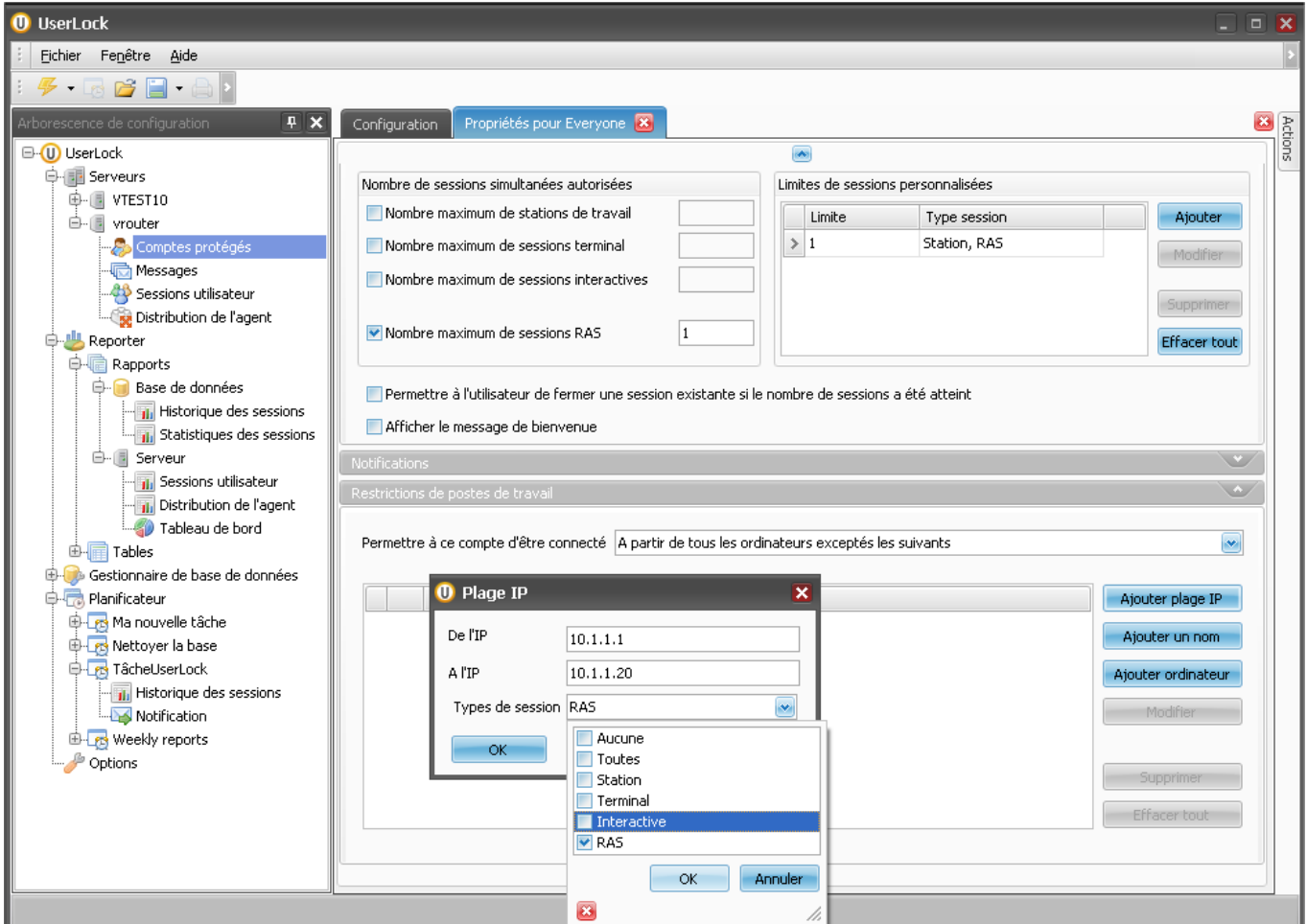
Cette nouvelle limitation est disponible dans les *Propriétés des Comptes protégés* UserLock sous la dénomination *Sessions RAS autorisées*.

- Limitations de session personnalisées

Pour restreindre le nombre de sessions simultanées pour plusieurs types de session, il est possible de créer une *Limitation de session personnalisée*. Par exemple, si une *Limitation de session personnalisée* est configurée à 1 pour les sessions de type Station et RAS, un utilisateur ne pourra pas ouvrir une session RAS s'il a déjà une session ouverte sur une station.

- Restrictions temporelles et restrictions de station

La fonctionnalité de restriction temporelle ou de station permet maintenant de choisir quel type de session sera impacté. Pour appliquer une restriction seulement sur les sessions RAS, il suffit de désélectionner tous les autres types de session.



For additional information, please contact IS Decisions at one of the following: