

NX2009955 / 72868_B 21/07/2020 1 (34)



Coffret ENSTO E-RTU 2020

Configuration Système

Tel. +33 (0)4 74 65 61 61 Fax +33 (0)4 74 62 96 57





Table	des matières	
1 0	NGLET "SYSTÈME"	4
1.1	CONFIGURATION DE L'HEURE ET DE LA DATE	4
1.2	MISE À JOUR LOGICIEL	5
1.3	FICHIER DE CONFIGURATION	5
1.4	REDÉMARRAGE	6
1.5	RESTAURATION	6
1.6	PARAMÈTRES DE SESSION	7
2 0	NGLET "MOT DE PASSE"	8
3 O	NGLET "UTILISATEURS"	9
4 OI	NGLET "AJOUTER UTILISATEUR"	10
5 OI	NGLET "FIREWALL"	11
5.1	STATUT DU FIREWALL	11
5.2	CONFIGURATION PROTECTION DOS (DENIAL OF SERVICE)	12
5.3	CONFIGURATION DES RÈGLES DU FIREWALL	13
5.4	CONFIGURATION DES PING	14
6 OI	NGLET "NTP"	14
6.1	STATUT DU CLIENT NTP	15
6.2	CONFIGURATION DU CLIENT NTP	15
7 0	NGLET "OPENVPN"	16
7.1	STATUT DU SERVEUR OPENVPN	16
7.2	CONFIGURATION DU SERVEUR OPENVPN	16
8 OI	NGLET "IPSEC"	18
8.1	STATUT DU TUNNEL IPSEC	18
8.2	CONFIGURATION DU TUNNEL IPSEC	18
9 O	NGLET "DHCP"	21
9.1	STATUT DU SERVEUR DHCP	21
9.2	CONFIGURATION DU SERVEUR DHCP	21
9.3	ADRESSES IP ALLOUÉES	22
10	ONGLET "SSH"	23
10.1	STATUT DU SERVEUR SSH	23
10.2	CONFIGURATION DU SERVEUR SSH	23
11	ONGLET "SERVEUR WEB"	

4PR-F8-H

Better life. With electricity.



	3 (34)	
11.1	STATUT DU SERVEUR WEB	24
11.2	CONFIGURATION DU SERVEUR WEB	24
12 ON	GLET "CLÉS DE CRYPTAGE ET CERTIFICATS"	26
12.1	CRL	26
12.2	Serveur WEB	27
12.3	OpenVPN	29
12.4	IPSec	30





NX2009955 / 72868_B 21/07/2020 4 (34)

1 ONGLET "SYSTÈME"



Figure 1 : Onglet "Système"

1.1 CONFIGURATION DE L'HEURE ET DE LA DATE

Pour configurer l'heure et la date du coffret, aller sur la page "Système" onglet "Système" (Figure 1) :

• Cliquer sur la roue dentée (1) pour ouvrir la fenêtre de dialogue suivante :

Date / Heure	2020-7-16 / 9:1:20 ද්ටු	
	Mettre à l'heure PC	
	JJ / MM / AAAA 16/07/2020	
	HH : MM 09 : 01	Q
	Enregistrer et prendre en compte	
Version	ITI2020 PR236 V1.0	-

Figure 2 : Fenêtre de dialogue de configuration de l'heure et de la date

Pour mettre le coffret à l'heure et à la date de votre PC, dans la fenêtre de dialogue (Figure 2) :

- Cliquer sur la case "Mettre à l'heure PC"
- Cliquer sur "Enregistrer et prendre en compte"

Pour mettre à l'heure et à la date manuellement, dans la fenêtre de dialogue (Figure 2) :

• Remplir les champs "JJ / MM / AAAA" et "HH : MM" comme souhaités





• Cliquer sur "Enregistrer et prendre en compte".

Note : Lorsque vous prenez en compte la modification de l'heure, il se peut que vous soyez déconnecté.

1.2 MISE À JOUR LOGICIEL

- Pour mettre à jour le logiciel du coffret, aller sur la page "Système" onglet "Système" (Figure 1) :
- Cliquer sur "Choisir un fichier" (2) dans la zone "Mise à jour"
- En fonction du navigateur internet, une boite de dialogue s'ouvre
- Sélectionner le fichier ZIP correspondant au logiciel
- Cliquer sur "Mettre à jour" (3)
- Attendre la fin du transfert
- La fenêtre de dialogue suivante s'ouvre :

(
	Votre version acutelle de logiciel est ITI2020 PR236 V1.0
'	Oui Annuler
l	

Figure 3 : Fenêtre de dialogue de mise à jour logiciel

- Cliquer sur "Oui" pour confirmer la mise à jour ou sur "Annuler" pour l'annuler
- Attendre la fin de la mise à jour

Note : La mise à jour est terminée lorsque la page de connexion au serveur web s'affiche Note : Il n'est pas possible de revenir sur une ancienne version du logiciel

1.3 FICHIER DE CONFIGURATION

Pour télécharger le fichier de configuration du coffret, aller sur la page "Système" onglet "Système" (Figure 1) :

- Cliquer sur "Télécharger" (4) dans la zone "Configuration"
- En fonction du navigateur internet, le fichier de configuration ZIP se télécharge

Pour <u>envoyer le fichier de configuration</u> vers le coffret, aller sur la page "Système" onglet "Système" (Figure 1)

- Cliquer sur "Choisir un fichier" (5) dans la zone "Configuration"
- En fonction du navigateur internet, une boite de dialogue s'ouvre
- Sélectionner le fichier ZIP correspondant à la configuration
- Cliquer sur "Envoyer et reboot" (6)
- La fenêtre de dialogue suivante s'ouvre :





Mettre à jour :	
La configuration des paramètres hors système	
✓ Les paramètres système	
Les textes	
Valider Annuler	

Figure 4 : Fenêtre de dialogue d'envoi du fichier de configuration

- En fonction de ce que vous souhaitez configurer, sélectionner :
 - "La configuration des paramètres hors système" pour configurer à partir du fichier tous les paramètres hors ceux qui sont sur la page "Système", exemple : paramètres de communication, paramètres des automatismes, ...
 - "Les paramètres systèmes" pour configurer à partir du fichier tous les paramètres qui sont sur la page "Système", exemple : paramètres des VPN, Firewall, ...
 - "Les textes" pour configurer tous les textes des afficheurs
- Cliquer sur "Valider" pour prendre en compte la configuration ou sur "Annuler" pour annuler
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche

1.4 REDÉMARRAGE

Pour <u>redémarrer</u> le coffret, aller sur la page "Système" onglet "Système" (Figure 1) :

- Cliquer sur "Reboot" (7) dans la zone "Reboot"
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche

1.5 **RESTAURATION**

Lorsque des modifications de paramètre (hors paramètres de la page "Système") sont faites mais qu'il n'y a pas eu de cliquer sur "Prendre en compte les modifications" il est possible de revenir en arrière et d'annuler les modifications.

Il est également possible de restaurer les paramètres du coffret comme à sa sortie d'usine.

Pour <u>annuler les modifications en cours</u>, aller sur la page "Système" onglet "Système" (Figure 1) :

- Cliquer sur "Restaurer la précédente configuration (hors paramètres systèmes)" (8) dans la zone "Restauration"
- La fenêtre de dialogue suivante s'ouvre :

Etes vous sur de vouloir restaurer le systeme avec la precedente configuration (hors parametres systemes)?
Oui Annuler
Figure 5 : Fenêtre de dialogue pour l'annulation des modifications des paramètres







- Cliquer sur "Oui" pour valider l'annulation des modifications des paramètres ou sur "Annuler" pour annuler
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche

Pour <u>restaurer les paramètres usines</u> du coffret **(uniquement possible par un utilisateur avec les droits "Administrator")**, aller sur la page "Système" onglet "Système" (Figure 1) :

- Cliquer sur "Restaurer les paramètres usine" (9) dans la zone "Restauration"
- La fenêtre de dialogue suivante s'ouvre :

Etes yous sur de vouloir restaurer le système avec les paramètres usine ?
Oui Annuler

Figure 6 : Fenêtre de dialogue de restauration des paramètres usines

- Cliquer sur "Oui" pour valider la restauration des paramètres usine ou sur "Annuler" pour annuler
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche

1.6 PARAMÈTRES DE SESSION

Pour <u>configurer les paramètres de session</u> des pages web **(uniquement possible par un utilisateur avec les droits "Administrator")**, aller sur la page "Système" onglet "Système" (Figure 1) :

- Remplir le champ "Timeout de session (s)" (10) pour définir le temps en seconde de déconnexion lorsque l'utilisateur ne fait pas d'action sur les pages web
- Remplir le champ "Nombre maximal de tentative de connexion" (11) pour définir le nombre maximal de tentative de connexion avant que l'utilisateur soit bloqué à cause d'un mauvais mot de passe renseigné
- Remplir le champ "Temps de blocage lors d'un trop grand nombre de tentative de connexion (s)" (12) pour définir le temps de blocage lorsqu'un utilisateur a rentré trop de mauvaise fois le mot de passe
- Cliquer sur "Enregistrer et prendre en compte les modifications" dans la zone "Paramètres" pour prendre en compte les modifications





NX2009955 / 72868_B 21/07/2020 8 (34)



2 ONGLET "MOT DE PASSE"

Mot de Passe

Changement du mot de passe Administrateur

Mot de passe actuel :		Ô
Nouveau mot de passe :		O
Confirmation du mot de passe :		O
	Valider	
	Annuler	

Figure 7 : Onglet "Mot de passe"

Pour <u>changer le mot de passe de l'utilisateur web connecté</u>, aller sur la page "Système" onglet "Mot de passe" (Figure 7) :

- Renseigner le mot de passe actuel dans le champ "Mot de passe actuel"
- Renseigner le nouveau mot de passe dans le champ "Nouveau mot de passe"
- Renseigner à nouveau le nouveau mot de passe dans le champ "Confirmation du mot de passe"
- Cliquer sur "Valider" pour valider le changement de mot de passe ou sur "Annuler" pour annuler

Note : Le mot de passe doit contenir au minimum 8 caractères dont un chiffre, une majuscule, une minuscule et un caractère spécial





NX2009955 / 72868_B 21/07/2020 9 (34)



3 ONGLET "UTILISATEURS"

Pataur						
vetore		Utilisateurs				
do pacco	Coroits pour l'utilisateur Maintenance :					
icatoure	Administrator					
r utilisateur	See All Pages					
irewall	Pages autorisées à voir (n'est pas pris en comp	te si 'See All Pages' est sélectionné) :				
NTP	Retards et Alarmes	Automatismes				
enVPN	✓ Télémesures	Communication et Protocoles				
PSec	Détection de Défaut	Enregistrement Mesures Cycliques				
OHCP	Paramètres Administrateur	✓ Libellé E/S				
SSH	Maintenance	Mot de Passe				
eur WEB	Système	✓ TSS Regroupement Défaut				
Cryptage et	DNP3 IP	VDNP3 Série				
rtificats	Z IEC101	IEC104				
	Analyseur IP	MODBUS RTU				
	MODBUS TCP					
	Enregistrer et prendre en compte					
	Droits pour l'utilisateur Visualisation :					
	Administrator					
	See All Pages					
	Pages autorisées à voir (n'est pas pris en compte si 'See All Pages' est sélectionné)					

Figure 8 : Onglet "Utilisateurs"

Cet onglet permet de configurer les droits des utilisateurs web et de changer leur mot de passe.

Pour <u>configurer les droits d'un utilisateur web</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "Utilisateurs" (Figure 8) :

- Cliquer sur la case "Administrator" pour que l'utilisateur ait les droits d'un administrateur
- Cliquer sur la case "See All pages" pour que l'utilisateur puisse voir toutes les pages web
- Sélectionner les pages que l'utilisateur peut voir dans la zone "Pages autorisées à voir"
- Cliquer sur "Enregistrer et prendre en compte" pour prendre en compte les modifications

Note : La configuration des droits se fait utilisateur par utilisateur

Pour <u>changer le mot de passe d'un utilisateur web</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "Utilisateurs" (Figure 8) :

- Cliquer sur la clé à côté du nom de l'utilisateur (1)
- En fonction du navigateur internet, une boite de dialogue s'ouvre
- Renseigner le nouveau mot de passe
- Cliquer sur "OK" pour valider le changement de mot de passe ou sur "Annuler" pour annuler

Note : Il n'est pas possible de changer le mot de passe d'un utilisateur avec les droits "Administrator" de cette manière

Note : Le mot de passe doit contenir au minimum 8 caractères dont un chiffre, une majuscule, une minuscule et un caractère spécial





4

NX2009955 / 72868 B 21/07/2020 10 (34)





Figure 9 : Onglet "Ajouter utilisateur"

Pour ajouter un utilisateur web (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "Ajouter utilisateur" (Figure 9) :

- Remplir le champ "Nom de l'utilisateur" (1) avec un nouveau nom d'utilisateur •
- Remplir le champ "Mot de passe" (2) avec le mot de passe du nouvel utilisateur ٠
- Cliquer sur la case "Demander de choisir un nouveau mot de passe à la première connexion" pour que • lorsque l'utilisateur se connectera la première fois qu'il soit invité à changer son mot de passe
- Cliquer sur "Ajouter" pour ajouter le nouvel utilisateur

Note : Le mot de passe n'a pas besoin de respecter la règle des mots de passe suivante : minimum 8 caractères dont un chiffre, une majuscule, une minuscule et un caractère spécial





NX2009955 / 72868_B 21/07/2020 11 (34)



Figure 10 : Onglet "Firewall"

5.1 STATUT DU FIREWALL

Pour <u>afficher le statut du Firewall</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "Firewall" block "Firewall" (Figure 10) :

- Cliquer sur l'icône graphique (1)
- La fenêtre de dialogue du statut du Firewall s'ouvre, exemple :





NX2009955 / 72868_B 21/07/2020

12 (34)

							Statut	du Firewall	•
Chain	INPUT	(policy	DROP 28	82 p	ackets,	121K b	ytes)		
pkts	bytes	target	prot	opt	in	out	source	destination	
54679	1414	ACCEPT	a11		10	any	anywhere	anywhere	
1481	86880		tcp	-	any	any	anywhere	anywhere	tcp dpt:ssh ctstate NEW recent: SET name:
66	3168	DROP	tcp		any	any	anywhere	anywhere	tcp dpt:ssh ctstate NEW recent: UPDATE se
3376	609K	ACCEPT	tcp		eth1	any	anywhere	anywhere	tcp dpt:ssh
0	0	ACCEPT	udp		eth1	any	anywhere	anywhere	udp dpt:bootps
0	0	ACCEPT	tcp		eth1	any	anywhere	anyshere	tcp dpt:www
62757	568	ACCEPT	tcp		eth1	any	anywhere	anywhere	tcp dpt:https
0	8	ACCEPT	udp		eth0	any	anywhere	anywhere	udp dpt:500
0	9	ACCEPT	udp		eth0	any	anywhere	anywhere	udp dpt:4500
0	9	ACCEPT	tcp		eth0	any	anywhere	anywhere	tcp dpt:1194
10	511	ACCEPT	tcp		eth0	any	anywhere	anywhere	tcp dpt:2404
18627	2188K	ACCEPT	tcp		eth0	any	anywhere	anywhere	tcp dpt:ssh
0	0	ACCEPT	tcp		eth1	any	anywhere	anywhere	tcp dpt:19998
0	0	ACCEPT	tcp		eth1	any	anywhere	anywhere	tcp dpt:2404
41	2940	ACCEPT	icmp		any	any	anywhere	anywhere	limit: avg 10/sec burst 30
0	0	DROP	icmp		any	any	anywhere	anywhere	
pkts Chain	bytes OUTPUT	target (polic	prot y DROP 0	opt	in kets, 0	out bytes)	source	destination	
pkts	bytes	target	prot	opt	in	out	source	destination	
54679	14M	ACCEPT	all		any	10	anywhere	anywhere	
4148	2682K	ACCEPT	tcp		any	ethi	anywhere	anywhere	tcp spt:ssh
0	6	ACCEPT	udp		any	eth1	anywhere	anywhere	udp spt:bootps
0	0	ACCEPT	tcp		any	eth1	anywhere	anywhere	tcp spt:www
52754	27M	ACCEPT	tcp	-	any	eth1	anywhere	anywhere	tcp spt:https
0	0	ACCEPT	udp		any	eth0	anywhere	anywhere	udp spt:500
e	Ð	ACCEPT	udp		any	eth0	anywhere	anywhere	udp spt:4500
0	0	ACCEPT	tcp		any	eth0	anywhere	anywhere	tcp spt:1194
13	684	ACCEPT	tcp		any	eth0	anywhere	anywhere	tcp spt:2404
18999	3395K	ACCEPT	tcp		any	eth0	anywhere	anywhere	tcp spt:ssh
Ð	Ð	ACCEPT	tcp		any	eth1	anywhere	anywhere	tcp spt:19998
0	0	ACCEPT	tcp		any	eth1	anywhere	anywhere	tcp spt:2404
17	1020	ACCEPT	icmp		any	any	anywhere	anywhere	
Chain	port-	canning	(0 refe	renc	es)				
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	RETURN	tcp		any	any	anywhere	anywhere	tcp flags:FIN,SYN,RST,ACK/RST limit: avg
	1 63	PLAN IN CO.			1.		Construction of the second second		

Figure 11 : Fenêtre de dialogue du statut du Firewall

5.2 CONFIGURATION PROTECTION DOS (DENIAL OF SERVICE)

Pour <u>configurer la protection DoS</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "Firewall" block "Firewall" (Figure 10) :

- Remplir le champ "Max de connexion simultanée par client" (2) pour définir le nombre maximum de connexion TCP simultanée d'un client
- Remplir le champ "Max de nouvelles connexions d'un client par seconde" (3) pour définir le nombre maximum de nouvelle connexion TCP d'un client par seconde
- Remplir le champ "Burst de connexion d'un client" (4) pour définir le nombre de connexion TCP rapide d'un client
- Cliquer sur "Enregistrer et reboot" (11) pour prendre en en compte les modifications
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche

Note : Il faut activer la protection DoS pour chaque règle du firewall

Note : Attention l'activation de la protection DoS peut ralentir la connexion TCP





NX2009955 / 72868_B 21/07/2020 13 (34)



Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer la règle générale et les règles spécifiques du Firewall

5.3 CONFIGURATION DES RÈGLES DU FIREWALL

Pour <u>configurer la règle générale du Firewall</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "Firewall" block "Firewall" (Figure 10) :

- Choisir la règle générale "Policy" (5) du Firewall : "ACCEPT" → Toutes les connexions IP sont acceptées sauf si une règle spécifique impose autre chose ; "DROP" → Toutes les connexions IP sont rejetées sauf si une règle spécifique impose autre chose
- Cliquer sur "Enregistrer et reboot" (11) pour prendre en en compte les modifications
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer la protection DoS et les règles spécifiques du Firewall

Pour <u>configurer les règles spécifiques du Firewall</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "Firewall" block "Firewall" (Figure 10) :

- Cliquer sur l'icône "+" (6) pour ajouter une nouvelle règle
- Remplir les champs :
 - "Name" pour donner un nom à la règle (sans espace)
 - "Target" pour accepter (ACCEPT) ou rejeter (DROP) la connexion
 - "Protocole" pour spécifier le type de connexion IP (TCP ou UDP)
 - "Source IP" pour accepter ou rejeter l'adresse IP spécifié (en mettant le mot clé "anywhere" cela signifie toutes les adresses IP)
 - "Source MAC" pour accepter ou rejeter l'adresse MAC spécifié (en mettant le mot clé "anywhere" cela signifie toutes les adresses MAC)
 - "Port" pour spécifier le port IP accepté ou rejeté
 - "DoS" pour activer la protection DoS
 - "Interface" pour spécifier l'interface (par défaut, eth0 = Communication ; eth1 = Configuration ; eth2 = Extension)
- Cliquer sur "Enregistrer et reboot" (11) pour prendre en en compte les modifications
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer la protection DoS et la règle générale du Firewall

Pour <u>supprimer une règle spécifique du Firewall</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "Firewall" block "Firewall" (Figure 10) :

- Cliquer sur l'icône "Poubelle" de la règle à supprimer (exemple 7)
- Cliquer sur "Enregistrer et reboot" (11) pour prendre en en compte les modifications
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche





Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer la protection DoS et la règle générale du Firewall

5.4 CONFIGURATION DES PING

Pour <u>autoriser/refuser les PING</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "Firewall" block "Ping" (Figure 10) :

- Sélectionner ou désélectionner la case "Autoriser les ping" (8) pour respectivement autoriser ou refuser les PING
- Cliquer sur "Enregistrer et reboot" (12) pour prendre en en compte les modifications
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer la protection ICMP

Pour configurer la protection ICMP (uniquement possible par un utilisateur avec les droits

"Administrator"), aller sur la page "Système" onglet "Firewall" block "Ping" (Figure 10) :

- Remplir le champ "Max de connexions d'un client par seconde" (2) pour définir le nombre maximum de connexion ICMP d'un client par seconde
- Remplir le champ "Burst de connexion d'un client" (4) pour définir le nombre de connexion ICMP rapide d'un client
- Cliquer sur "Enregistrer et reboot" (12) pour prendre en en compte les modifications
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer l'autorisation ou le refus des PING

6 ONGLET "NTP"

ENSTO		Système		\frown
🐟 Retour	2	NTP		3
Système		Statut : Désactivé		
Mot de passe				
Utilisateurs	10	Activer le client NTP à chaque	démarrage	4
Ajouter utilisateur	Serveurs		P.	Œ
Firewall	Serveur	192 168 100 100		<u>ا</u>
NTP		Enregistrer et reboat		
OpenVPN	(L	errogener atteaen)
IPSec				
DHCP				
SSH				
Serveur WEB				
Clés de Cryptage et Certificats				

Figure 12 : Onglet "NTP"





6.1 STATUT DU CLIENT NTP

Pour <u>visualiser le statut du client NTP</u> (activé ou désactivé) **(uniquement possible par un utilisateur avec les droits "Administrator")**, aller sur la page "Système" onglet "NTP" (Figure 12) :

• Le champ "Statut" (1) indique si le client NTP est activé ou désactivé

6.2 CONFIGURATION DU CLIENT NTP

Pour <u>activer/désactiver le client NTP</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "NTP" (Figure 12) :

- Sélectionner ou désélectionner la case "Activer le client NTP à chaque démarrage" (2) pour respectivement activer ou désactiver le client NTP
- Cliquer sur "Enregistrer et reboot" pour prendre en en compte les modifications
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer de configurer les serveurs NTP

Pour <u>ajouter un serveur NTP</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "NTP" (Figure 12) :

- Cliquer sur l'icône "+" (3) pour ajouter un serveur
- Remplir le champ "IP" pour spécifier l'adresse IP du serveur NTP
- Cliquer sur "Enregistrer et reboot" pour prendre en en compte les modifications
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer l'activation ou la désactivation du client NTP

Pour <u>supprimer un serveur NTP</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "NTP" (Figure 12) :

- Cliquer sur l'icône "Poubelle" du serveur à supprimer (exemple 4)
- Cliquer sur "Enregistrer et reboot" pour prendre en en compte les modifications
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer l'activation ou la désactivation du client NTP





NX2009955 / 72868_B 21/07/2020 16 (34)

7 ONGLET "OPENVPN"



Figure 13 : Onglet "OpenVPN"

7.1 STATUT DU SERVEUR OPENVPN

Pour visualiser le statut du serveur OpenVPN (uniquement possible par un utilisateur avec les

- droits "Administrator"), aller sur la page "Système" onglet "OpenVPN" (Figure 13) :
- Le champ "Statut" (1) indique si le serveur OpenVPN est activé ou désactivé
- Le champ "Adresse IP Virtuel du serveur" (2) indique l'adresse IP virtuelle du serveur OpenVPN lorsqu'il est connecté

Note : L'adresse IP virtuel du serveur est l'adresse IP avec laquelle il faut communiquer pour passer par le tunnel VPN

7.2 CONFIGURATION DU SERVEUR OPENVPN

Pour <u>activer/désactiver le serveur OpenVPN</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "OpenVPN" (Figure 13) :

- Sélectionner ou désélectionner la case "Activer le serveur OpenVPN à chaque démarrage" (3) pour respectivement activer ou désactiver le serveur OpenVPN
- Cliquer sur "Enregistrer et reboot" pour prendre en en compte les modifications
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer le serveur OpenVPN

Pour <u>configurer le serveur OpenVPN</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "OpenVPN" (Figure 13) :

• Remplir le champ "Adresse IP LAN" pour spécifier l'adresse IP de l'interface du coffret par laquelle doit passer le VPN. Exemple, si l'adresse IP de eth0 (COM) est 192.168.0.1, ce champ doit être rempli avec cette adresse







- Remplir le champ "Port" pour spécifier le port TCP ou UDP du serveur
- Remplir le champ "Type d'interface" pour spécifier le type d'interface (TAP ou TUN)
- Remplir le champ "Protocole" pour spécifier le type de protocole (TCP ou UDP)
- Remplir le champ "Adresse réseau virtuelle du tunnel VPN" pour spécifier l'adresse de base du réseau virtuel du tunnel VPN
- Remplir le champ "Masque réseau virtuel du tunnel VPN" pour spécifier le masque réseau virtuel du tunnel VPN
- Sélectionner ou désélectionner la case "Vérification du certificat client dans la CRL" pour respectivement activer ou désactiver la vérification des certificats clients dans la CRL lors d'une connexion au serveur
- Cliquer sur "Enregistrer et reboot" pour prendre en en compte les modifications
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche Note : Dans l'exemple de la Figure 13, l'adresse réseau virtuelle du tunnel est 10.8.0.0 et le masque 255.255.255.0 donc le serveur aura par exemple l'adresse 10.8.0.1 et un client se verra assigné l'adresse 10.8.0.10

Note : Attention si la vérification du certificat client dans la CRL est activée il faut que la CRL soit présente dans le coffret avant d'enregistrer

Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer l'activation ou la désactivation du serveur OpenVPN

Note : Les icônes ⁶⁰ et ⁶⁰ indiquent si les fichiers correspondant sont présents dans le coffret ou non. L'ajout de ces fichiers se fait dans l'onglet "Clés de Cryptage et Certificats"





NX2009955 / 72868_B 21/07/2020 18 (34)



8 ONGLET "IPSEC"



Figure 14 : Onglet "IPSec"

8.1 STATUT DU TUNNEL IPSEC

Pour <u>visualiser le statut du tunnel IPSec</u> (activé ou désactivé) **(uniquement possible par un utilisateur avec les droits "Administrator")**, aller sur la page "Système" onglet "IPSec" (Figure 14) :

• Le champ "Statut" (1) indique si le tunnel IPSec est activé ou désactivé

8.2 CONFIGURATION DU TUNNEL IPSEC

Pour <u>activer/désactiver le tunnel IPSec</u> (uniquement possible par un utilisateur avec les droits

"Administrator"), aller sur la page "Système" onglet "IPSec" (Figure 14) :

- Sélectionner ou désélectionner la case "Activer le tunnel IPSec à chaque démarrage" (2) pour respectivement activer ou désactiver le tunnel IPSec
- Cliquer sur "Enregistrer et reboot" (3) pour prendre en en compte les modifications
- Attendre le redémarrage du coffret





Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer le tunnel IPSec

Pour <u>configurer le tunnel IPSec</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "IPSec" (Figure 14) :

- Configurer la partie coffret (serveur) :
 - Remplir le champ "Adresse IP LAN" pour spécifier l'adresse IP de l'interface du coffret par laquelle doit passer le VPN. Exemple, si l'adresse IP de eth0 (COM) est 192.168.0.1, ce champ doit être rempli avec cette adresse
 - Remplir le champ "Adresse IP Virtuelle du tunnel" pour spécifier l'adresse IP virtuelle que prendra le coffret pour communiquer par le tunnel VPN
 - Remplir le champ "Adresse IP WAN du modem" pour spécifier l'adresse IP WAN si le coffret est relié à un modem (Radio IP ou GPRS ou autre) sinon vide
 - Remplir le champ "Type d'authentification" pour spécifier le type d'authentification du coffret auprès du SCADA
 - Remplir le champ "ID du certificat" pour spécifier l'ID présent dans le certificat x509 qui sert à l'authentification du coffret auprès du SCADA
- Configuration de la partie SCADA (client) :
 - Remplir le champ "Adresse IP WAN" pour spécifier l'adresse IP WAN du SCADA qui se connectera au coffret (en mettant le mot clé "%any" cela signifie toutes les adresses IP)
 - Remplir le champ "Adresse IP Virtuelle du tunnel" pour spécifier l'adresse IP virtuelle que prendra le SCADA pour communiquer par le tunnel VPN
 - Remplir le champ "Type d'authentification" pour spécifier le type d'authentification du SCADA auprès du coffret
 - Remplir le champ "Utilisateur EAP" pour spécifier le nom d'utilisateur pour l'authentification du SCADA auprès du coffret
 - Remplir le champ "Mot de passe EAP" pour spécifier le mot de passe pour l'authentification du SCADA auprès du coffret
- Configuration du tunnel :
 - Remplir le champ "Méthode d'échange des clés" pour spécifier la méthode d'échange des clés
- Configuration IKE (Echange des clés) :
 - Remplir le champ "Algorithme de cryptage" pour spécifier le type d'algorithme de cryptage
 - Remplir le champ "Algorithme d'intégrité" pour spécifier le type d'algorithme d'intégrité
 - Remplir le champ "Groupe Diffie Hellman" pour spécifier le groupe Diffie Hellman
- Configuration ESP (Echange des données) :
 - Remplir le champ "Algorithme de cryptage" pour spécifier le type d'algorithme de cryptage
 - Remplir le champ "Algorithme d'intégrité" pour spécifier le type d'algorithme d'intégrité
 - Remplir le champ "Groupe Diffie Hellman" pour spécifier le groupe Diffie Hellman
 - Cliquer sur "Enregistrer et reboot" (3) pour prendre en en compte les modifications
- Attendre le redémarrage du coffret







Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer l'activation ou la désactivation du tunnel IPSec

Note : Les icônes ⁶⁰ et ⁶⁰ indiquent si les fichiers correspondant sont présents dans le coffret ou non. L'ajout de ces fichiers se fait dans l'onglet "Clés de Cryptage et Certificats"

Pour <u>télécharger des fichiers de configuration client pour Windows ou Linux correspondant à la</u> <u>configuration du serveur</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "IPSec" (Figure 14) :

- Cliquer sur "Télécharger le fichier de configuration client équivalent Linux" pour télécharger le fichier de configuration client pour Linux
- Cliquer sur "Télécharger le fichier de création du client Windows" pour télécharger le fichier de configuration client pour Windows. Ce fichier contient des commandes Power Shell, il faut ouvrir un terminal Power Shell avec les droits Administrateurs et exécuter les commandes pour créer le client IPSec





NX2009955 / 72868_B 21/07/2020 21 (34)

9 ONGLET "DHCP"

ENSTO		:	Système	
🐟 Retour	6		DHCP	
Système	C		Statut: Active	2
Mot de passe				
Utilisateurs		🗹 Activer le	DHCP à chaque démarrage	
Ajouter utilisateur	Sous-Réseau	192 168 10.0	Masque	255 255 255 0
Firewall	Début plage IP allouée	192 168 10 10	Fin plage IP allouée	192 168 10 20
NTP	DNS		Passerelle	
OpenVPN	Temps d'allocation par défaut	(S)600	Temps d'allocation max (s)	(1200
IPSec			Enregistrer et reboot	3,
DHCP				
SSH		Ad	resses IP allouees	
Serveur WEB	Nom	Adresse MAC	Adresse IP	Expiration
Clés de Cryptage et Certificals				

Figure 15 : Onglet "DHCP"

9.1 STATUT DU SERVEUR DHCP

Pour <u>visualiser le statut du DHCP</u> (activé ou désactivé) **(uniquement possible par un utilisateur avec les droits "Administrator")**, aller sur la page "Système" onglet "DHCP" block "DHCP" (Figure 15) :

• Le champ "Statut" (1) indique si le serveur DHCP est activé ou désactivé

9.2 CONFIGURATION DU SERVEUR DHCP

Pour <u>activer/désactiver le DHCP</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "DHCP" block "DHCP" (Figure 15) :

- Sélectionner ou désélectionner la case "Activer le DHCP à chaque démarrage" (2) pour respectivement activer ou désactiver le serveur DHCP
- Cliquer sur "Enregistrer et reboot" pour prendre en en compte les modifications
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer le serveur DHCP

Pour <u>configurer le serveur DHCP</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "DHCP" block "DHCP" (Figure 15) :

- Remplir le champ "Sous-Réseau" pour spécifier le sous-réseau dans lequel les adresses IP seront allouées. Doit correspondre à l'interface eth1 (Configuration)
- Remplir le champ "Masque" pour spécifier le masque du sous-réseau
- Remplir le champ "Début plage IP allouée" pour spécifier le début de la plage des adresses IP allouées
- Remplir le champ "Fin plage IP allouée" pour spécifier la fin de la plage des adresses IP allouées
- (Optionnel) Remplir le champ "DNS" pour spécifier l'adresse IP du serveur DNS
- (Optionnel) Remplir le champ "Passerelle" pour spécifier l'adresse IP de la passerelle
- Remplir le champ "Temps d'allocation par défaut (s)" pour spécifier le temps d'allocation par défaut d'une adresse IP





NX2009955 / 72868_B 21/07/2020 22 (34)

- Remplir le champ "Temps d'allocation max (s)" pour spécifier le temps d'allocation maximum d'une adresse IP
- Cliquer sur "Enregistrer et reboot" (3) pour prendre en en compte les modifications
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer l'activation ou la désactivation du serveur DHCP

9.3 ADRESSES IP ALLOUÉES

Pour <u>visualiser les adresses IP allouées par le serveur DHCP</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "DHCP" block "Adresses IP allouées" (Figure 15) :

- Le champ "Nom" correspond au nom du client connecté au serveur
- Le champ "Adresse MAC" correspond à l'adresse MAC du client connecté au serveur
- Le champ "Adresse IP" correspond à l'adresse IP du client que le serveur a alloué
- Le champ "Expiration" correspond à la date d'expiration de l'adresse IP du client avant renégociation





Clés de Cryptage et Certificats NX2009955 / 72868_B 21/07/2020 23 (34)

10 **ONGLET "SSH"** ENSTO Système Retour SSH 2 Système Statut : Active Mot de passe Activer le SSH à chaque démarrage Utilisateurs Enregistrer et reboot Ajouter utilisateur Firewall **OpenVPN IPSec** DHCP SSH Serveur WEB

Figure 16 : Onglet "SSH"

10.1 STATUT DU SERVEUR SSH

Pour <u>visualiser le statut du serveur SSH</u> (activé ou désactivé) **(uniquement possible par un utilisateur avec les droits "Administrator")**, aller sur la page "Système" onglet "SSH" (Figure 16) :

• Le champ "Statut" (1) indique si le SSH est activé ou désactivé

10.2 CONFIGURATION DU SERVEUR SSH

Pour activer/désactiver le serveur SSH (uniquement possible par un utilisateur avec les droits

"Administrator"), aller sur la page "Système" onglet "SSH" (Figure 16) :

- Sélectionner ou désélectionner la case "Activer le SSH à chaque démarrage" (2) pour respectivement activer ou désactiver le SSH
- Cliquer sur "Enregistrer et reboot" pour prendre en en compte les modifications
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche





11

NX2009955 / 72868_B 21/07/2020 24 (34)

ONGLET "SERVEUR WEB"





11.1 STATUT DU SERVEUR WEB

Pour <u>visualiser le statut du serveur WEB</u> (activé ou désactivé) **(uniquement possible par un utilisateur avec les droits "Administrator")**, aller sur la page "Système" onglet "Serveur WEB" (Figure 17) :

Le champ "Statut" (1) indique si le serveur WEB est activé ou désactivé

11.2 CONFIGURATION DU SERVEUR WEB

Pour <u>activer ou désactiver l'accès à distance du serveur WEB</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "Serveur WEB" (Figure 17) :

- Sélectionner ou désélectionner la case "Accès au page WEB via l'interface eth0 (COM)" pour respectivement activer ou désactiver l'accès à distance
- Remplir le champ "Adresse IP eth0 (COM)" avec l'adresse IP de l'interface Ethernet eth0 (COM)
- Cliquer sur "Enregistrer et reboot" pour prendre en en compte les modifications
- Attendre le redémarrage du coffret

Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer les autres fonctionnalités du serveur WEB

Pour <u>activer ou désactiver l'authentification mutuelle</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "Serveur WEB" (Figure 17) :

- Sélectionner ou désélectionner la case "Activer l'authentification mutuelle par certificat" pour respectivement activer ou désactiver l'authentification mutuelle
- Sélectionner ou désélectionner la case "Vérification du certificat client dans la CRL" pour respectivement activer ou désactiver la vérification des certificats clients dans la CRL lors d'une connexion au serveur
- Cliquer sur "Enregistrer et reboot" pour prendre en en compte les modifications
- Attendre le redémarrage du coffret





NX2009955 / 72868_B 21/07/2020 25 (34)



Note : Le redémarrage est terminé lorsque la page de connexion au serveur web s'affiche Note : Avant de cliquer sur "Enregistrer et reboot" il est possible en même temps de configurer les autres fonctionnalités du serveur WEB

Note : Attention si la vérification du certificat client dans la CRL est activée il faut que la CRL soit présente dans le coffret avant d'enregistrer

Note : L'authentification mutuelle oblige le client à s'identifier auprès du serveur WEB avec un certificat Note : Les icônes ^(S) et ^(S) indiquent si les fichiers correspondant sont présents dans le coffret ou non. L'ajout de ces fichiers se fait dans l'onglet "Clés de Cryptage et Certificats"









12.1 CRL

Pour <u>configurer la CRL</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "Clés de Cryptage et Certificats" (Figure 18) :

Système

- Cliquer sur le volet "CRL" (1)
- Le volet de configuration de la CRL s'ouvre :

ENSTO

🚓 Retour	Clès de Cryptage et Certificats 5	
Système	6	
Mot de passe	URL U	•
Utilisateurs	Envoyer CRL PEM:	
Ajouter utilisateur	CRL (.pem): Choisir un fichier Aucun fichier choisi	
Firewall	Envoyer	
(NTP.)	Reboot pour prendre en compte les modifications	
OpenVPN		
IPSec	Serveur web	~
DHCP	OpenVPN	~
SSH	IPSec	~
Serveur WEB		

Clés de Cryptage et Certificats

4PR-F8-H

Figure 19 : Volet de configuration de la CRL

- Cliquer sur "Choisir un fichier" (5)
- En fonction du navigateur internet, une boite de dialogue s'ouvre





- Sélectionner le fichier PEM codé en base 64 correspondant à la CRL
- Cliquer sur "Envoyer" (6) pour transférer la CRL

Note : Après appui sur "Envoyer" la CRL est chargée dans le coffret mais n'est pas prise en compte, il faut redémarrer le coffret pour qu'elle le soit en appuyant sur "Reboot pour prendre en compte les modifications"

12.2 Serveur WEB

Pour <u>configurer les clés et certificats du serveur WEB</u> (uniquement possible par un utilisateur avec les droits "Administrator"), aller sur la page "Système" onglet "Clés de Cryptage et Certificats" (Figure 18) :

- Cliquer sur le volet "Serveur WEB" (2)
- Le volet de configuration des clés et certificats du serveur WEB s'ouvre :

The intervention of the in	Clés de Cryptage et Certificats		
Système	31		
dot de pase 7	arveur Web		
Utilisatours	You do not set to be the state of the set for the set for the set of the set		
outer ublisateur	Zone de sauvegarde de la cie privee et du certificat	Zone Memoire	
Firewall	Generer Cle Privés	J Lire Cle Publique	_
NIP	Like Certificat		
OpenVPN	Lite Certificat CA		
IPSec G	ánérer CSR PEM:		
DHCP	Pays (2 lettres)	Département	
SSH	Ville	Société	
rvour W	Service	Nom de l'hôte	
o Cry 8	Nom	Adresse e-mail	
E	woyer Certificat PEM: 10 Certificat (.crt): Ch	olsir un fichier Aucun fichier choisi	
		Envoyer 11	
E	1voyer Certificat PEM CA: 12 Certificat (crt): Chi	sisir un fichier Aucun fichier choisi	
E	1voyer Certificat PEM CA: 12 Certificat (.crt): Ch	blair un fichier Aucun fichier choisi Envoyer	
E	Ivoyer Certificat PEM CA: 12 Certificat (.crt): Ch Ivoyer Paramètre Diffie Hellman 4096 PEM. Parmètre DH (.pem):	bisir un fichier Aucun fichier choisi Envoyer 13 Choisir un fichier Aucun fichier choisi	
E	nvoyer Certificat PEM CA: 12 Certificat (.crt): Ch ivoyer Paramètre Diffie Hellman 4096 PEM: Parmètre DH (.pem): [blair un fichier Envoyer 13 Cholair un fichier Aucun fichier cholal Envoyer	
Ē	nvoyer Certificat PEM CA: 12 Certificat (.crt): Ch ivoyer Paramètre Diffie Hellman 4096 PEM. Parmètre DH (.pem): [Reboot pour pren	bisir un fichier Envoyer 13 Choisir un fichier Aucun fichier choisi Envoyer dre en compte les modifications	
E	nvoyer Certificat PEM CA: 12 Certificat (.crt): Ch nvoyer Paramètre Diffie Heilman 4096 PEM: Parmètre DH (.pem): [Reboot pour pren cenVPN	olsir un fichier Aucun fichier choisi Envoyer 13 Choisir un fichier Aucun fichier choisi Envoyer dre en compte les modifications	~

Figure 20 : Volet de configuration des clés et certificats du serveur WEB





- Cliquer sur "Générer Clé Privée" (7) pour générer la clé privée du serveur WEB
- Générer la demande de signature de certificat (CSR) du serveur WEB (8) :
 - Remplir le champ "Pays (2 lettres)" pour spécifier les 2 lettres du pays du certificat (exemple : FR)
 - Remplir le champ "Département" pour spécifier le département du certificat (exemple : Rhône)
 - Remplir le champ "Ville" pour spécifier la ville du certificat (exemple : Lyon)
 - Remplir le champ "Société" pour spécifier l'entreprise du certificat (exemple : Ensto)
 - Remplir le champ "Service" pour spécifier le service du certificat (exemple : Sécurité)
 - Remplir le champ "Nom de l'hôte" pour spécifier le nom de l'hôte du certificat (exemple : Ensto)
 - Remplir le champ "Nom" pour spécifier le nom du certificat (exemple : Certificat WEB)
 - Remplir le champ "Adresse e-mail" pour spécifier le l'adresse e-mail du certificat (exemple : security@ensto.com)
 - Cliquer sur "Générer CSR" pour générer et télécharger le CSR au format PEM codé en base 64
 - En fonction du navigateur internet, le fichier se télécharge
- Envoyer la demande de signature à une autorité de certification de votre choix afin de générer le certificat du serveur WEB
- Transfert du certificat du serveur WEB :
 - Cliquer sur "Choisir un fichier" (9)
 - En fonction du navigateur internet, une boite de dialogue s'ouvre
 - Sélectionner le fichier CRT codé en base 64 correspondant au certificat du serveur WEB
 - Cliquer sur "Envoyer" (10) pour transférer le certificat
- Transfert du certificat de l'autorité de certification :
 - Cliquer sur "Choisir un fichier" (11)
 - En fonction du navigateur internet, une boite de dialogue s'ouvre
 - Sélectionner le fichier CRT codé en base 64 correspondant au certificat de l'autorité de certification
 - Cliquer sur "Envoyer" (12) pour transférer le certificat
- Transfert du paramètre Diffie Hellman :
 - Générer un fichier PEM codé en base 64 contenant un paramètre Diffie Hellman de 4096 bits
 → Il est possible de générer se paramètre grâce à l'outil "openssl" sous Linux avec la
 commande "openssl dhparam -out dhparam.pem 4096"
 - Cliquer sur "Choisir un fichier" (13)
 - En fonction du navigateur internet, une boite de dialogue s'ouvre
 - Sélectionner le fichier PEM codé en base 64 correspondant au paramètre Diffie Hellman
 - Cliquer sur "Envoyer" (14) pour transférer le certificat

Note : Lorsqu'une nouvelle clé privée est générée il faut également générer un nouveau certificat pour qu'il correspond à cette nouvelle clé

Note : Une fois tous les fichiers transférés sur le coffret il faut le redémarrer pour qu'ils soient pris en compte en appuyant sur "Reboot pour prendre en compte les modifications"







12.3 OpenVPN

Pour configurer les clés et certificats du serveur OpenVPN (uniquement possible par un utilisateur avec les

droits "Administrator"), aller sur la page "Système" onglet "Clés de Cryptage et Certificats" (Figure 18) :

- Cliquer sur le volet "OpenVPN" (3)
- Le volet de configuration des clés et certificats du serveur OpenVPN s'ouvre :

ENSTO

Système

 Retour 	Clés de Cryptage et Certificats				
Systômo	CRL	~			
Mot de pase	Serveur Web	~			
Utilisator 15	OpenVPN	×			
Ajoutor utilisa.		and the second sec			
Firowall	Zone de sauvegarde de la cle privée et du certificat	Zone Mémoire 👻			
NTP	Générer Clé Privée	Life Cle Publique			
OpenVPN	L u	re Certificat			
IPSec	Lire Certificat CA				
DHCP	Générer CSR PEM:	8			
SSH	Pays (2 lettres)	Département			
Servour WEB	Ville	Société			
Clés de Cry t	Service	Nom de l'hôte			
	Nom	Adresse e-mail			
	Liste des extensions à ajoute	er lors de la génération du certificat:			
	authorityKeyIdenti	fier = keyid, issuer:always			
	G	énérer CSR 17			
	Envoyer Certificat PEM 18				
	Certificat (crt) Chain	ir un fichier Aurun fichier chain			
	and any fairly fairly fairly	Envoyer			
		19			
	Envoyer Certificat PEM CA: 20				
	Certificat (.crt): Choisir un fichier Aucun fichier choisi				
		Envoyer 21			
	Envoyer Paramètre Diffie Hellman 2048 PEM	(22)			
	Parmétre DH (pem): Choisir un fichier Aucun fichier choisi				
		Envoyer			
	Reboot pour prendra	e en compte les modifications			
	IPSec	~			
	L'anna				

Figure 21 : Volet de configuration des clés et certificats du serveur OpenVPN

- Cliquer sur "Générer Clé Privée" (15) pour générer la clé privée du serveur OpenVPN
- Générer la demande de signature de certificat (CSR) du serveur OpenVPN (16) :
 - Remplir le champ "Pays (2 lettres)" pour spécifier les 2 lettres du pays du certificat (exemple : FR)
 - Remplir le champ "Département" pour spécifier le département du certificat (exemple : Rhône)
 - Remplir le champ "Ville" pour spécifier la ville du certificat (exemple : Lyon)
 - Remplir le champ "Société" pour spécifier l'entreprise du certificat (exemple : Ensto)
 - Remplir le champ "Service" pour spécifier le service du certificat (exemple : Sécurité)





- Remplir le champ "Nom de l'hôte" pour spécifier le nom de l'hôte du certificat (exemple : Ensto)
- Remplir le champ "Nom" pour spécifier le nom du certificat (exemple : Certificat Serveur OpenVPN)
- Remplir le champ "Adresse e-mail" pour spécifier le l'adresse e-mail du certificat (exemple : security@ensto.com)
- Cliquer sur "Générer CSR" pour générer et télécharger le CSR au format PEM codé en base 64
- En fonction du navigateur internet, le fichier se télécharge
- Envoyer la demande de signature à une autorité de certification de votre choix afin de générer le certificat du serveur OpenVPN
- Transfert du certificat du serveur OpenVPN :
 - Cliquer sur "Choisir un fichier" (17)
 - En fonction du navigateur internet, une boite de dialogue s'ouvre
 - Sélectionner le fichier CRT codé en base 64 correspondant au certificat du serveur OpenVPN
 - Cliquer sur "Envoyer" (18) pour transférer le certificat
- Transfert du certificat de l'autorité de certification :
 - Cliquer sur "Choisir un fichier" (19)
 - En fonction du navigateur internet, une boite de dialogue s'ouvre
 - Sélectionner le fichier CRT codé en base 64 correspondant au certificat de l'autorité de certification
 - Cliquer sur "Envoyer" (20) pour transférer le certificat
- Transfert du paramètre Diffie Hellman :
 - Générer un fichier PEM codé en base 64 contenant un paramètre Diffie Hellman de 2048 bits
 → Il est possible de générer se paramètre grâce à l'outil "openssl" sous Linux avec la
 commande "openssl dhparam -out dh2048.pem 2048"
 - Cliquer sur "Choisir un fichier" (21)
 - En fonction du navigateur internet, une boite de dialogue s'ouvre
 - Sélectionner le fichier PEM codé en base 64 correspondant au paramètre Diffie Hellman
 - Cliquer sur "Envoyer" (22) pour transférer le certificat

Note : Lorsqu'une nouvelle clé privée est générée il faut également générer un nouveau certificat pour qu'il correspond à cette nouvelle clé

Note : Une fois tous les fichiers transférés sur le coffret il faut le redémarrer pour qu'ils soient pris en compte en appuyant sur "Reboot pour prendre en compte les modifications"

12.4 IPSec

Pour <u>configurer les clés et certificats du serveur IPSec</u> (uniquement possible par un utilisateur avec les desite "Administrator"), aller sur la page "Suttème" anglet "Clés de Countage et Cartificats" (Figure 18) :

- droits "Administrator"), aller sur la page "Système" onglet "Clés de Cryptage et Certificats" (Figure 18) :
 - Cliquer sur le volet "IPSec" (4)
 - Le volet de configuration des clés et certificats du serveur IPSec s'ouvre :





ENSTO

NX2009955 / 72868_B 21/07/2020

31 (34)

Système

🗢 Retour	Clés de Cryptage et Certificats		
Système	CBI		~
Mot de passe	Cancer Mak		
Utilisateurs	Servedr Web		•
Ajouter utilis 22	OpenVPN		~
Firewall	IPSec		~
NTP	Zone de sauvegarde de la clé privée et du certificat	Zone Mémoire	~
OpenVPN	Générer Clé Privée	Lire Clé Publique	
IPSec	Lire Certificat		10
DHCP	Générer CSR PEM		
SSH	Pays (2 lettres)	Département	
Serveur WEB	Ville	Société	
Clés de Cryptage et	Ville Ville	Suciete	
Certific	Service	Nom de l'hote	
24	Nom	Adresse e-mail	
	Adresse IP LAN du coffret ou Adresse IP WAN du modern	Adresse IP WAN lorsque le coffret est connecté à un modern	
	Liste des extensions à ajouter authorityKeyldentifie	r lors de la génération du certificat: er = keyid, issuer:always	
	Gér	vérer CSR 25	
	Envoyer Certificat PEM: 26 Certificat (.crt): Chelsin	un fichier Aucun fichier choisi	
	E	invoyer]
	Rebost pour prendre	en compte les modifications	

Figure 22 : Volet de configuration des clés et certificats du serveur IPSec

- Cliquer sur "Générer Clé Privée" (23) pour générer la clé privée du serveur IPSec
- Générer la demande de signature de certificat (CSR) du serveur IPSec (24) :
 - Remplir le champ "Pays (2 lettres)" pour spécifier les 2 lettres du pays du certificat (exemple : FR)
 - Remplir le champ "Département" pour spécifier le département du certificat (exemple : Rhône)
 - Remplir le champ "Ville" pour spécifier la ville du certificat (exemple : Lyon)
 - Remplir le champ "Société" pour spécifier l'entreprise du certificat (exemple : Ensto)
 - Remplir le champ "Service" pour spécifier le service du certificat (exemple : Sécurité)
 - Remplir le champ "Nom de l'hôte" pour spécifier le nom de l'hôte du certificat (exemple : Ensto)
 - Remplir le champ "Nom" pour spécifier le nom du certificat (exemple : Certificat Serveur IPSec)
 - Remplir le champ "Adresse e-mail" pour spécifier le l'adresse e-mail du certificat (exemple : security@ensto.com)
 - Si le coffret est relié à modem (Radio IP ou GPRS ou autre), remplir le champ "Adresse IP LAN du coffret ou Adresse IP WAN du modem" pour spécifier l'adresse IP WAN du modem
 - Si le coffret est relié en local, remplir le champ "Adresse IP LAN du coffret ou Adresse IP WAN du modem" pour spécifier l'adresse IP de eth0 (COM) du coffret
 - Cliquer sur "Générer CSR" pour générer et télécharger le CSR au format PEM codé en base 64
 - En fonction du navigateur internet, le fichier se télécharge





NX2009955 / 72868_B 21/07/2020 32 (34)

- Envoyer la demande de signature à une autorité de certification de votre choix afin de générer le certificat du serveur IPSec
- Transfert du certificat du serveur IPSec :
 - Cliquer sur "Choisir un fichier" (25)
 - En fonction du navigateur internet, une boite de dialogue s'ouvre
 - Sélectionner le fichier CRT codé en base 64 correspondant au certificat du serveur IPSec
 - Cliquer sur "Envoyer" (26) pour transférer le certificat

Note : Lorsqu'une nouvelle clé privée est générée il faut également générer un nouveau certificat pour qu'il correspond à cette nouvelle clé

Note : Une fois tous les fichiers transférés sur le coffret il faut le redémarrer pour qu'ils soient pris en compte en appuyant sur "Reboot pour prendre en compte les modifications"

4PR-F8-H





NX2009955 / 72868_B 21/07/2020 33 (34)



Note



NX2009955 / 72868_B 21/07/2020 34 (34)

Fiche suivi retour matériel

Service Après-Vente

210, rue Léon Jouhaux – BP 10446 FR – 69656 Villefranche-sur-Saône Cedex Fixe : +33 (0)4 74 65 61 60 Mobile : +33 (0)6 08 93 26 31

4PR-F8-H

Ce document est la propriété de la société Ensto Novexia, il ne peut être ni reproduit, ni communiqué à des tiers sans autorisation écrite This document is the property of Ensto NOVEXIA, it may not be reproduced, disclosed without written authorization

