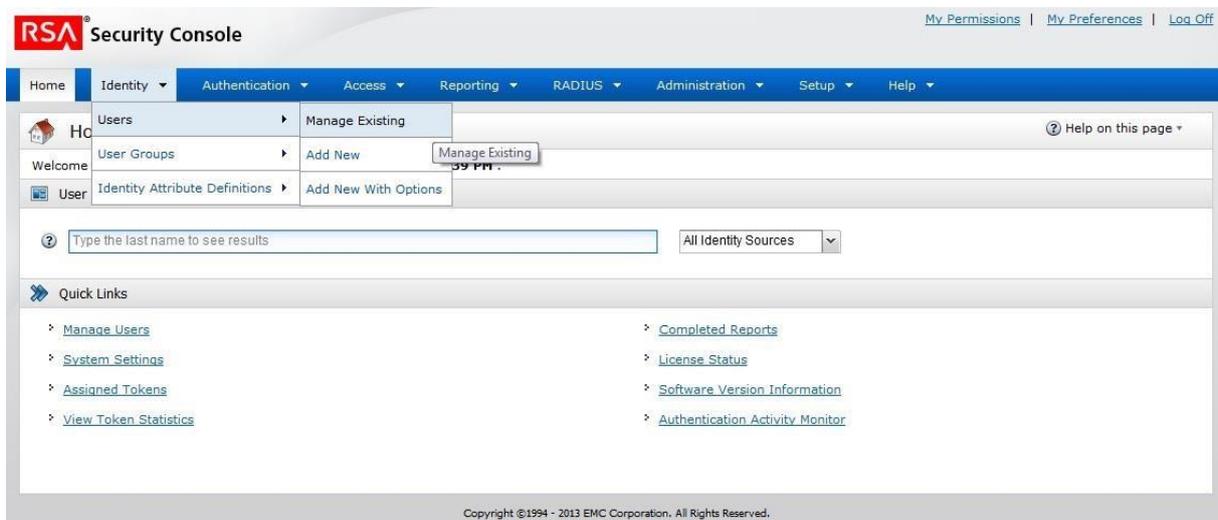




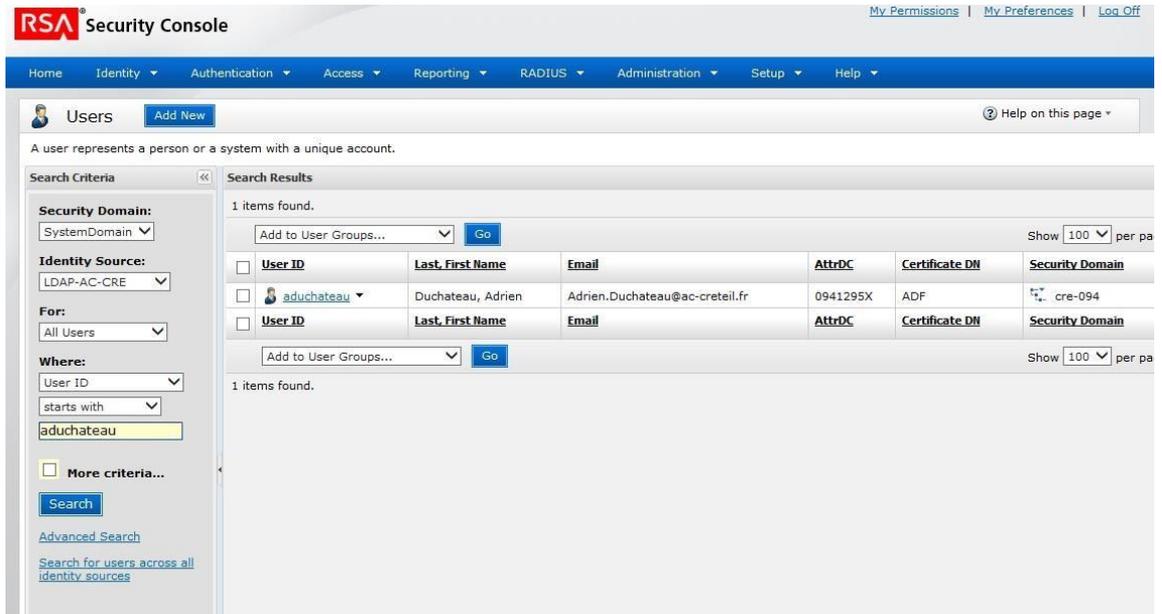
Les clés OTP sont utilisées au sein de l'Académie de Créteil pour sécuriser l'accès à certaines applications. La sécurité est assurée par le fait que la clef OTP donne un code qui change toutes les minutes de plus la clé possède une date de validité (durée de vie de la pile). La console de gestion contient la date de validité de la clef, on peut donc savoir et prévoir les remplacements avant expiration. Pour info quand on arrive à la date d'expiration de la clef les chiffres disparaissent

PARTIE 1 :

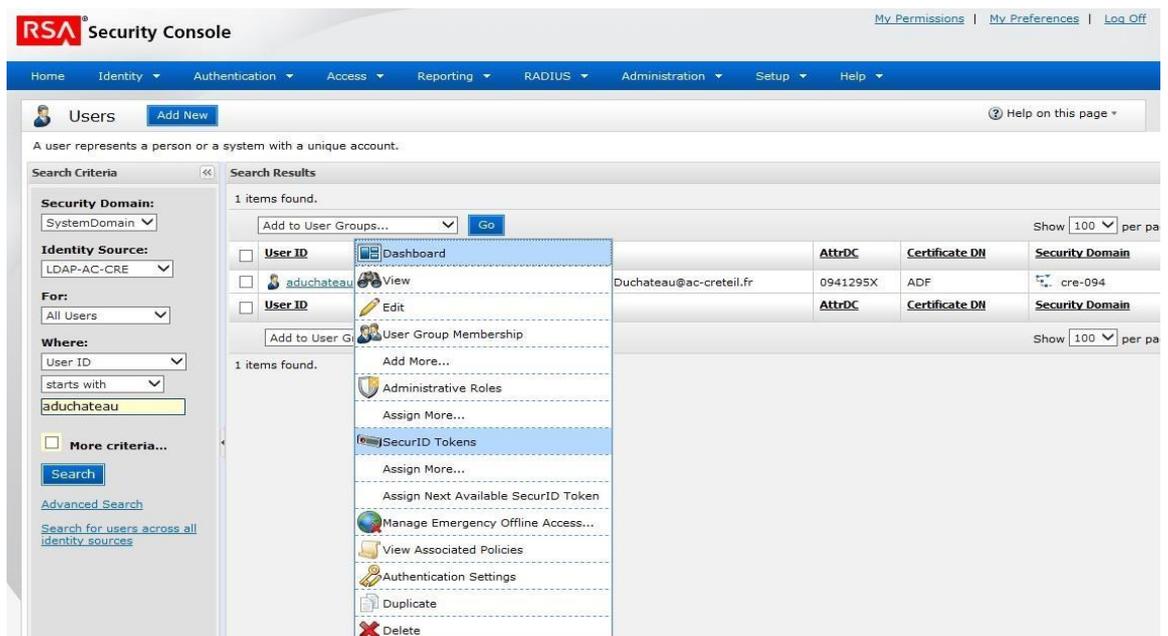
1) Pour attribuer une clé à un utilisateur, il faut se rendre dans la console RSA et dans le menu suivant.



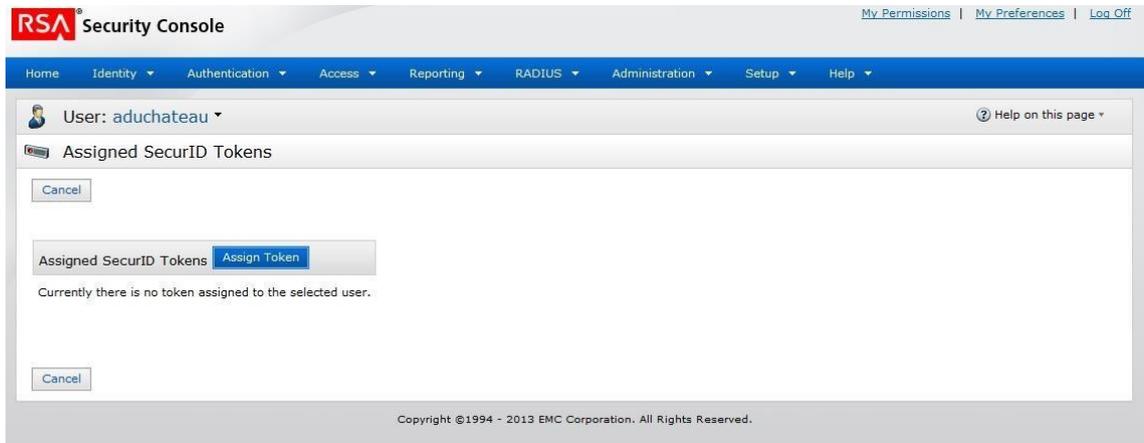
- 2) Il est nécessaire de remplir le nom d'utilisateur qui est composé de la première lettre du prénom suivi du nom de famille et éventuellement d'un chiffre en l'occurrence 'Adrien Duchateau' obtient comme identifiant 'aduchateau'.



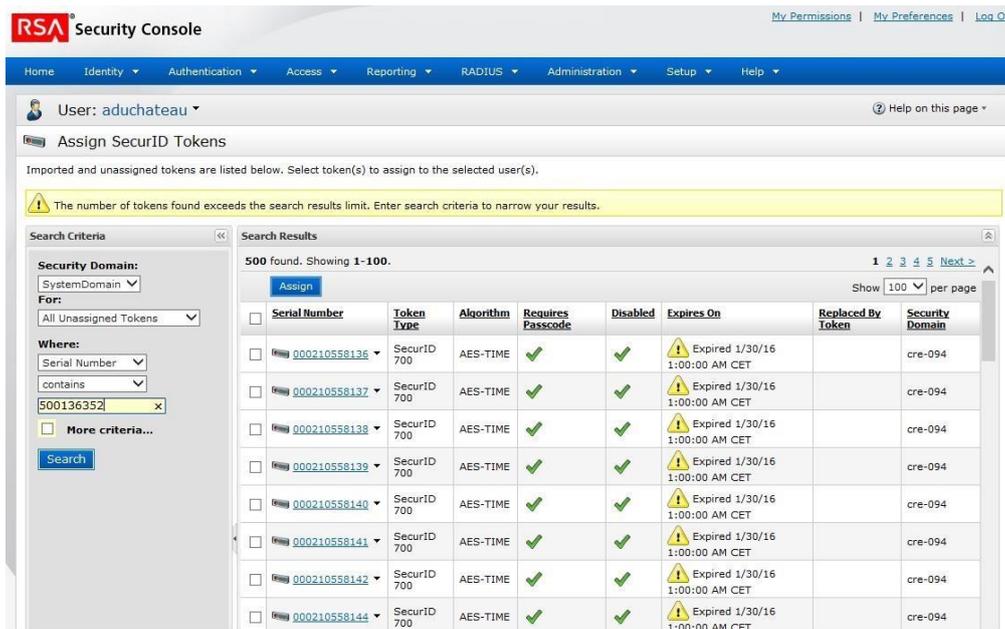
- 3) Effectuez un clic droit sur le nom d'utilisateur et sélectionnez 'SecurID Tokens' pour rattacher une clé OTP à un compte.



4) Cliquez sur le bouton **'Assign Token'** pour effectuer la suite.



5) Recherchez la clé OTP que vous souhaitez attribuer.



6) Sélectionnez le bouton **‘Assign’** pour affilier le numéro de clé OTP au compte précédemment indiqué.

Imported and unassigned tokens are listed below. Select token(s) to assign to the selected user(s).

Search Criteria

Security Domain: SystemDomain

For: All Unassigned Tokens

Where: Serial Number contains 500136352

Search Results

1 items found.

Serial Number	Token Type	Algorithm	Requires Passcode	Disabled	Expires On	Replaced By Token	Security Domain
000500136352	SecurID 700	AES-TIME	✓	✓	9/30/21 2:00:00 AM CEST		SystemDomain

7) Quand vous voyez l’encadré vert ci-dessus, cela signifie que la clé à bien était assignée au compte souhaité.

Assigned 1 token(s) to 1 user(s). For software tokens, click the token and select Distribute from the context menu.

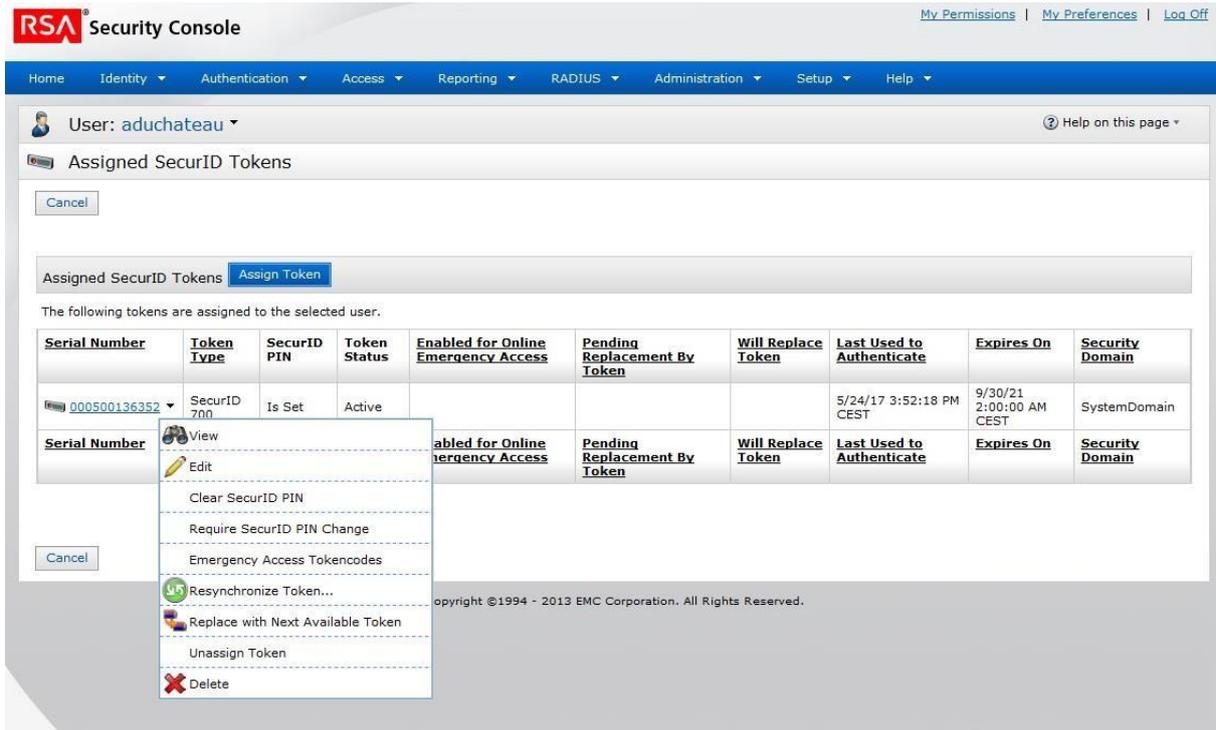
Assigned SecurID Tokens

The following tokens are assigned to the selected user.

Serial Number	Token Type	SecurID PIN	Token Status	Enabled for Online Emergency Access	Pending Replacement By Token	Will Replace Token	Last Used to Authenticate	Expires On	Security Domain
000500136352	SecurID 700	Not Set	Active					9/30/21 2:00:00 AM CEST	SystemDomain

8) Lorsque vous avez effectué les étapes précédentes, il est possible d'effectuer certaines actions sur les clés comme :

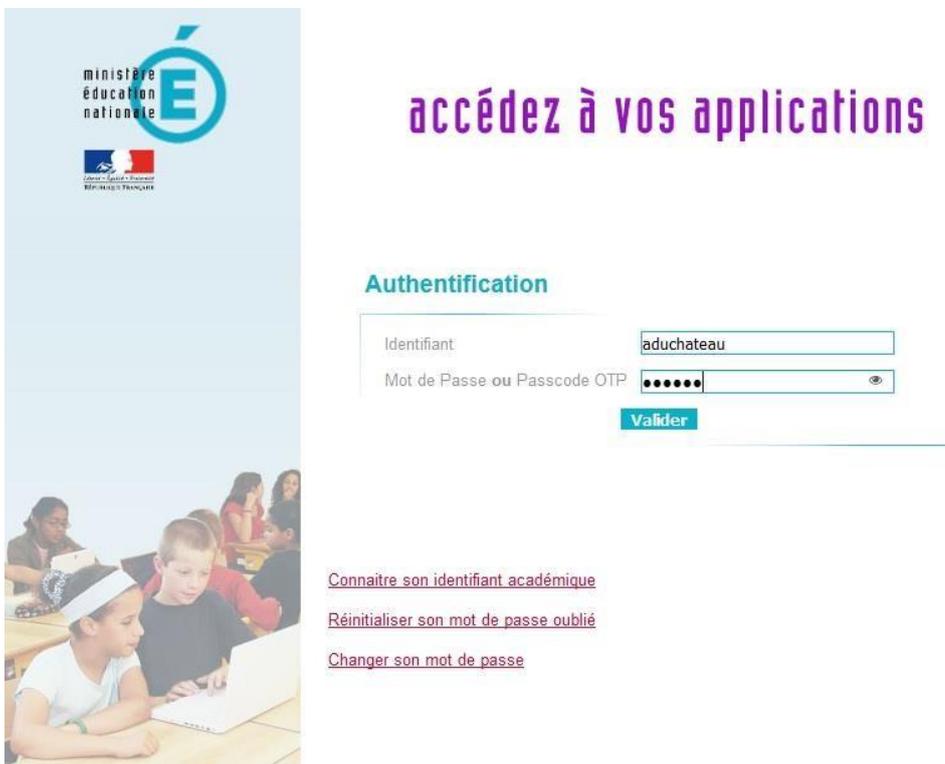
- de retirer le code PIN
- désallouer la clé du compte (pour la réattribuer à quelqu'un d'autre)



PARTIE 2 :

Après avoir effectué la partie 1, vous pouvez maintenant définir votre code PIN, voici la marche à suivre pour cela.

- 1) Rendez-vous sur le site '<https://externet.ac-creteil.fr>' et indiquez votre identifiant et votre mot de passe (celui que vous utilisez sur l'intranet). Vous pouvez '**Valider**'.



ministère
éducation
nationale

accédez à vos applications

Authentification

Identifiant

Mot de Passe ou Passcode OTP

[Connaitre son identifiant académique](#)

[Réinitialiser son mot de passe oublié](#)

[Changer son mot de passe](#)

- 2) Vous êtes maintenant à l'étape de saisie du code PIN, vous devez saisir un code PIN en 4 et 6 caractères de lettres, des chiffres ou un mélange des deux. Il ne peut pas être '0000' ou certaines combinaisons simples. Le code PIN doit aussi obligatoirement être différent du mot de passe habituel du compte. En cas de réinitialisation de code PIN on ne peut pas utiliser les 3 derniers codes PIN utilisés.



accédez à vos applications

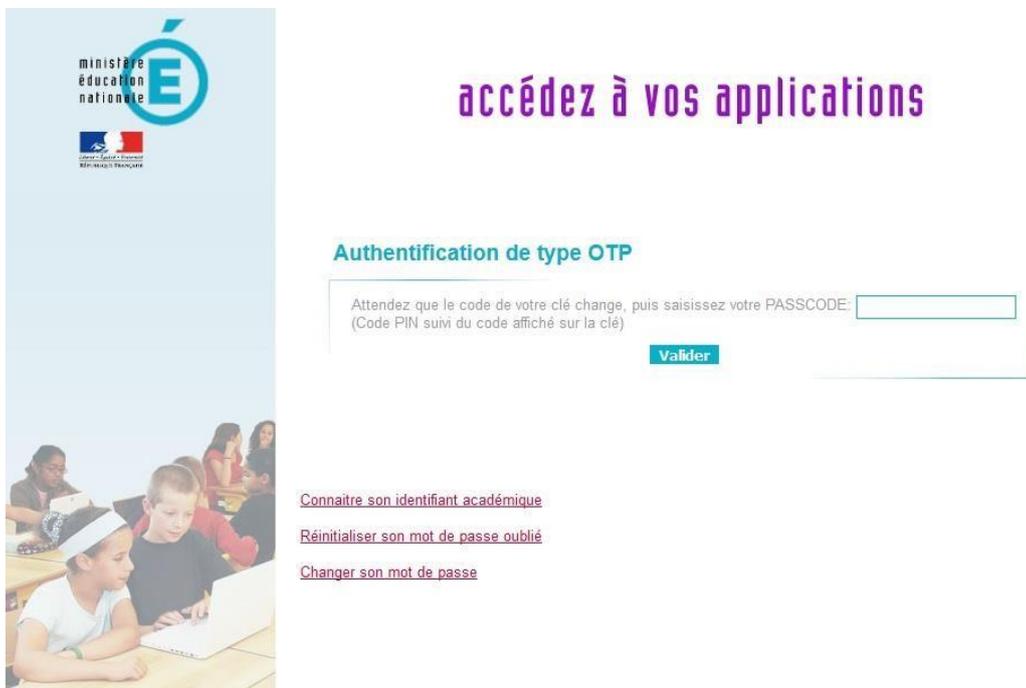
Authentification de type OTP

Saisissez votre nouveau code PIN, contenant de 4 à 6 caractères:

Confirmez votre nouveau code PIN

Valider

3) Vous devez maintenant indiquer votre code PIN saisi auparavant suivi du code que votre clé affiche.

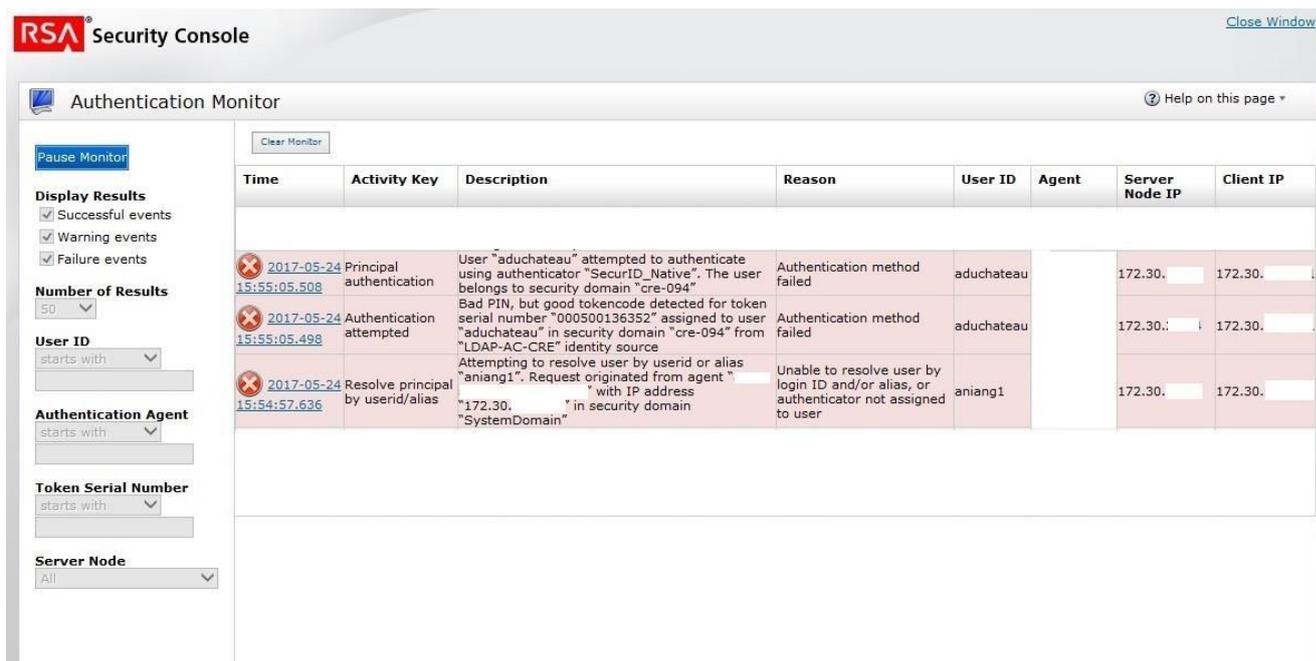


4) Vous êtes maintenant connecté sur le portail ARENA avec votre clé OTP.



LA CONSOLE RSA :

Nous possédons une console pour avoir un suivi de toutes les actions OTP qui sont faites. (Erreur de PIN, Clé OTP pas rattachée au compte etc...)



The screenshot shows the RSA Security Console Authentication Monitor interface. On the left, there are filters for 'Display Results' (Successful, Warning, Failure events), 'Number of Results' (50), 'User ID', 'Authentication Agent', 'Token Serial Number', and 'Server Node'. The main area displays a table of events:

Time	Activity Key	Description	Reason	User ID	Agent	Server Node IP	Client IP
2017-05-24 15:55:05.508	Principal authentication	User "aduchateau" attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "cre-094"	Authentication method failed	aduchateau		172.30. . .	172.30. . .
2017-05-24 15:55:05.498	Authentication attempted	Bad PIN, but good tokencode detected for token serial number "000500136352" assigned to user "aduchateau" in security domain "cre-094" from "LDAP-AC-CRE" identity source	Authentication method failed	aduchateau		172.30. . .	172.30. . .
2017-05-24 15:54:57.636	Resolve principal by userid/alias	Attempting to resolve user by userid or alias "aniang1". Request originated from agent "172.30. . . with IP address "172.30. . . in security domain "SystemDomain"	Unable to resolve user by login ID and/or alias, or authenticator not assigned to user	aniang1		172.30. . .	172.30. . .

Nous pouvons observer ci-dessus que l'utilisateur 'aduchateau' saisi un mauvais un code PIN avec la bonne clé OTP qui est rattaché à son compte.

Un trop grand nombre de mauvaises connexions dans un laps de temps défini provoque le blocage de clé pour un certain nombre d'heures. Quand le nombre d'essai est trop important et en trop peu de temps cela peut aller jusqu'au verrouillage du compte utilisateur pour l'accès OTP (une action manuelle du service d'assistance est alors nécessaire pour rendre cet accès de nouveau fonctionnel à l'utilisateur.)

Les chiffres présents sur la clé OTP ne sont utilisables qu'une seule fois. Il faut donc théoriquement attendre 1 minute entre chaque essai de connexion.