Présentation

Depuis Qubes 2018, le système d'authentification a évolué pour supporter aussi une authentification de type TOTP, spécifique à chaque serveur Qubes.
Il est ainsi possible d'autoriser des clients ou des partenaires à accéder aux pages d'administration des installations Qubes qui les concernent.
Le protocole TOPT étant basé sur l'heure courante, l'utilisation de ce moyen d'authentification impose que le serveur concerné et l'application qui génère les OTP soient à l'heure.

Procédure client pour activer l'administration OTP

Pour chaque serveur concerné, l'administrateur doit envoyer un mail au support Creative IT avec :

- le nom du serveur
- la liste des identifiants autorisés à administrer les OTP de ce serveur
    - Il s'agit d'identifiants entre 3 et 10 caractères, choisis librement par le client
- la clé serveur générée par ServerKey.bat :
    - Télécharger le zip ServerKey.zip
    - Le dézipper et lancer ServerKey.bat
    - Copier la clé indiquée

Pour chaque serveur concerné, le support Creative IT renverra alors :

- un fichier « otp.key »
- une liste d'URL de paramétrage des secrets utilisateurs (un par identifiant administrateur)

Le fichier « otp.key » devra être copié dans le dossier « Creative IT » du serveur concerné.
Pour que les exécutables Creative IT utilisent ce fichier, ils doivent être redémarrés.
Le plus simple est donc de redémarrer le service QubesGuardian une fois que le fichier est en place pour que les services Qubes l'utilisent.

Chaque administrateur a 24H pour accéder à son URL, qui lui affichera un QRCode permettant de paramétrer son application de gestion des OTP.

Pour générer des OTP, les utilisateurs peuvent utiliser l'application de leur choix, pourvu qu'elle soit compatible avec le protocole T-OTP.
Nous recommandons d'utiliser une application connue de gestion des OTP sur téléphone (ex : Google Authenticator, Free OTP, Authy, …), dans laquelle il suffira de photographier le QRCode pour paramétrer une nouvelle authentification.

Pour accéder à un utilitaire d'administration protégé par AdminSec, il suffit de saisir son identifiant et le code OTP généré par l'application en utilisant l'authentification associé au serveur concerné (NB : dans ce

cas, le challenge ne sert à rien).

Procédure pour gérer des administrateurs locaux

Un administrateur qui a un code OTP valide (ou un mastercode) peut gérer manuellement une liste d'identifiants autorisés pour l'administration d'un service donné.
Il faut se connecter sur la page http d'administration du service (généralement **/admin.sys**) puis cliquer sur *Configure OTP for admin pages*.
On peut alors ajouter/modifier/supprimer un identifiant autorisé à se connecter aux pages d'administration de ce service.

Quand on ajoute un identifiant, si on veut utiliser le même secret pour plusieurs services, on peut le préciser.
Sinon, si on ne précise pas de secret, le service en génère un automatiquement.

Il faut valider avec le service support le niveau de sécurité que vous souhaité :

- sécurité simple : un même utilisateur aura une seule authentification pour tous les serveurs sur lesquels il est déclaré
- sécurité normale : un même utilisateur aura une authentification différente pour les serveurs de PROD et de TEST
- sécurité renforcée : un même utilisateur aura des authentifications différentes pour chaque serveur

NB : il faut renforcer la sécurité si ne veut pas qu'un vol de secret d'un utilisateur sur un serveur ne compromette les autres serveurs.