BELKIN®

OmniView® Serveur de console série

Manuel de l'utilisateur

F1DP116Sea

Table of Contents

Présentation du produit 1
- Introduction 1
- Contenu de l'emballage 1
- Fonctions du serveur de console 2
- Matériel requis 3
- Configuration requise 3
- Illustrations de l'appareil 4
- Voyants lumineux, bouton et connecteurs 5
- Spécifications 6

Installation locale 7
- Installation sur bureau ou montage en baie 8
- Connexion des périphériques cibles au serveur de console 9

Configuration réseau 10
- Interface de navigateur web 10
- Attribution des adresses IP à partir du port de la console--VT-100 (Console, Telnet, SSH) 13
- Interface de gestion de navigateur web 16

Paramètres réseau 18
- Configuration de l'adresse IP : 18
- Filtrage IP 19
- Configuration du Serveur d'Impression 21
  - Local 21
  - RADIUS et Local 21
- DNS Dynamique 22
- RADIUS 23
- Configuration du Serveur RADIUS 24
- HTTPS/SSL 24

Ports série 25
- Configuration 25
  - Authentification de port 25
  - Activer/Désactiver le port 26
  - Titre de port 26
  - Modes de fonctionnement 27
    - Mode du serveur de console 27
    - Mode du serveur de terminal 28
    - Mode modem d'accès distant 29
  - Paramètres du port série 29
  - Connexion du port 30
  - Fonction Pause 31
- Connexion 31
  - Applet Java Telnet 32
- Fonction série à série 34

Etat de système et fichier journal **37**
État du système 37
Connexion au système 37

Administration de système **39**
Administration utilisateur 39
Ajout d'un utilisateur 39
Retrait d'un utilisateur 40
Modification de l'Access Control List (ACL) 41
Modification du mot de passe 42
Date et heure (NTP) 42
Mise à jour du micrologiciel 43
Mise à niveau à partir de l'interface Web 43
SSL Certificate [Certificat SSL] 44
Certificat de protocole HTTP sécurisé 45
Rétablir les paramètres par défaut 49
Redémarrer 49

Caractéristiques techniques **50**
Paramètres par défaut 50

Annexe A : Adaptateurs **51**

Annexe B : Brochages Ethernet (RJ45) **54**
Brochage RJ45 câble Ethernet standard RJ45 54

Annexe C : Numéros de port réservés de TCP/UDP **55**

Annexe D : Glossaire de protocole **56**

Annexe E : Création de fichiers CA **58**

Informations **60**

Introduction

Nous vous remercions d'avoir choisi le serveur de console série Belkin OmniView (serveur de console). Ce périphérique fournit aux administrateurs le monitorage sécurisé des serveurs, des routeurs, des interrupteurs, et d'autres périphériques série de n'importe où sur le réseau d'entreprise TCP/IP, sur internet, ou par les connexions modem à distance, même lorsque le serveur est indisponible via le réseau.

Le serveur de console fournit ce qui suit :

- Sécurisation du chemin de données au moyen de SSH ou Web/SSL
- Une interface web sécurisée et cryptée sur SSL (HTTPS)
- Cryptage SSHv2, pour tenir des mots de passe d'accès de serveur à l'abri des hackers
- Support de tous les clients populaires SSH
- Accès sécurisé de tout navigateur activé par Java
- Connexions aux ports de console série à l'aide des câbles CAT5 standard, sans les tracas du câblage sur mesure

Contenu du coffret

1 x Serveur de console série OmniView

1 x Cordon d'alimentation AC

5 x Kit adaptateur série à RJ45 (5 pièces)

1 x Adaptateur série de port de console local

1 x Câble de 6 pieds RJ45-RJ45 CAT5

1 x Guide de démarrage rapide

1 x Manuel de l'utilisateur sur CD-ROM

1 x périphérique de montage dans une baie et vis

1 x Jeu de dessous

Fonctions du serveur de console

- **Gestion intrabande et extrabande**
  Les solutions de gestion de port de console offrent un accès distant, fiable, et sécurisé aux ports de console série via les réseaux intrabande et les options de connectivité extrabande, telles que l'accès au terminal série et au modem pour connexion à distance.
- **Gestion des périphériques de réseau/serveurs de réseau centralement, à distance et de façon sécurisée**
  Des solutions de gestion de port de console fiables vous permettent de crypter des données sensibles à l'aide des protocoles testés tels que SSH/v2, SSL.
- **Gestion de périphériques divers**
  L'émulation de terminal ASCII ou VT-1 00 simple n'est pas suffisante pour gérer ces types de périphérique étendus. Les centres de traitement des données d'aujourd'hui comportent un vaste mélange d'UNIX®, Linux®, RISC, mainframe, et serveurs de Windows®, ainsi que d'autres périphériques gérés en série tels que le routeur, la passerelle, le pare-feu, le PBX, l'UPS, le DAN, les périphériques NAS, et les tableaux de connexion intelligents.
- **Surveillance proactive et alarme pour aider le diagnostic de système**
  Les applications, et même les systèmes d'exploitation, envoient des messages à la console de système. Ces messages contiennent l'erreur et l'information de panique qui précède souvent un crash de système. À la différence des serveurs terminaux, les serveurs de port de console bufférisent ces messages en temps réel et permettent à des administrateurs de parcourir et de rechercher ces données par la suite ; ils envoient également spontanément un e-mail pour alerter l'administrateur IT de l'événement critique.
- **Contrôleur d'alimentation distant et sécurité**
  Via le port série, ce périphérique sert de maître de commande pour contrôler les blocs multiprises. Il peut contrôler des blocs multiples (jusqu'à 15).
- **Fournit la fonction série à série**
  Ceci permet au périphérique de s'intégrer dans un convertisseur terminal pour fournir les ports VGA et de clavier localement, ou les connecter à un switch KVM pour consolider l'administration.
- **Listes des ports d'accès pour les utilisateurs**
  Grâce à l'Access Control List (ACL) de l'administration des comptes utilisateur, tous les comptes utilisateurs excepté **admin** sont autorisés à avoir un jeu de ports série. Les utilisateurs peuvent accéder et effectuer des modifications de configuration à ces ports série autorisés et attribués par un compte **admin**.

Matériel requis

- Kit de connectivité universel (inclus)
- Câble RJ45-RJ45 CAT5 (inclus)

Configuration requise

Navigateur Web

Navigateur		
Système d'exploitation	Microsoft Internet Explorer version 6.0 SP1 et plus récent	Firefox version 2.0 et plus récent
Windows 2000 SP2	Oui	Oui
Windows Server 2003	Oui	Oui
Windows XP	Oui	Oui
Windows Vista	Oui	Oui
Red Hat Linux 3 et 4	Non	Oui
Sun Solaris 9 et 10	Non	Oui
Novell SUSE Linux 9 et 10	Non	Oui
Fedora Core 4 et 5	Non	Oui
Mac OS X 10.4+	Non	Oui

Plug-In Java

L'interface web du serveur de console exige l'installation de JRE (environnement d'exécution de Java) v6.0 et ultérieure. Vous pouvez obtenir le dernier logiciel de Java à partir du site Web : http://www.java.com/en/download/manual.jsp.

Illustrations de l'appareil

Panneau avant/arrière

Fig. 1 - Vue avant

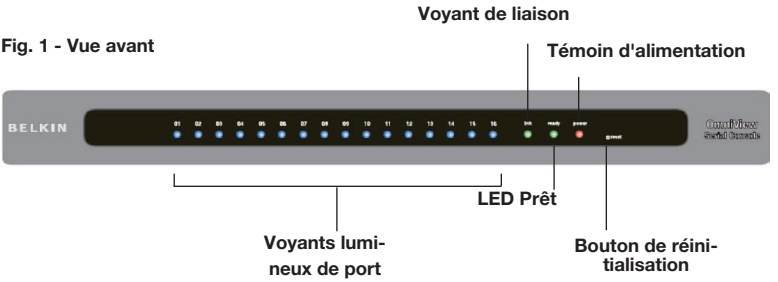
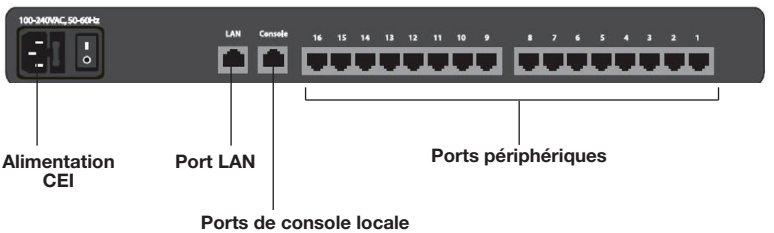


Fig. 2 - Vue arrière



Voyants lumineux, bouton et connecteurs

Voyants	Signification
Alimentation	**Rouge –** relatif à l'alimentation *Allumé : alimentation en cours*
Liaison	**Liaison/Act/10/100Mbps Ethernet :** **Orange –** connexion Ethernet 10BaseT en cours **Vert –** connexion Ethernet 100BaseT en cours *Clignotant : si transfert de données* *Allumé : si aucun transfert de données et liaison en cours*
Prêt	**Vert** – clignote à toutes les secondes lorsque le système est prêt
Activité au port (un voyant par port)	**Bleu** – activité *Allumé : en cours d'utilisation (connexion au port réussie)* *Clignotant : activité au port série*

- Bouton **RESET** : Appuyez rapidement et relâchez le bouton pour redémarrer le serveur de console. Appuyez sur et maintenez le bouton « RESET » enfoncé pendant plus de cinq secondes pour définir l'unité à son paramétrage de configuration par défaut.
- Connecteur **ETHERNET** RJ45 : Interface Ethernet
- Connecteur **CONSOLE** RJ45 : Interface de console locale RS232
- **Autres connecteurs** RJ45 : ports série

Spécifications

Caractéristique	Spécification
Général	**Voyants** Alimentation (rouge) Prêt (vert, clignotant normalement), Lien/Act/10/100Mbps (Ethernet orange: 10Mbps, vert : 100Mbps)
	Activité (bleue pour chaque port série)
	Bouton poussoir pour la réinitialisation ou la restauration des valeurs par défaut
	RTC (real-time clock) (horloge temps réel)
Interface série	16 ports (F1DP116S)
	Mode port série (RS232)
	Connecteur série (RJ45)
	Vitesse baud (300 à 115200)
	Contrôle de flux (Aucun, RTS/CTS, Xon/Xoff)
Interface LAN	Connecteur RJ45
	IEEE 802.3 - 10/100BaseT
	Auto-détection, duplex intégral ou semi-duplex
Fonction port	**Modes de fonctionnement**
	Serveur de console
	Serveur terminal
	Modem accès distant
	Série à série (sur port 16 seulement)
Protocoles :	TCP, UDP, IP, arp, ICMP, HTTP/HTTPS, Telnet, DHCP/BOOTP, PPA,
	SMTP, DNS, NTP
	DNS Dynamique
Fonction relative au protocole	Temps d'inactivité de TCP (temps de maintien TCP)
	Temps d'inactivité série
	Surveillance port
Sécurité	Accès de mot de passe
	Filtrage IP
	SSHv2
	HTTPS/SSL
Authentification	Base de données utilisateur locale
	PAP/CHAP (pour l'accès distant de modem)
	RADIUS
Gestion :	Console locale (menu ou ligne de commande)
	SSH, telnet
	Pages Web (HTTP/HTTPS)
	Mise à jour du micrologiciel via l'interface web
	Mise en mémoire tampon et connexion du port
	Affichage de l'état du système complet
Alimentation et environnement	Entrée CA (100 ~ 240VAC, 50 ~ 60Hz)
	Température de fonctionnement : -10° à 80° C
	Température de stockage : -20° à 85° C
	Humidité : 0-90% sans condensation
Certifications	CE, FCC
	UL
Mécanique	1 périphérique de montage dans une baie 19˝
	Dimensions (cm): 43,2 x 18,0 x 4,2

Remarque : Ces spécifications sont sujettes à modification sans préavis.

Où installer la console de serveur :
Le boîtier du switch est conçu pour être installé de manière autonome ou dans une baie. Le switch peut être monté dans une baie de serveurs standard de 19 pouces au moyen du kit de montage (supports et vis) fourni.

Prenez en considération les éléments suivants avant de choisir l'emplacement d'installation de la console :

- l'emplacement des serveurs par rapport à la console
- la longueur des câbles utilisés pour brancher vos périphériques à la console
- la source d'alimentation - ne connectez l'appareil seulement à la source d'alimentation spécifiée sur l'unité. Quand des composants électriques multiples sont installés dans une baie, assurez-vous que les puissances nominales de tous les composants ne dépassent pas les capacités de circuit.

Longueur de câble exigée (pour CAT5)
Les signaux de données binaires série (RS232) transmettent mieux jusqu'aux distances de 15 m. Au-delà, les risques de dégradation du signal augmentent. Ainsi, Belkin vous recommande de ne pas utiliser un câblage CAT5 UTP de plus de 15 mètres, entre le serveur de console et les serveurs branchés.

Câbles et adaptateurs
Belkin vous recommande vivement d'utiliser des câbles de raccordement de la catégorie 5e, FastCAT5e, ou de la catégorie 6 de Belkin pour votre serveur de console afin d'assurer l'intégrité de signal.

Câbles de raccordement UTP Belkin :

A3L791-XX-YYY (CAT5e)

A3L850-XX-YYY (FastCAT™ 5e)

A3L980-XX-YYY (CAT6)

Reportez-vous à l'annexe B à la page 54 pour ce qui est des fonctions des broches.

Adaptateur série Belkin :

F1D120ea (RJ45F–DB9F DTE)

F1D121ea (RJ45F–DB25F DTE)

F1D122ea (RJ45F – DB25M DCE)

F1D123ea (RJ45F–DB25M DTE)

F1D124ea (RJ45F–RJ45M CISCO)

F1D120ea-8PK (pack de 8 F1D120ea)

F1D124ea-8PK (pack de 8 F1D124ea)

Reportez-vous à l'annexe A à la page 51 pour les illustrations détaillées de chaque adaptateur série.

Installation sur bureau ou montage en baie

Le serveur de console peut être mis sur des ordinateurs de bureau ou monté dans une baie de 19 pouces/1U.

Remarque : Avant de commencer, repérez l'adresse MAC et le numéro de série à l'arrière de la console du serveur. Vous pouvez avoir besoin de ces informations plus tard au cours de l'installation, alors nous vous recommandons vivement de les noter ci-dessous avant de monter la console de serveur dans votre baie.

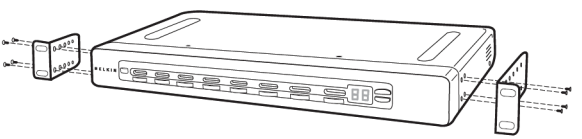
Adresse M**AC**	**Numéro de série :**

Le Serveur de console est livré avec des fixations de montage réglables parfaitement adaptées à une installation dans des baies de 19 pouces. Les supports de fixation proposent trois positions de réglage, ce qui permet d'aligner la face du serveur de console avec les extrémités des rails ou de placer la console de serveur de façon à ce qu'il dépasse à l'avant des rails. Procédez comme suit pour obtenir facilement le réglage souhaité.

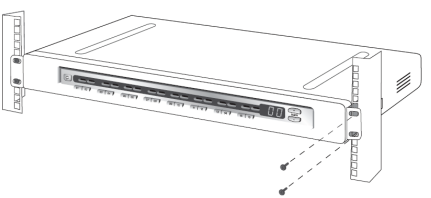
Fixations de montage en baie

1 Déterminez la profondeur à laquelle vous désirez installer la console de serveur dans la baie. Choisissez les orifices correspondants sur les fixations.

2 Fixez le support de montage sur le côté du serveur de console à l'aide des vis cruciformes fournies. (Reportez-vous au schéma ci-dessous).



3. Montez le serveur de console dans le rail de la baie et fixez-le à l'aide des vis. (Reportez-vous au schéma ci-dessous).



Votre serveur de console est ainsi solidement ancré dans la baie. Vous pouvez maintenant brancher vos périphériques.

Connexion des périphériques cibles au serveur de console

1. Eteignez le ou les périphériques que vous allez connecter à votre serveur de console.
2. Connectez le câble Ethernet au port avec l'étiquette LAN.
3. Localisez le cordon d'alimentation inclus et branchez l'extrémité appropriée à la prise secteur à l'arrière du serveur de console. Branchez ensuite l'autre extrémité à la prise secteur appropriée.

Remarque : Attendez environ 100 secondes pour que le serveur de console termine le processus de démarrage.

4. Choisissez un port numéroté disponible à l'arrière de votre serveur de console. Branchez l'extrémité d'un câble de connexion UTP (4-paires, jusqu'à 15 mètres) au port sélectionné, et branchez l'autre extrémité au périphérique cible. Il est possible de devoir ajouter l'adaptateur approprié servant d'interface à votre périphérique cible. Pour de plus amples informations, reportez-vous à l'annexe A à la page 51 de ce manuel.
5. Répétez cette procédure pour tous les périphériques cibles. (Reportez-vous au schéma ci-dessous).

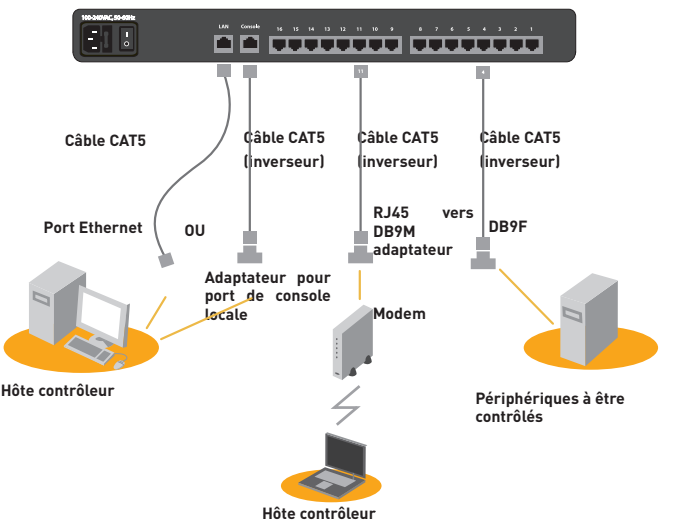


Fig. 3 Configuration de connexion de câblage - ce schéma illustre les connexions du câble témoin pour différentes interfaces.

Avant de pouvoir connecter un périphérique cible, vous devrez configurer les paramètres réseau. Le serveur de console offre deux méthodes de paramétrage réseau : via l'interface du navigateur web browser ou via le port de console local.

Le serveur de console offre le support pour le protocole de configuration dynamique de l'hôte DHCP (DHCP) et l'adressage IP statique. Belkin recommande qu'une adresse IP soit réservée au serveur de console et qu'elle reste statique pendant la connexion au réseau.

Interface de navigateur web

L'interface web offre une manière simple de configurer le serveur de console. L'administrateur peut configurer toutes les caractéristiques techniques par le Web.

Paramétrages initiaux

La section suivante fournissent les instructions de paramétrage de l'adresse IP pour le serveur de console série OmniView.

Étape 1 Identification de l'adresse IP

Après avoir connecté votre serveur de console au réseau et après l'avoir mis sous tension, un serveur DHCP (Dynamic Host Configuration Protocol) sur votre réseau attribuera automatiquement une adresse IP, une adresse de passerelle et un masque de sous-réseau à la console IP.

Pour identifier l'adresse IP de votre réseau, servez-vous de l'adresse MAC situé à l'arrière du serveur de console. Si aucun serveur DHCP n'est présent sur votre réseau, le serveur de console démarrera avec l'adresse IP fixe suivante : 192.168.2.156.

Si vous désirez connecter plus d'une console de serveur au même réseau sans serveur DHCP, connectez chaque console IP à votre réseau l'une après l'autre et modifiez l'adresse IP fixe de chaque unité avant de connecter la suivante.

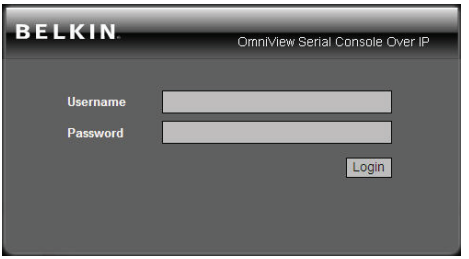
Remarque : Si un serveur DHCP est ajouté à votre réseau ultérieurement, le serveur de console recevra une nouvelle adresse IP du serveur DHCP. Pour conserver l'adresse IP fixe originale, il est nécessaire de désactiver le DHCP (voir page 18).

Etape 2 Connexion à l'interface Web

Après avoir identifié l'adresse IP de votre périphérique, ouvrez votre navigateur web. La liste des navigateurs pris en charge peut être trouvée à la page 3.

Saisissez l'adresse IP du serveur de console dans la zone d'adresse du navigateur, en utilisant ce format : http://XXX.XXX.XXX.XXX (exemple : http://76.255.43.173). La page de connexion apparaît (voir la page suivante). Ajoutez cette page à vos signets pour pouvoir y accéder plus facilement.

Remarque : le protocole HTTPS peut être utilisé pour la communication avec un cryptage SSL (Secure Socket Layer). Après vous être connecté à la page de configuration HTTPS de la console de serveur, vous verrez peut-être deux avertissements. Cliquez « Oui » à chacun.



Page de connexion

Entrez le nom d'utilisateur et le mot de passe par défaut suivants (respecter les majuscules et les minuscules) :

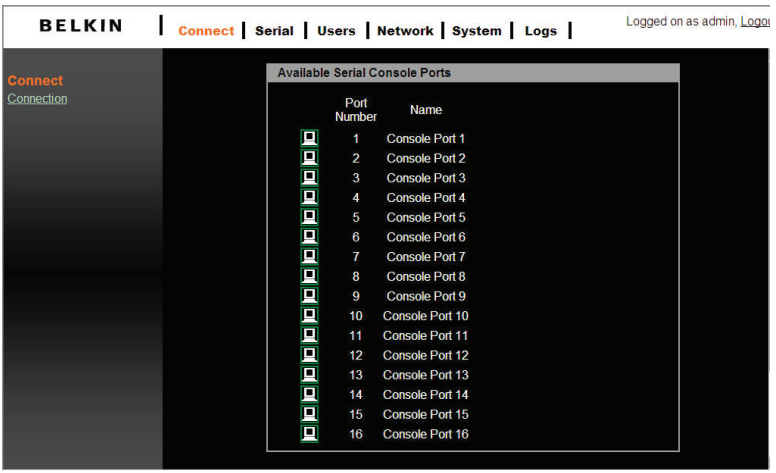
Nom d'utilisateur	Mot de passe
admin	admin

Il y a deux niveaux de privilèges d'accès :

Nom d'utilisateur	Mot de passe par défaut	Privilèges d'accès
admin	admin	Accès complet

L'administrateur peut ajouter ou retirer un utilisateur facilement via les pages Web de l'administration système.

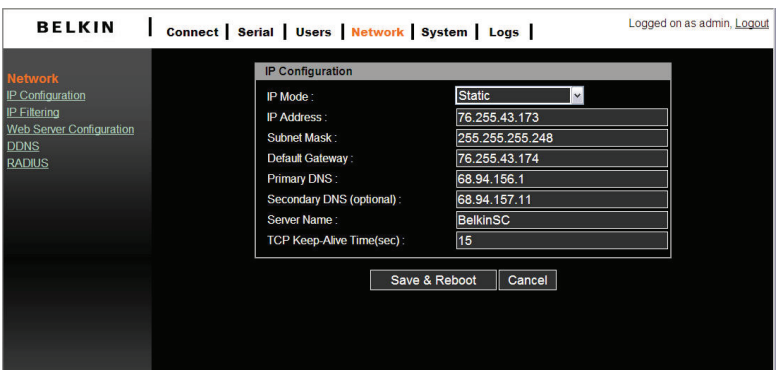
Clique Ouverture de session. L'interface Web s'ouvre à la page « Connecter » (voir ci-dessous).



Page Connexion principale

Etape 3 Configuration de réseau

Cliquez sur « Réseau » pour ouvrir la page de Configuration de réseau (voir ci-dessous).



Page Configuration réseau

Ici vous pouvez affecter une IP statique et d'autres paramètres réseau.

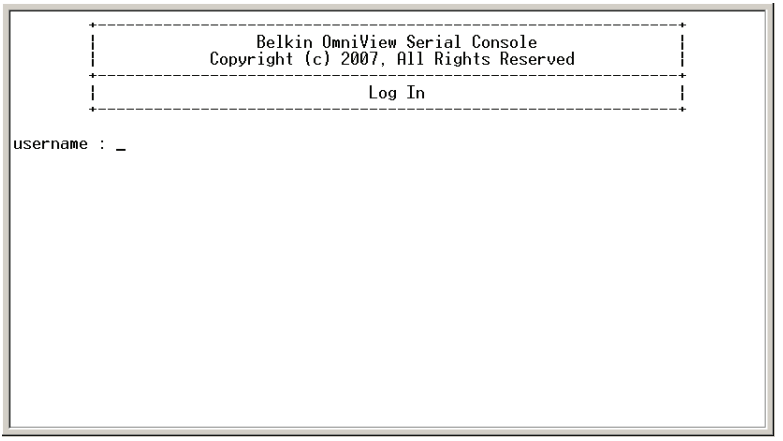
Cliquez sur « Enregistrer et Redémarrer » pour enregistrer tout paramètre de configuration réseau.

Remarque : Si l'usager laisse le navigateur web inactif pendant plus de **30 minutes,** la session de connexion expirera minuterie en mettant fin à la connexion.

Attribution des adresses IP à partir du port de la console--VT-100 (Console, Telnet, SSH)

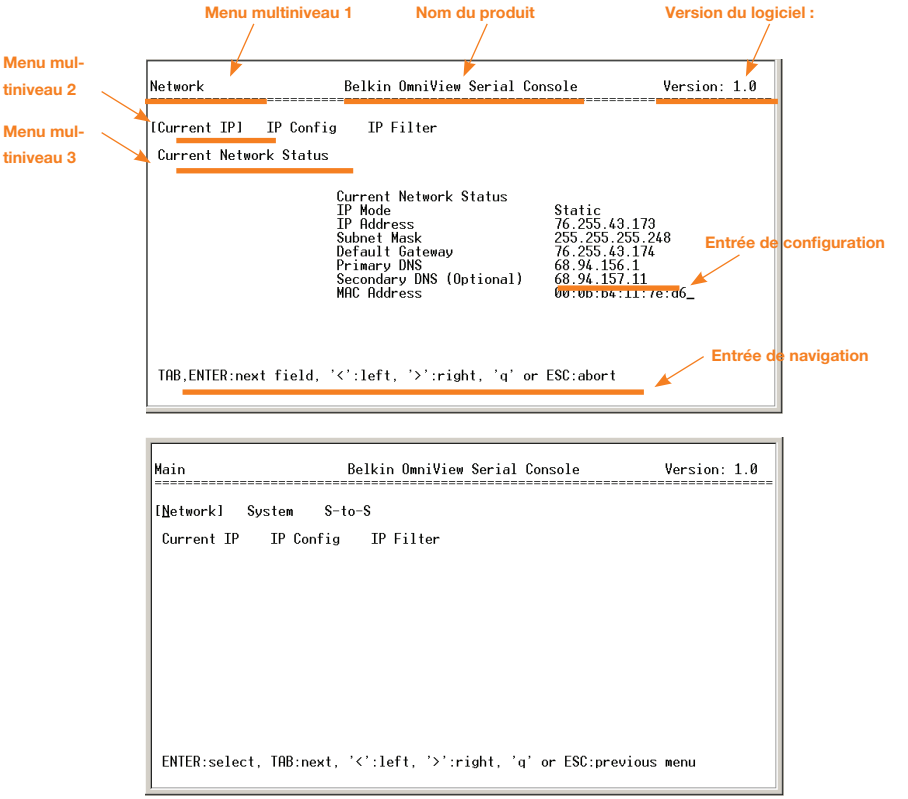
Le serveur de console offre également une interface de ligne de commande conviviale et gérée par des menus. Vous pouvez connecter tout simplement un terminal VT-100 au port local de console pour accéder au serveur de console. Ceci est utile si vous ne connaissez pas les paramètres de réseau du serveur de console et que vous ne pouvez pas y accéder. Le port de la console locale vous permet d'afficher ou de modifier les paramètres (adresse IP, masque de sous-réseau, etc.).

1. Connectez le porte de console situé sur le panneau arrière à un port série sur un hôte PC à l'aide du câble CAT5 et l'adaptateur RJ45/DB9F du porte local de console inclus avec le serveur de console Belkin.
2. Configurez un programme d'émulation de terminal, tel que le HyperTerminal, à l'aide des paramètres suivants :
   - Vitesse baud = 115200
   - Bits d'informations = 8
   - Bits d'arrêt = 1
   - Parité = aucun
   - Contrôle de flux = aucun



Remarque : Les noms d'utilisateur et les mots de passe sont identiques à ceux qui sont définir par l'interface web. Les valeurs par défaut sont « admin/admin ».

La figure suivante illustre la structure d'interface.



La disposition de Menu

Réseau > config d'IP

La page à gauche affiche les éléments de la configuration d'IP.

1. Pour le **mode IP**, vous pouvez actionner la barre d'espacement pour sélectionner le Mode statique ou le Mode DHCP.
2. Pour ce qui est de **l'adresse IP, le masque de sous-réseau, la passerelle par défaut, le DNS principal, et le DNS secondaire**, vous pouvez modifier ces paramètres réseau.
3. Après avoir modifié les paramètres et l'entrée finale, le serveur de console vous invitera à confirmer par un OUI ou un NON. Si vous répondez OUI, le serveur de console redémarrera et sauvegardera les paramètres dans la mémoire flash.

Réseau > IP courant

Pour afficher les paramètres de réseau courants.

Réseau > Filtre IP

Pour activer/désactiver la fonction de filtre IP.

Système > Redémarrage

Pour redémarrer le serveur de console.

Système > Réinitialiser par défaut

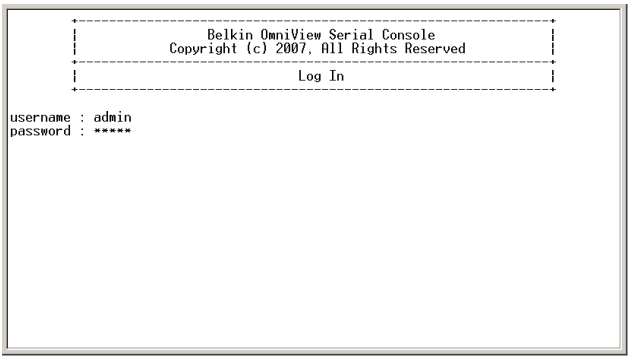
Pour réinitialiser la configuration au paramétrage par défaut de l'usine.
Remarque : Seul l'utilisateur **admin** a le privilège d'exécuter cette fonction.

Système > état

Pour afficher l'état du système.

S-à-S > Sélectionnez le port série à série

Pour activer la connexion entre ports série via le port 16. Reportez-vous à la section « Fonction Série à Série » à la page 34 pour plus de détails.



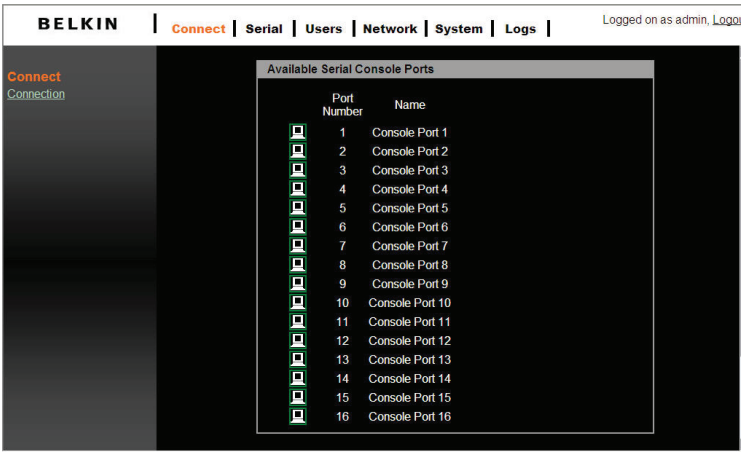
Remarque :
Seulement l'utilisateur **admin** a le privilège de se connecter à VT100. Tous les autres utilisateurs ne sont pas autorisés à effectuer la configuration avec VT-100.

Interface de gestion du navigateur web

Le serveur de console supporte les protocoles HTTP et HTTPS (HTTP sur SSL). Les utilisateurs doivent s'authentifier en se connectant au système avec un nom d'utilisateur et un mot de passe corrects.

Pour accéder aux pages de gestion web du serveur de console, entrez l'adresse IP de l'unité ou le nom d'hôte résoluble dans le champ URL/emplacement du navigateur web. Ceci vous dirigera vers l'écran de connexion.

La figure sur la page suivante montre la page d'accueil de l'interface de gestion web. Une barre de menu s'affiche en haut de la page. Le sous-menu s'affichera le long du côté gauche de la page, et vous permettra de modifier des réglages de paramètre pour l'élément sélectionné en haut de menu.

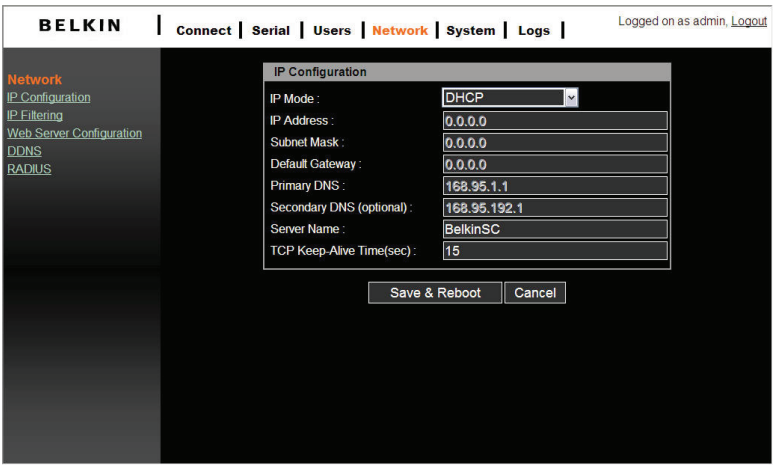


Si disponible, la page permettra à des utilisateurs d'appliquer ou annuler leurs actions. Pour appliquer toutes les modifications, sélectionnez « Appliquer » et les nouvelles valeurs seront appliquées à la configuration. Si vous ne souhaitez pas enregistrer les nouvelles valeurs, cliquez tout simplement sur « Annuler » et toutes les modifications apportées seront supprimées en restaurant les valeurs précédentes.

Vous pouvez configurer les paramètres de réseau IP via VT100 ou l'interface web. Ces parties décrivent la configuration par l'interface web.

Configuration de l'adresse IP :

Le serveur de console exige d'une adresse IP valide pour fonctionner dans l'environnement réseau de l'utilisateur. Si l'adresse IP n'est pas facilement disponible, contactez l'administrateur système en vue d'obtenir une adresse IP admissible pour le serveur de console.



Il y a deux types de bureaux d'attribution d'IP que vous pouvez choisir :

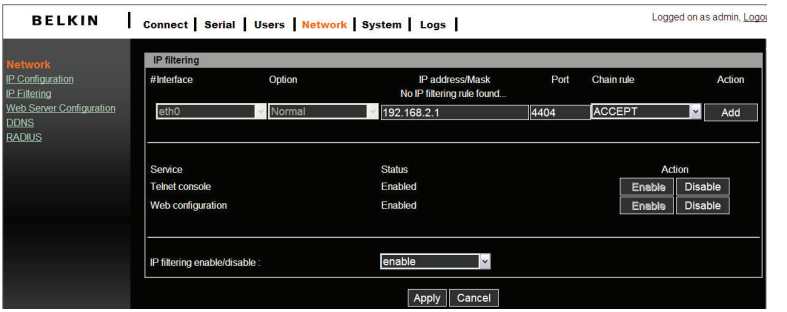
- IP fixe
- DHCP (Dynamic Host Configuration Protocol)

L'unité est livrée avec DHCP définie comme valeur par défaut. Si aucun serveur DHCP n'est présent sur votre réseau, le serveur de console démarrera avec l'adresse IP fixe suivante : 192.168.2.156.

Le nouveau paramètre de configuration IP peut être sauvegardé en cliquant sur « Enregistrer et Redémarrer ».

Filtrage IP

La fonction de filtrage d'IP empêche les hôtes non autorisés d'accéder au serveur de console en spécifiant des règles.



L'adresse IP/masque spécifie les zones de hôte en entrant dans l'adresse IP de base de l'hôte suivie de « / » et du masque de sous-réseau (« / » est un séparateur exigé entre l'adresse IP et le masque de sous-réseau). Les adresses IP d'hôte sont filtrées en fonction de la règle définie.

Le tableau ci-dessous fournit des exemples d'adresse IP/paramètres de masque.

Zones d'hôte spécifiée	Adresse IP de base de l'hôte	Masque de sous-réseau
N'importe quel hôte	0.0.0.0	0.0.0.0
192.168.2.120	192.168.2.120	255.255.255.255
192.168.2.1 ~ 192.168.2.254	192.168.2.0	255.255.255.0
192.168.0.1 ~ 192.168.255.254	192.168.0.0	255.255.0.0
192.168.2.1 ~ 192.168.1.126	192.168.2.0	255.255.255.128
192.168.2.129 ~ 192.168.2.254	192.168.2.128	255.255.255.128

Le « port » est un port ou une plage de port du serveur de console auquel les hôtes tentent d'accéder.

Règle de chaîne

La règle de chaînes détermine si l'accès des hôtes est permis ou non. Elle peut être l'une de deux valeurs :

- **ACCEPTER:** accès autorisé
- **REFUSER :** accès non autorisé

Si le serveur de console reçoit un paquet de TCP, il le traitera avec la règle à chaînes représentée ci-après. L'ordre de processus est important, le paquet passera en premier par la règle de chaîne 1. S'il satisfait à la règle, il agira ; autrement, elle passera à la règle à chaîne 2.

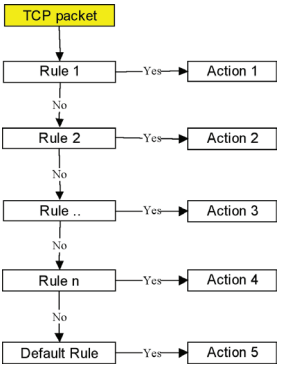
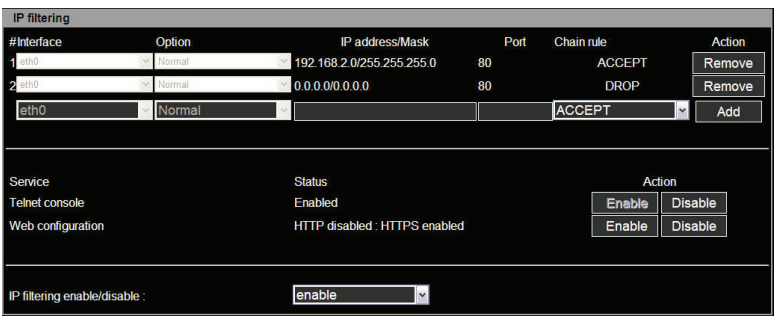


Fig. 4 Règle de chaînes de filtre d'IP

Vous pouvez ajouter une nouvelle règle de filtrage IP en définissant les propriétés dans la ligne d'ajout disponible qui suit. Une fois que la règle est écrite, cliquez sur « Ajouter » pour enregistrer l'action. Vous pouvez retirer une règle en cliquant sur « Retirer ».



Dans l'exemple ci-dessus, les règles sont appliquées dans l'ordre suivant :

#1. Ces hôtes appartenant au sous-réseau 192.168.2.x peuvent accéder au serveur de console (par le port 80 http).

#2. Tous les hôtes ne peuvent pas accéder au serveur de console (par le port 80 http).

Après avoir appliqué ces règle, seuls les hôtes qui appartiennent au sous-réseau 192.168.2.x peuvent accéder au serveur de console (par le port 80 http).

En plus de la règle de chaîne de filtre IP mentionnée ci-dessus, l'interface web fournit également un moyen pratique d'activer/désactiver telnet (port 23) ou le port de configuration web (port 80/443). Ces services sont principalement destinés à la configuration du serveur de console. Cliquer sur « Activer/Désactiver » dans le champ « action » aidera à ajouter/ modifier la règle de chaîne rapidement sans le tracas d'avoir modifier manuellement la règle.

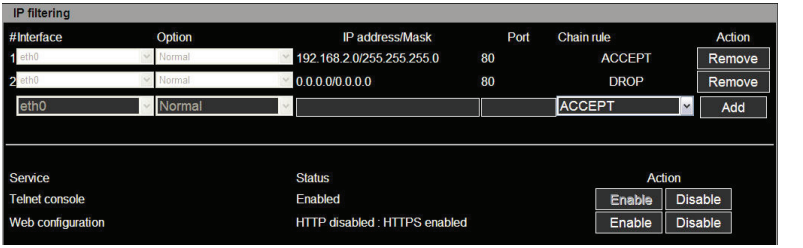
Remarque :
Pour obtenir un meilleur alignement du texte, un client telnet VT-100 est préférable pour l'alignement du texte. PuTTY est l'un de ces clients telnet recommandés qui offrent un meilleur alignement du texte dans l'interface utilisateur. Il est possible de le télécharger sur

Configuration du Serveur d'Impression

Le serveur web du serveur de console prend en charge les protocoles HTTP et HTTPS (HTTP sur SSL) simultanément.
Vous pouvez sélectionner la méthode d'authentification de l'utilisateur pour la connexion web. Le serveur de console fournit actuellement des méthodes d'authentification courante de Local et RADIUS.

Local

Le serveur de console par défaut indique la base de données locale permettant l'authentification de l'utilisateur lors de la connexion au serveur web.



RADIUS et Local

Le serveur de console se rapporte en premier au serveur RADIUS pour le compte utilisateur. Si le compte utilisateur n'est pas trouvé ou que le serveur RADIUS est en panne, les consultations de serveur de console consulter sa propre base de données locale pour trouver le compte utilisateur. L'unité ne permettra pas à un utilisateur de se connecter si l'on ne trouve ni un RADIUS ou ni un compte de base de données locale. Le paramètre de serveur RADIUS peut être configuré par l'utilisateur via la page de configuration du serveur RADIUS. Consultez la page 24.

DNS Dynamique

Si un utilisateur se connecte au serveur de console à une ligne DSL ou utilise une configuration DHCP pour obtenir une adresse IP dynamique du réseau, l'adresse IP pourrait changer. Ceci peut rendre difficile de savoir si une adresse IP a changé, ou quelle est la nouvelle l'adresse IP.

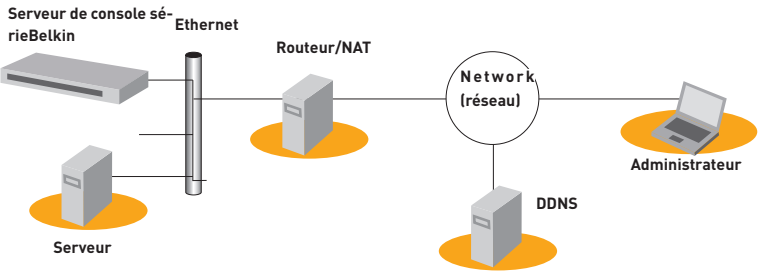
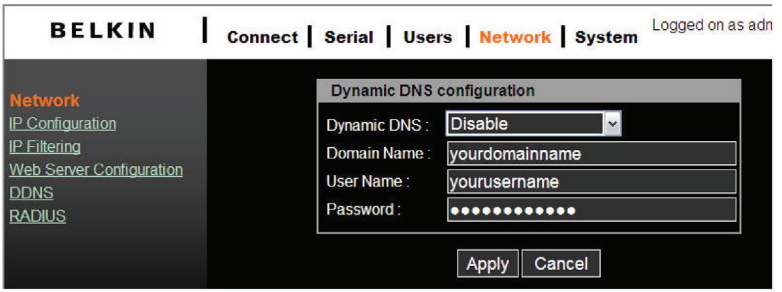


Fig. 5 DNS dynamique

Le service dynamique DNS est fourni par plusieurs ISP et organisations pour s'occuper de cette question. En utilisant un service dynamique DNS, vous pouvez accéder au serveur de console par le nom d'hôte inscrit dans le serveur DNS dynamique quelle que soit la modification d'adresse IP. Par défaut, le serveur de console ne supporte que le service dynamique DNS offert Dynamic DNS Network Services, LLC (www.dyndns.org).

Pour utiliser le service dynamique DNS fourni par des services réseau dynamiques DNS, vous devez configurer un compte dans le CIF (Centre Informations Réseau) de leurs membres - http://members.dyndns.org). Vous pouvez alors ajouter un nouveau lien d'hôte dynamique DNS après avoir une connexion à leur CIF des membres de service réseau dynamique DNS.

Après avoir activé le service dynamique DNS dans le menu Configuration DNS dynamique, vous devez entrer le nom de domaine, le nom d'utilisateur, et le mot de passe enregistrés. Après avoir appliqué la modification de configuration, vous serez en mesure d'accéder au serveur de console uniquement avec le nom de domaine. Le DNS (système de nom de domaine) est le service d'internet qui traduit des noms de domaine en adresses IP.



Remarque :
Le champ du nom de domaine nécessite un Qualified Domain Name (FQDN), et non pas simplement un nom d'hôte enregistré.

RADIUS

L'authentification est le procédé d'identification d'une personne, habituellement sur la base d'un nom d'utilisateur et d'un mot de passe. Le serveur de console supporte plusieurs options d'authentification, telles que les « Local » et « RADIUS », pour authentifier les utilisateurs qui accèdent au port série. Si l'authentification est définie sur « Local », l'unité utilisera sa propre liste des utilisateurs pour en authentifier un. Si configuré autrement, le serveur de console demandera l'authentification des serveurs d'authentification externes (c.-à-d., RADIUS). La figure ci-dessous illustre conceptuellement le processus d'authentification de l'utilisateur à l'aide d'un serveur externe d'authentification.

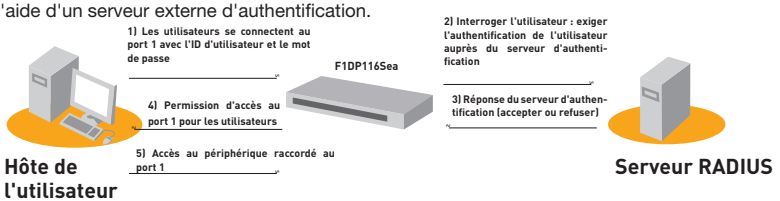
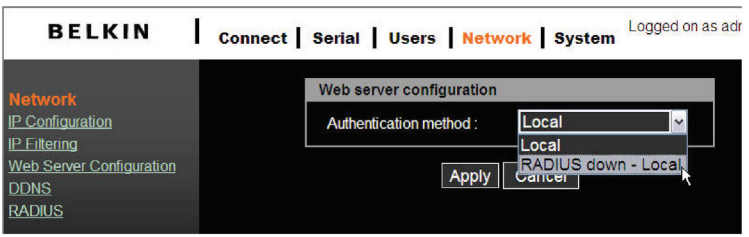
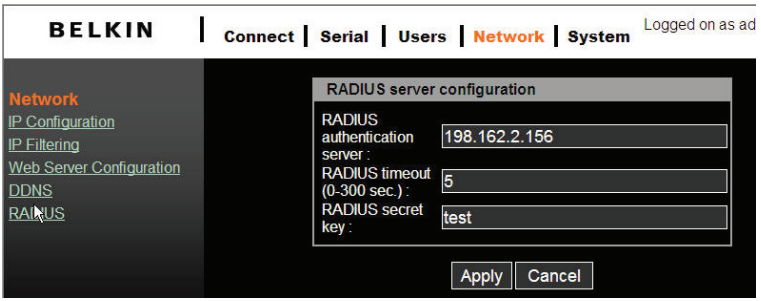


Fig. 6 RADIUS



Configuration du Serveur RADIUS



Remarque :
Pour que le service RADIUS puisse être utilisé, un serveur RADIUS doit avoir été

HTTPS/SSL

Le serveur de console supporte les services HTTP et HTTPS (HTTP sur SSL) simultanément. Vous pouvez activer ou désactiver la fonction de sécurité de chaque port individuellement.

HTTPS fournit une interface web sécurisée et cryptée via SSL (secure sockets layer).

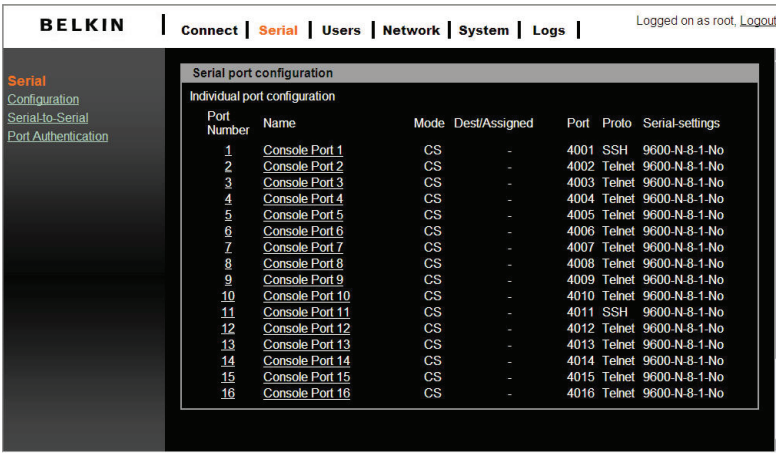
Les étapes suivantes doivent être utilisées pour le protocole HTTPS :

1. Changez l'URL de « http://xxx.xxx.xxx/ » en « https://xxx.xxx.xxx/ ».
2. Une fois la connexion établie, votre navigateur affichera une icône de « Verrouillage ».

Double-cliquez sur le symbole de verrouillage pour afficher les informations de certificat détaillées.

Configuration

Sous l'en-tête de menu « Série », cliquez sur « Configuration » pour afficher le récapitulatif des ports.

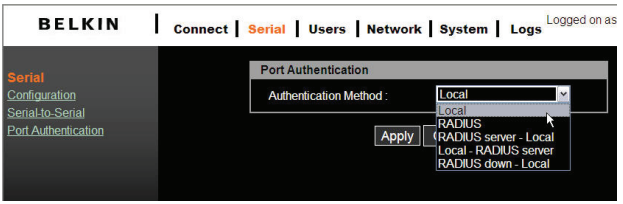


Notez que si le « Port série » est désactivé, le panneau « Configuration de port série » affichera le port dans une police grise foncée. Un port série activé sera affiché avec une police blanche en gras.

Authentification de port

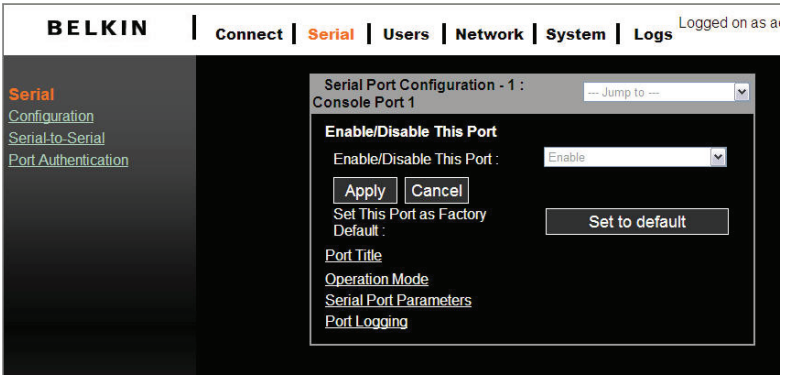
L'authentification est le procédé d'identification d'une personne, habituellement sur la base d'un nom d'utilisateur et d'un mot de passe. Le serveur de console supporte plusieurs options d'authentification, telles que les « Local » et « RADIUS », pour authentifier les utilisateurs qui accèdent au port série. Consultez la page 23.

Si l'authentification est définie sur « Local », le serveur de console utilisera sa propre liste des utilisateurs pour en authentifier un. Si configuré pour RADIUS, l'unité demandera l'authentification des serveurs d'authentification externes (c.-à-d., RADIUS). La figure ci-dessous illustre conceptuellement le processus d'authentification de l'utilisateur à l'aide d'un serveur externe d'authentification.



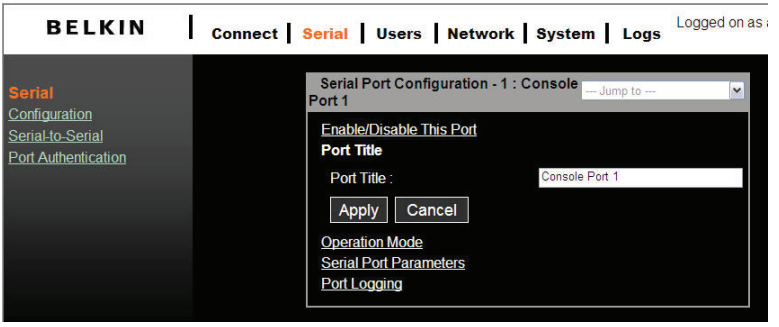
Activer/Désactiver le port

Chaque port série peut être individuellement activé ou désactivé. Un port série désactivé n'est pas accessible à l'utilisateur. Les utilisateurs peuvent réinitialiser le port série aux paramètres par défaut en cliquant sur le bouton « Définir à la valeur par défaut ».



Titre de port

Les utilisateurs peuvent écrire des informations descriptives pour chaque port en se basant sur le périphérique relié à ce dernier.



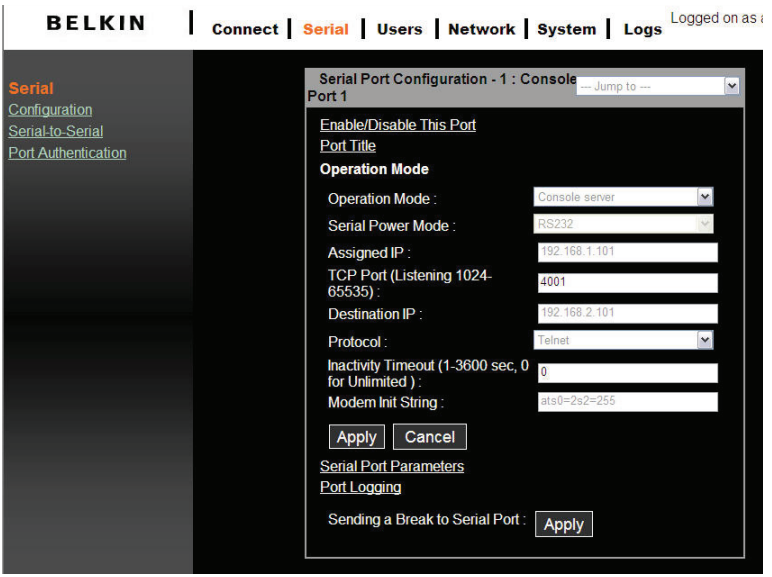
Nous pouvons utiliser le raccourci, « --Sauter à-- », dans le coin en haut à droite pour sélectionner et configurer un autre port.

Modes de fonctionnement

L'unité de serveur de console fournit quatre types de mode d'intervention. Ces derniers sont décrits ci-dessous.

Remarque :

- Le dernier port (par ex. le port 16) peut être utilisé comme « ESP externe » (Entry Serial Port - port série en entrée) en mode de fonctionnement « série à série ». Consultez la section « Fonction série à série » pour de plus amples informations.



Mode serveur de console

Configurer un port série comme serveur de console crée une prise de TCP sur l'unité qui écoute un lien de telnet ou d'utilisateur SSH. Quand vous vous connectez à la prise de TCP, vous avez accès au périphérique fixé au port série comme si le périphérique avait été connecté directement au réseau. Des flux de données peuvent être envoyés dans les deux sens entre le périphérique et le programme client telnet/SSH. RawTCP est également supporté avec le mode serveur de console.

Les paramètres suivants sont configurables en mode serveur de console :

Numéro d'écoute de port TCP
Vous pouvez également accéder à un port série par l'adresse IP du serveur de console et le numéro de écoute de port TCP du port série.

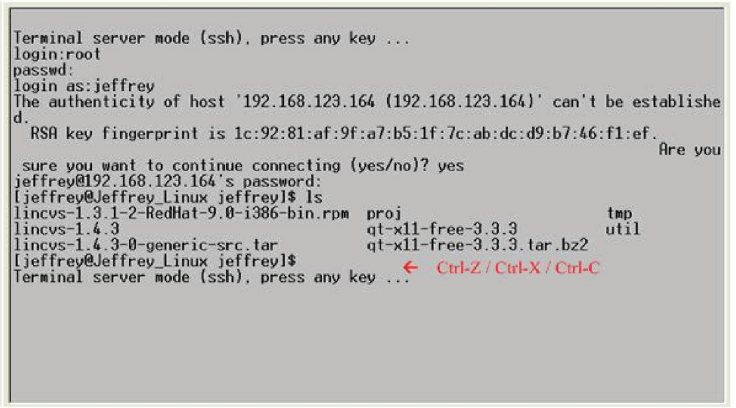
Si l'adresse IP du serveur de console et le port série sont affectés comme 192.168.123.100 et que le numéro de écoute de port TCP est 4001, l'utilisateur peut le connecter au port comme suit : telnet 192.168.123.100 4001

Protocole
Sélectionnez « Telnet », « SSH », ou « TCP brut » comme protocole. Si les utilisateurs utilisent un programme client telnet, sélectionnez « Telnet ». Si les utilisateurs utilisent un programme client SSH, sélectionnez « SSH ». Si le « TCP brut » est sélectionné, la communication directe de la prise TCP est disponible entre le serveur de console et l'hôte distant.

Temporisation d'inactivité
Activez cette fonction pour éviter qu'un client reste sur une connexion TCP s'il n'y a pas eu d'activité sur un port série pendant une longue période de temps. Si la « temporisation d'inactivité » est activée, et qu'il n'y a aucune activité de données entre le serveur de console et le client Telnet/SSH pendant l'intervalle spécifique de temporisation d'inactivité (c.-à-d., aucune activité de données par le port série), la session TCP existante sera automatiquement fermée. Si vous voulez conserver la connexion indéfiniment, configurez la temporisation d'inactivité à « 0 ».

Entretien TCP (aucune configuration requise)
Pour éviter le verrouillage de la connexion TCP, le serveur de console continuera à vérifier l'état de la connexion entre le client telnet/SSH et le serveur de console en envoyant périodiquement des paquets d'« entretien ». Si le client telnet/SSH ne répond pas aux paquets, le système supposera l'arrêt de la connexion. Le serveur de console fermera alors la connexion telnet/SSH existante, quel que soit l'inactivité réglée. Ceci empêchera la connexion TCP de se verrouiller si une application n'est pas bien fermée ou que le lien de réseau est coupé.

Mode serveur de terminal
En mode serveur de terminal, le port série du serveur de console est configuré pour attendre des données du périphérique connecté au port. Si des données sont trouvées, le serveur de console initiera une session TCP comme client telnet ou SSH à un serveur prédéfini. Le serveur doit être défini par des utilisateurs avant que le port puisse être configuré pour un client telnet ou SSH. Ce mode peut être utilisé pour accéder aux serveurs d'accès sur le réseau à partir d'un terminal de série. RawTCP est également supporté avec le mode serveur de terminal.



Afin de mettre fin à une session telnet/SSH/RawTCP en mode de serveur de terminal, vous pouvez utiliser ces trois séquences de touches de contrôle (Ctrl-Z / Ctrl-X / Ctrl-C).

Mode modem accès distant

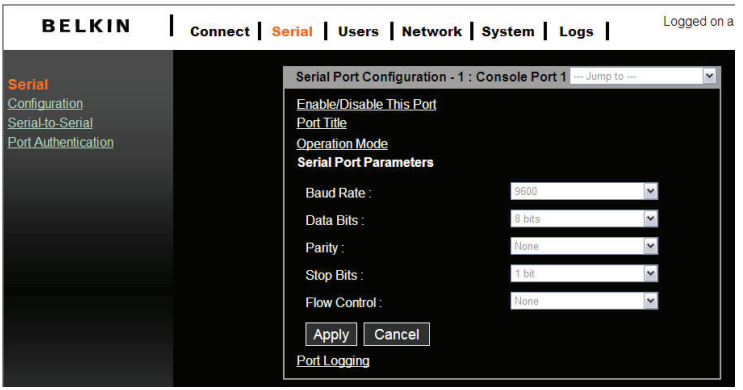
Avec ce mode, le serveur de console suppose le raccordement d'un modem externe au port série en attente d'une connexion d'appel entrant provenant d'un site distant. Si un utilisateur effectue un appel entrant à l'aide d'une application de terminal, le serveur de console acceptera la connexion et affichera l'invite ou le menu approprié pour l'utilisateur qui vient de se connecter.

Mode série à série

Pour plus de détail sur ce mode, reportez-vous à la section « Fonction série à série » à la page 34 pour des groupes pour ce mode.

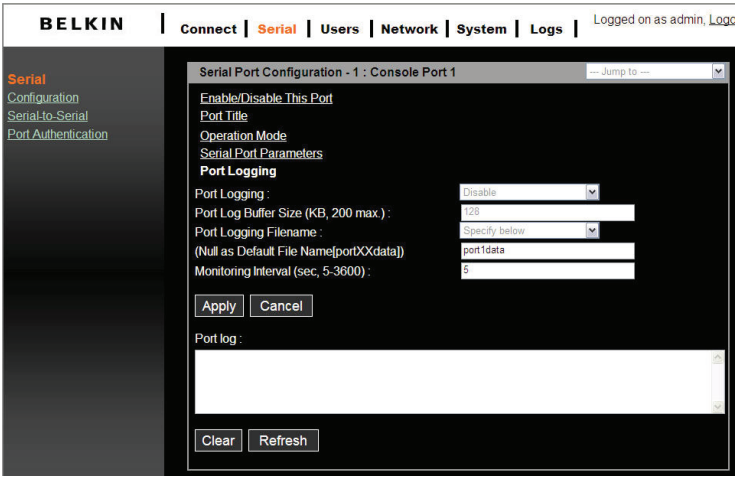
Paramètres du port série

Pour connecter le périphérique série au port série du serveur de console, les paramètres de son port série doivent répondre parfaitement aux exigences du périphérique série relié.



Connexion du port

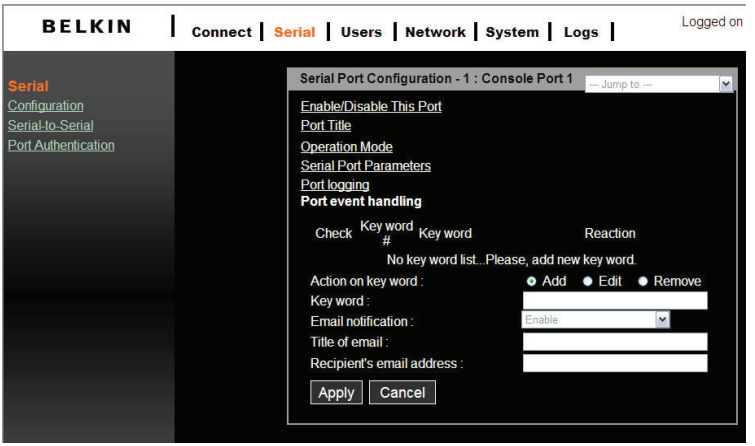
En mode serveur de console, les données reçues du port série de navigation seront bufférisées dans la mémoire de l'unité.



La fonction « Connexion de port » n'est valide et visible seulement que si le mode de fonctionnement du port série est configuré sur le mode de serveur de console.

Si l'option « Connexion de port » est activée, l'usager peut faire chercher au serveur de console un mot clé défini à partir des données de connexion de port et envoyer un e-mail à un administrateur par les configurations de « Réception d'événement de port ». Chaque réaction peut être configurée individuellement sur chaque mot clé. La réaction peut être fournie par un e-mail.

Cliquez sur « Réception d'événement de port ».



La taille de tampon mémoire pour des données de connexion est de 192K par port. Si les données de connexion se développent plus que la capacité de stockage, les nouvelles données recouvriront les données précédentes.

Fonction Pause

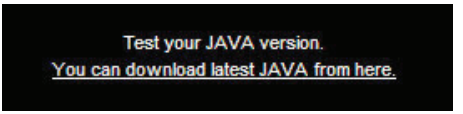
En mode de serveur de console, le serveur est capable d'envoyer des signes de « interruption » à un périphérique série connecté. Une interruption est parfois utilisée pour réinitialiser une ligne de communication ou pour changer le mode du matériel de communication, comme par exemple un MODEM. Certains périphériques cibles, tels qu'un serveur Sun™ Solaris™, exigent un caractère nul (interruption) pour générer un signal « OK ». L'effet d'« envoyer une interruption par le port série » équivaut à établir un « STOP-A » à partir d'un clavier Sun. Afin d'envoyer une interruption à un périphérique de série, configurez-le en mode « Serveur de console » et utilisez « Telnet » ou « RawTCP » comme protocole. Cliquez sur le bouton « Appliquer » pour envoyer un signal de rupture au port série désigné et puis à l'ordinateur ou au serveur relié.

Connexion

Le serveur de console fournit l'accès basé sur le web à un périphérique série cible sans faire appel à un programme client telnet indépendant. Ceci se fait à travers un applet Java.

Un applet Java est utilisé pour fournir l'interface utilisateur basée sur le texte et accéder au port série. Cet applet Java ne supporte que le telnet en mode serveur de console. L'utilisateur ne peut pas accéder au port série via le Web si le mode hôte du port est défini sur la connexion RawTCP. L'utilisateur est invité à entrer l'ID d'utilisateur et le mot de passe pour accéder au port. Une fois authentifié, l'utilisateur peut désormais accéder au port série.

Utilisez l'hyperlien situé au bas de la Page Connecter pour tester votre compatibilité Java. Ou utilisez le lien ci-dessous pour télécharger la dernière version de Java.



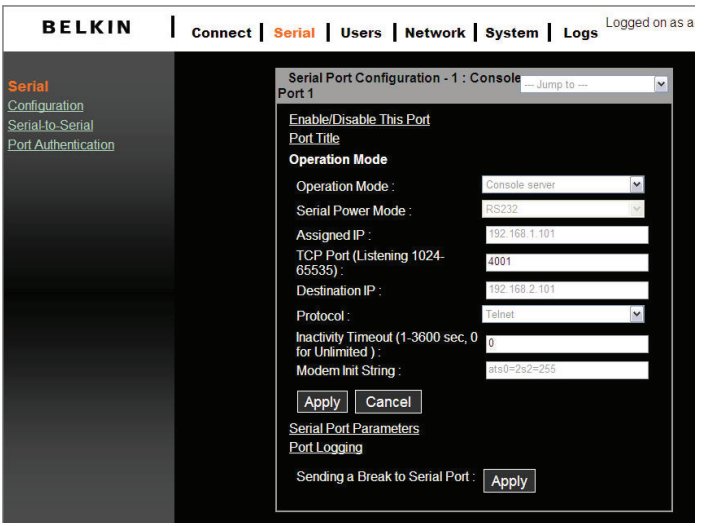
Assurez-vous d'activer l'option du support Java de votre navigateur et vérifiez également votre version d'environnement Java Runtime (connue sous le nom de version JRE). Vous aurez besoin de la version 1.6.0 ou ultérieure si vous nécessitez également le service de HTTP sécurisé (HTTPS).

Remarque :

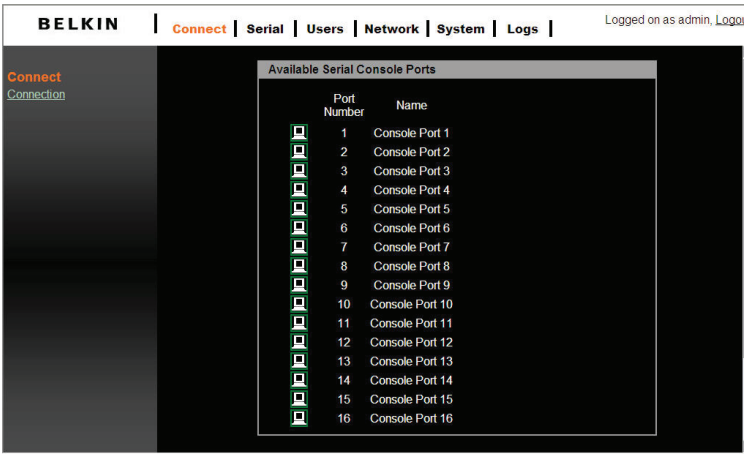
- Pour exécuter cette fonction, l'installation de JRE version 6.0 ou version ultérieure est requise par le système. Le logiciel Java est disponible sur http://www.java.com/en/download/.

Applet Java Telnet

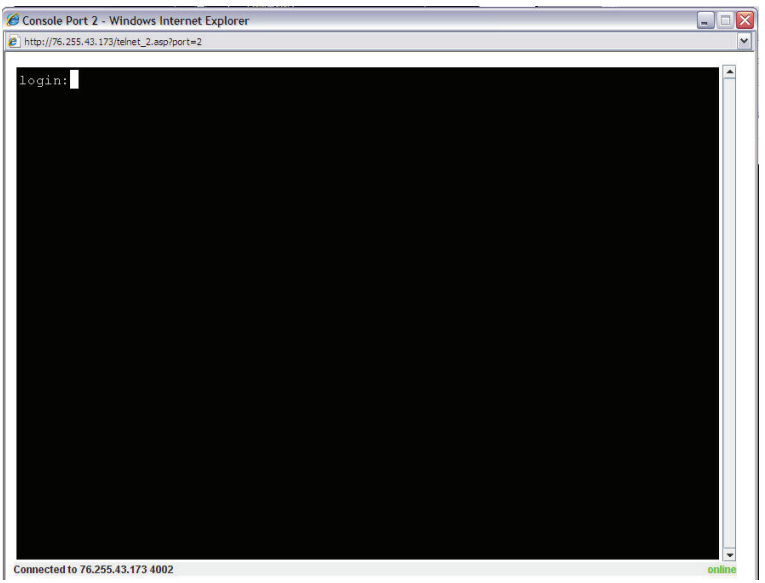
1. Sélectionnez le protocole telnet sous “Série > Configuration > Mode de fonctionnement”.



Sélectionnez « Connecter » dans le menu principal et cliquez sur l'icône du terminal à gauche. L'application d'émulation du terminal affichera dans une nouvelle fenêtre contextuelle et vous invitera à ouvrir une session. Si vous voyez une fenêtre vide, examinez votre système pour vous assurer de la compatibilité de la version Java.



2. Entrez le nom d'utilisateur et le mot de passe pour vous connecter, ainsi vous pouvez commencer à l'utiliser comme si vous lanciez un programme client telnet (par exemple, programme Telnet DOS, PuTTY).



Remarque : Le nom du port série actif apparaîtra sur la barre de fenêtre. Un indicateur d'état de connexion apparaîtra également en bas à droite de la fenêtre.

Fonction série à série

La fonction série à série vous permet d'utiliser un périphérique terminal simple (affichage vidéo et clavier) pour accéder et commander tout périphérique connecté au serveur de console sur les ports 1 à 15. Vous pouvez également utiliser un convertisseur terminal externe, comme le Belkin F1D084Eea, pour connecter votre serveur de console à un switch KVM et pour consolider la commande.

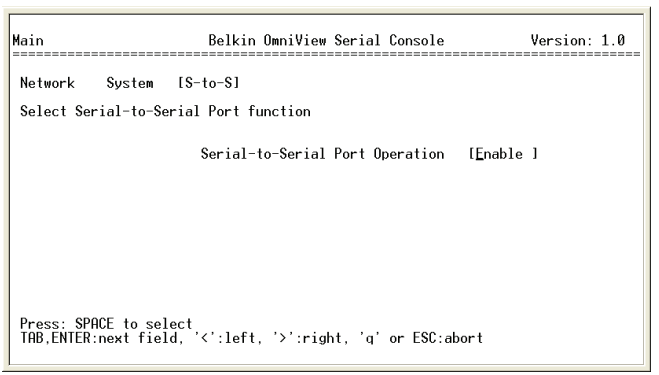
Installation

Pour installer, connectez votre périphérique terminal au port 16 du serveur de console. Ceci vous permettra d'accéder à un périphérique série connecté aux ports 1 à 15 seulement.

Activation et configuration série à série

Pour configurer la fonction série à série :

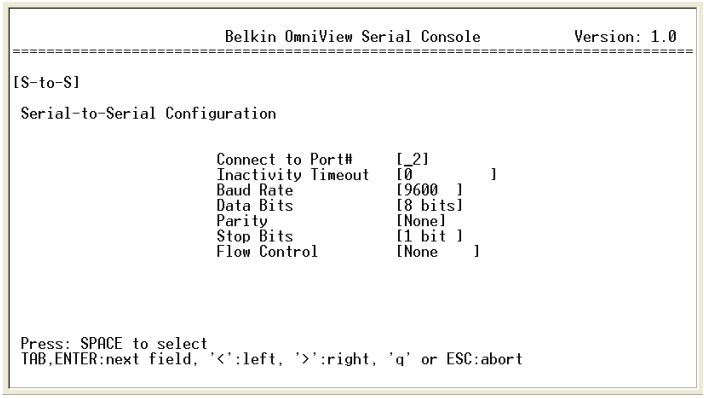
1. Entrez le mode de console de VT100 (voir « Attribution IP à partir de la section port de console Port-VT-100 (console, Telnet, SSH) » pour plus de détails) pour afficher l'écran de fenêtre.
2. Allez à l'option de menu multiniveau 2 [S-à-S] « fonctionnement de port Série à Série », et appuyez sur la barre d'espacement pour sélectionner « ACTIVER ». Confirmez la modification pour redémarrer automatiquement le système.



3. Déconnectez-vous à présent de la console locale et commencez une nouvelle session de terminal par la connexion au port 16.
4. Après le redémarrage (qui prendra environ une minute), l'écran illustré à la page suivante s'affiche. Configurez chaque paramètre de configuration. Tapez la valeur de la « Temporisation d'inactivité » et appuyez sur la barre d'espacement pour sélectionner le paramètre pour les autres éléments.

Remarque :

- Pour afficher l'écran de configuration série à série suivant, la fonction série à série doit avoir été activée. Le débit en bauds est fixé à 9600 8N1 (non modifiable) afin d'obtenir une meilleure compatibilité avec les dispositifs d'affichage terminal de tiers.



5. Choisissez le numéro de port auquel vous souhaitez effectuer la connexion et l'écran ci-dessous apparaîtra.

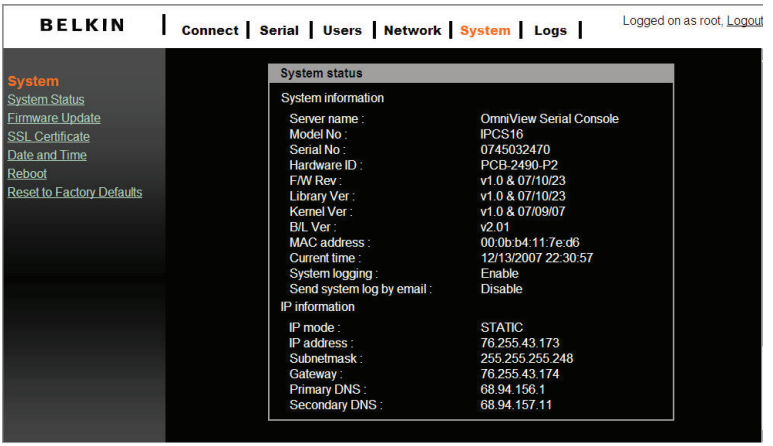
6. Tapez le nom d'utilisateur et le mot de passe. La connexion de canal de données entre le port 16 et le port série sélectionné sera établie, de manière à ce que l'administrateur puisse contrôler le périphérique série ou le serveur.

7. Appuyez sur les touches « Cntl » et « C » pour sortir de la fonction série à série retourner à l'écran principal de la console.

La page Web donne également des paramètres en lecture seule de la fonction série à série ; elle changera automatiquement selon la modification du paramètre sur la console VT100. Cliquez sur « Annuler » pour rafraîchir les valeurs.

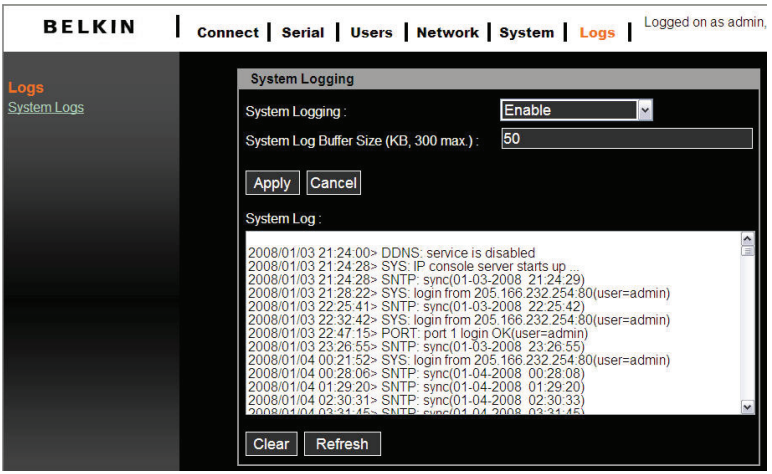
État du système

La page « Etat du système » indique les informations de système courant telles que le nom, le numéro de série, les versions de micrologiciel, l'adresse MAC, l'heure actuelle, et les paramètres de réseau. Les données ne peuvent pas être modifiées à partir de cette page. Cette page se rafraîchit automatiquement toutes les 10 secondes.



Connexion au système

Vous pouvez activer ou désactiver le processus de connexion de système et définir taille du tampon de connexion. La valeur par défaut du tampon de connexion de système est de 50 Ko et peut être affectée jusqu'à 300 Ko maximum. Si les données de connexion se développent plus que la taille du tampon affectée au préalable, les nouvelles données recouvriront les données précédentes.



Les événements de système suivants sont connectés à un stockage volatile cycliquement :

i) SYS (démarrage du système, minuterie au ralenti, authentification de compte de connexion)

ii) SNTP (synchronisation temporelle réseau)

iii) JOURNAL (effacer journal d'événements de système)

iv) PORT (authentification d'accès de port série)

v) DDNS (événement d'adresse IP dynamique de registre)

Administration utilisateur

Au démarrage, le système invitera l'utilisateur à entrer le mot de passe pour accéder au système. L'administrateur peut ajouter ou retirer un utilisateur facilement via les pages Web. Il y a deux niveaux de privilèges d'accès :

Nom d'utilisateur	Mot de passe par défaut	Privilèges d'accès
admin	admin	Accès complet
(définir utilisateur)	(définir utilisateur)	Il ne peut accéder qu'au « Port série » et à l'« Etat de système »

Une page « Refus d'accès » s'affichera si l'utilisateur n'est pas autorisé accéder à la page web.

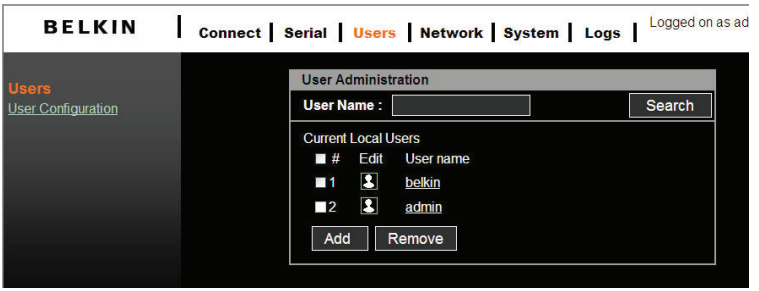
Ajout d'un utilisateur

Pour ajouter un utilisateur :

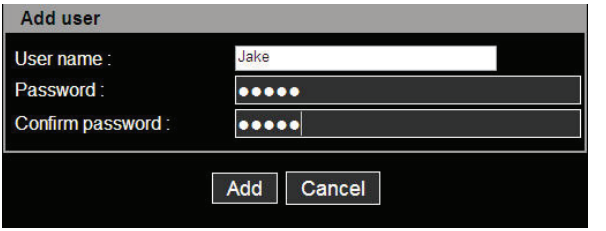
- Vérifiez les utilisateurs sur l'écran « Administration utilisateur ».
- Cliquez sur le bouton « Ajouter ».
- Tapez le nouveau nom d'utilisateur et le mot de passe.

Directives pour le nom d'utilisateur et mot de passe requis

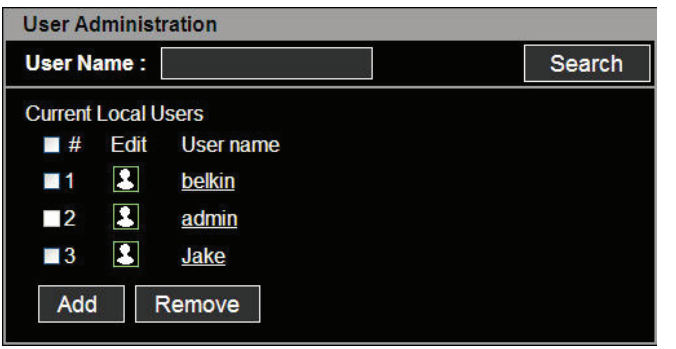
- Le premier caractère du nom d'utilisateur doit être une lettre d'alphabet.
- Le mot de passe doit être d'au moins trois caractères.
- Le nom d'utilisateur ou le mot de passe ne doit pas contenir plus que 32 caractères.
- Seul un utilisateur « admin » peut accéder au « Réseau » et au « Système d'administration ».



La figure ci-dessous affiche l'écran « Ajout d'un utilisateur ».



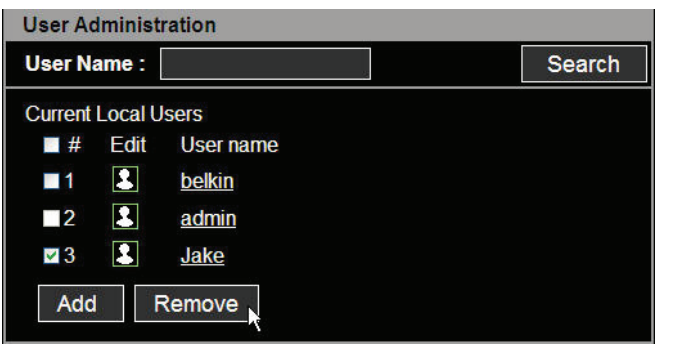
Le nouvel utilisateur apparaîtra maintenant dans la liste « Nom d'utilisateur ».



Suppression d'un utilisateur

Pour supprimer un utilisateur :

- Vérifiez les utilisateurs sur l'écran « Administration utilisateur ».
- Cliquez sur le bouton « Supprimer »



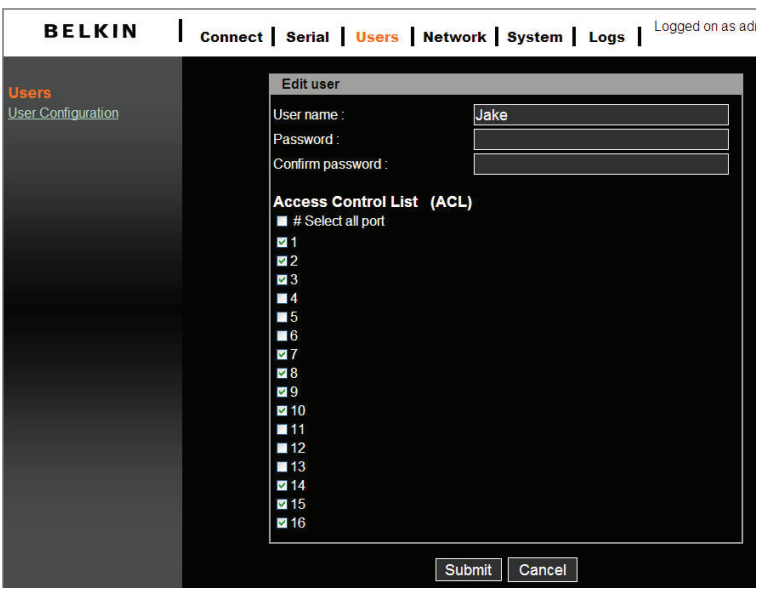
Modification de la Control Access list (ACL)

Le serveur de console fournit la sécurité ACL (Access Control List) où vous pouvez spécifier l'accès utilisateur discrètement par différents ports seulement, au lieu d'indiquer tous les ports.

Pour modifier l'ACL :

- Vérifiez les utilisateurs sur l'écran « Administration utilisateur ».
- Cliquez sur l'icône « Modifier ».
- Entrez le nom d'utilisateur et le mot de passe.
- Sélectionnez le port auquel vous souhaitez accéder.
- Cliquez sur le bouton « Envoyer ».

Une fois que le compte utilisateur ACL est défini, les utilisateurs peuvent accéder ou apporter des modifications de configuration uniquement aux ports série autorisés. Les utilisateurs ne seront pas en mesure de voir ou de configurer les ports série non autorisés.



Modification du mot de passe

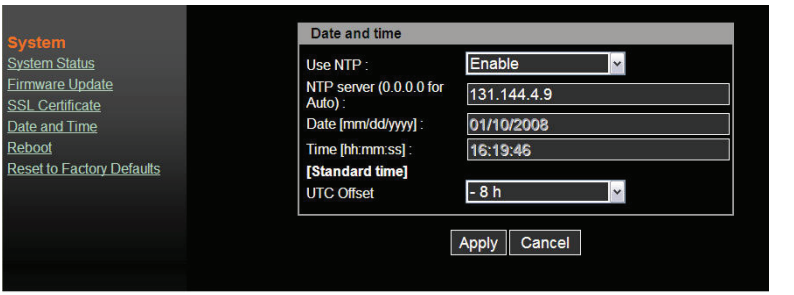
Pour modifier les paramètres du compte utilisateur, ouvrez l'écran « Modifier l'utilisateur » en sélectionnant le nom d'utilisateur dans l'écran de « Configuration utilisateur » et en modifiant les paramètres du compte utilisateur tels qu'ajouter un utilisateur.

Date et heure (NTP)

Le serveur de console met à jour les informations relatives à la date et à l'heure du jour. Les paramètres d'horloge et de calendrier sont enregistrés grâce à une batterie interne. L'utilisateur peut changer la date du jour et l'heure.

Deux options sont disponibles pour programmer la date et l'heure : La première option consiste à permettre au serveur NTP de garder les paramètres de la date et de l'heure. Si la fonction NTP est activée, le serveur de console obtiendra les informations concernant la date et l'heure du serveur NTP à chaque redémarrage, puis il s'aligne automatiquement par rapport au temps de serveur NTP toutes les heures. Si le serveur NTP est défini à 0.0.0.0, le serveur de console utilisera automatiquement les serveurs NTP par défaut. Dans ce cas-ci, il devrait être connecté du réseau à Internet. La deuxième méthode consiste à définir la date et l'heure manuellement sans utiliser le serveur NTP. Dans ce cas-ci, les informations concernant la date et l'heure sont stockées grâce à la batterie interne de secours.

Par convention, les météorologistes utilisent un fuseau horaire, GMT (GMT). Ce fuseau est également connu comme fuseau universel (UTC). Vous pouvez définir le fuseau et le décalage horaire de l'UTC selon l'emplacement de l'utilisateur pour programmer la date et l'heure du système avec précision, et le décalage horaire de l'UTC. La valeur « x » de « décalage horaire » peut être un nombre entier positif ou négatif. Reportez-vous au site Web http://time_zone.tripod.com/ pour le décalage horaire de l'UTC.



Remarque :

- Le serveur de console offre une fonction d'HTR (horloge temps réel) alimentée par une pile au lithium (CR2032, 3 V). Ainsi, la date et l'heure seront conservés même si l'unité subit une panne de courant.
- Si vous perdes les informations relatives à la date et l'heure de façon répétée, veuillez replacer
  la pile.
- Remplacez la pile CR2032 de 3 V avec une pile identique ou de type équivalent recommandé par le fabricant de la pile. Une nouvelle pile peut exploser si elle est installée de façon inadéquate. Jetez les piles usagées conformément aux consignes

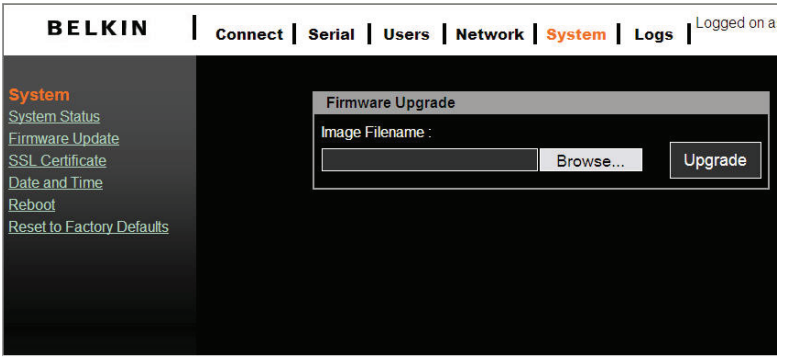
Mise à niveau du micrologiciel

Le micrologiciel peut être facilement mis à niveau via une page Web. Cette section décrit les procédures de mise à jour.

La dernière version de micrologiciel est disponible chez www.belkin.com/support.

Mise à niveau à partir de l'interface web

Reportez-vous à la page web « Système > Mise à niveau du micrologiciel ».

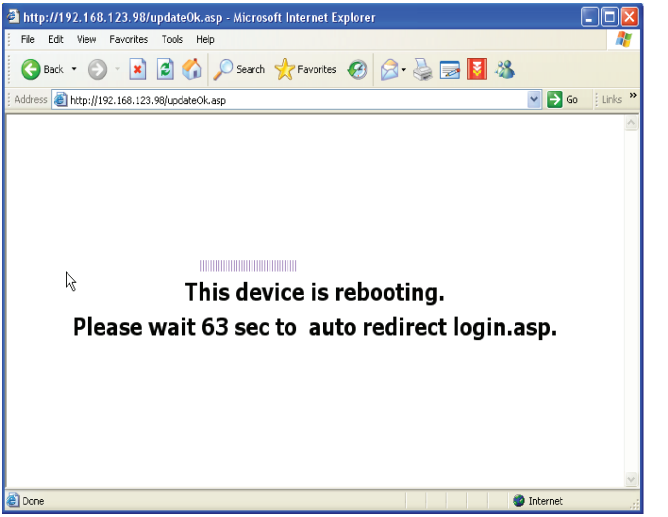


Cliquez sur « Parcourir » pour rechercher le fichier de micrologiciel dans la fenêtre de l'explorateur. Naviguez dans votre PC et sélectionnez le fichier de micrologiciel. Cliquez sur « Ouvrir » pour confirmer votre choix.

Une fois que le fichier de micrologiciel approprié est sélectionné, cliquez sur « Mettre à niveau » pour commencer le processus de mise à niveau du micrologiciel. L'interface web affichera la barre de progression pour indiquer le déroulement du transfert des fichiers. En même temps, le port LED sur le panneau avant clignotera également en série pour indiquer que la procédure de mise à niveau est en cours.

Avertissement !!! NE PAS débrancher l'alimentation ou le câble Ethernet pendant ce processus de mise à jour. Faire ainsi peut entraîner un échec de mise à niveau et détruire l'image dans la mémoire.

Le serveur de console commencera automatiquement un redémarrage à la fin de l'opération de mise à niveau pour activer le nouveau micrologiciel. Une fois que le compteur expire, le navigateur vous redirigera vers la page d'accueil pour la connexion. Vous pouvez vous reporter à la page « Etat de système » pour vérifier la version de micrologiciel et pour confirmer l'opération de mise à niveau.

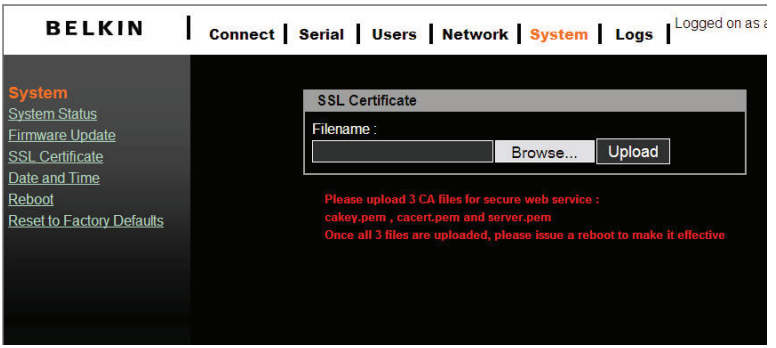


SSL Certificate [Certificat SSL]

Un certificat SSL est une identification numérique qui contient les informations attestant que le certificat appartient à une personne, une entreprise, au serveur, ou à toute autre entité marquée dans le certificat. Le serveur de console supporte le HTTP sécurisé (https) pour apporter la modification de configuration via la page Web. Le certificat SSL côté serveur identifie le serveur de console de sorte que vous puissiez compter sur le certificat et apporter la modification de configuration en toute confiance.

Le serveur de console est capable de télécharger les fichiers de certificat personnalisés sur le serveur web. La suite de certificat comprend trois fichiers (cacert.pem, cakey.pem, et server.pem). Chacun des trois fichiers de certificat sera téléchargé pour compléter la mise à niveau de certificat. L'interface de téléchargement de fichier est semblable à la mise à niveau du micrologiciel.

Une fois que tous les fichiers de certificat sont téléchargés, les utilisateurs commenceront une commande de redémarrage manuellement pour rendre le nouveau certificat efficace.



Parcourez les dossiers préparés CA (suivez la procédure décrite à l'annexe E pour préparer correctement les trois fichiers CA avec les mêmes noms de fichiers attribués), et téléchargez ces fichiers sur le serveur de console. Veuillez vérifier une deuxième fois chaque fichier avant de télécharger. Une mauvaise suite de fichier CA peut désactiver la fonction HTTP.

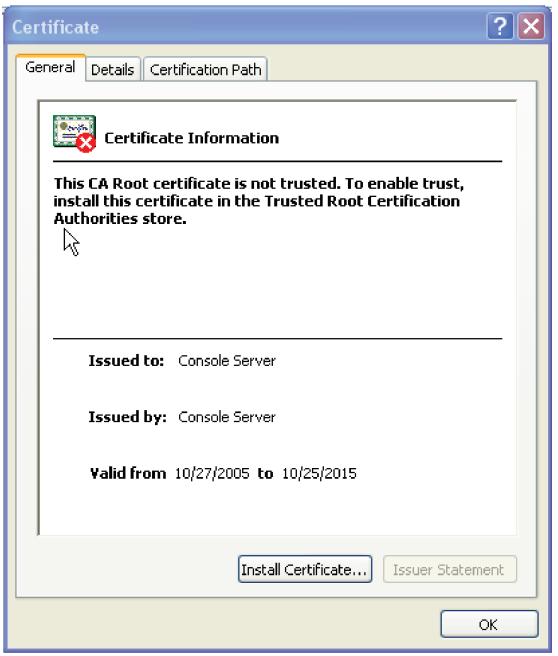
Remarque :

- Si les fichiers CA sont endommagés, l'utilisateur peut faire un retour en arrière sur les fichiers CA pour restaurer les paramètres par défaut d'usine, en sélectionnant « System > Reset to Factory Defaults ». Les anciens fichiers CA seront restaurés.
- Parce que la longueur du chemin d'accès au fichier CA est limitée (256 caractères), nous vous recommandons de placer tous vos fichiers sous « C:\upgrade » pour en

Certificat HTTP sécurisé

Un service web de serveur de console sécurisé est lancé par la connexion https du navigateur (port de service 443). Le navigateur vous alertera avec une alarme de sécurité pour vous avertir du certificat. Vous devez accepter le certificat pour démarrer le service web. Les utilisateurs peuvent choisir d'« Afficher le certificat » et de le justifier si le serveur web connecté est digne de confiance.

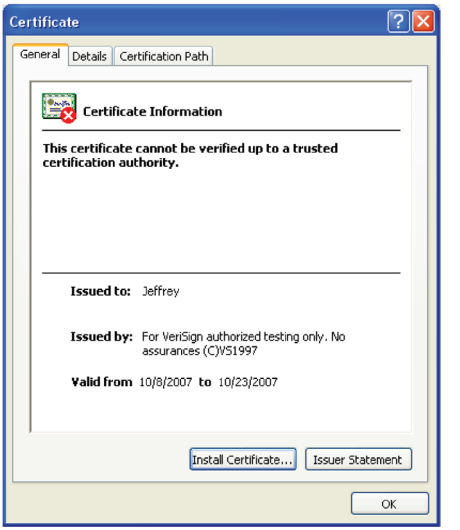

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

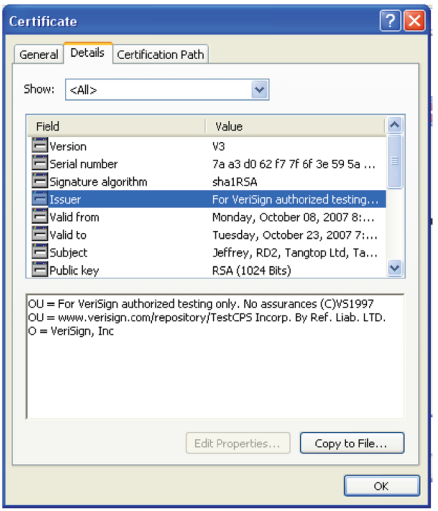

Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: Console Server
Issued by: Console Server
Valid from 10/27/2005 to 10/25/2015
Install Certificate...
Issuer Statement
OK

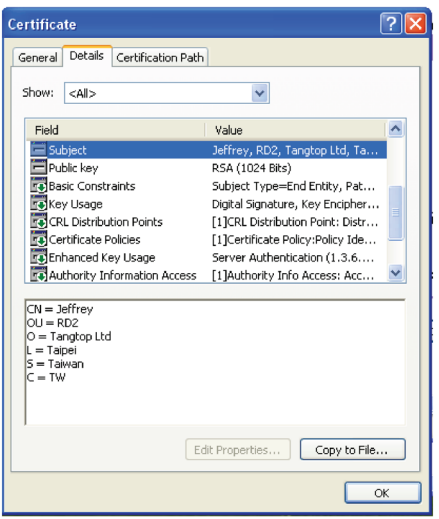
L'autre façon de reconnaître une connexion web sécurisée d'une autre dangereuse consiste à rechercher un symbole de verrouillage sur votre navigateur (coin en bas à droite du navigateur Internet Explorer). Vous pouvez double-cliquer sur le symbole pour examiner les informations détaillées du certificat côté serveur.

Une fois que vous avez préparé une suite de fichier CA publiquement, téléchargez-la de la page « Certificat SSL ». Un redémarrage du système est exigé pour que l'opération prenne effet.

L'exemple suivant explique un certificat publiquement signé et des informations enregistrées par l'autorité de certification (VeriSign).




Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
7a a3 d0 62 f7 7f 6f 3e 59 5a ...
Signature algorithm
sha1RSA
Issuer
For VeriSign authorized testing...
Valid from
Monday, October 08, 2007 8:...
Valid to
Tuesday, October 23, 2007 7:...
Subject
Jeffrey, RD2, Tangtop Ltd, Ta...
Public key
RSA (1024 Bits)
OU = For VeriSign authorized testing only. No assurances (C)V51997
OU = www.verisign.com/repository/TestCPS Incorp. By Ref. Liab. LTD.
O = VeriSign, Inc
Edit Properties...
Copy to File...
OK

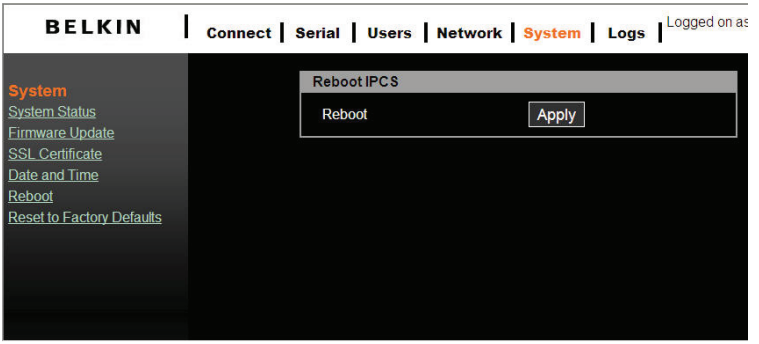

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
Jeffrey, RD2, Tangtop Ltd, Ta...
Public key
RSA (1024 Bits)
Basic Constraints
Subject Type=End Entity, Pat...
Key Usage
Digital Signature, Key Encipher...
CRL Distribution Points
[1]CRL Distribution Point: Distr...
Certificate Policies
[1]Certificate Policy:Policy Ide...
Enhanced Key Usage
Server Authentication (1.3.6....
Authority Information Access
[1]Authority Info Access: Acc...
CN = Jeffrey
OU = RD2
O = Tangtop Ltd
L = Taipei
S = Taiwan
C = TW
Edit Properties...
Copy to File...
OK

Rétablir les paramètres par défaut

Pour retourner au paramétrage par défaut d'usine, cliquez sur « Appliquer ».

Redémarrer

Vous pouvez déclencher le serveur de console pour exécuter un redémarrage logiciel via le réseau. La fonction de redémarrage est obligatoire lorsque le téléchargement du certificat Ca est terminé.



Paramètres par défaut

Nom du serveur	BelkinSC
DHCP	Activé
Adresse IP	192.168.2.156
Masque réseau	255.255.255.0
Passerelle	192.168.2.1
Numéro de série :	xxxxxxxxx (imprimé au dos de l'unité)
Adresse MAC	xx:xx:xx:xx (imprimé au dos de l'unité)
Version et Date	Version du micrologiciel actuel - numéro et date
Nom d'utilisateur	admin
Mot de Passe	admin
Protocole (série)	Telnet
Protocole (web)	HTTP
Filtre IP	Désactiver
Ports série --	
Débit en bauds	9600
Données/arrêt	8-1
Parité	Aucun(e)
Contrôle du flux	Aucun(e)
Temporisation série	0 secondes
Mode de fonctionnement	Serveur de console
Port TCP	**Port 1:** 4001 **Port 2:** 4002 - - - - - - - - **Port 16:** 4016

F1D120ea (RJ45F–DB9F DTE)

Adaptateur femelle DB9 DTE

Applications : Bay Accelar, Nortel, etc.

Référence :F1D122ea - Emballage unique

F1D120ea8PK - Emballage 8

Adaptateur		
Signal	RJ45	DB9F
DSR	1	4
DCD	6	
RTS	2	8
GND	3	5
TxD	4	2
RxD	5	3
CTS	7	7
DTR	8	6 1 (DCD)

F1D121ea (RJ45F–DB25F DTE)

Adaptateur femelle DB25 DTE

Applications : périphériques DTE tels que le PC

Référence :F1D121ea - Emballage unique

Adaptateur		
Signal	RJ45	DB25F
DSR	1	20
DCD	6	
RTS	2	5
GND	3	7
TxD	4	3
RxD	5	2
CTS	7	4
DTR	8	6
		8 (DCD)

F1D122ea (RJ45F – DB25M DCE)

Adaptateur mâle DB25 DCE

Applications : Modems

Référence :F1D122ea - Emballage unique

Adaptateur		
Signal	RJ45	DB25M
DSR	1	6
RTS	2	4
GND	3	5
TxD	4	2
RxD	5	3
DCD	6	1
CTS	7	5
DTR	8	20

F1D123ea (RJ45F–DB25M DTE)

Adaptateur mâle DB25 DTE

Applications : Sun SPARC, etc.

Référence : F1D122ea - Emballage unique

Adaptateur		
Signal	RJ45	DB25M
DSR	1	20
DCD	6	
RTS	2	5
GND	3	7
TxD	4	3
RxD	5	2
CTS	7	4
DTR	8	6

F1D124ea (RJ45F–RJ45M CISCO)

Adaptateur mâle RJ45

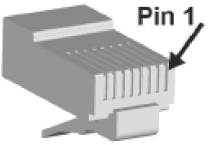
Applications : Périphériques Sun

Référence :F1D122ea - Emballage unique

F1D124ea8PK - Emballage de 8

Adaptateur		
Signal	RJ45	RJ45M
DSR	1	2
RTS	2	8
GND	3	4
		5
TxD	4	6
RxD	5	3
CTS	7	1
DTR	8	7

Brochage de sortie du câble Ethernet standard RJ45

Broche	Description	
1	Tx+	
2	Tx-	
3	Rx+	
4	NC	
5	NC	
6	Rx-	
7	NC	
8	NC	

Annexe C : Numéros de port réservés de TCP/UDP

Les numéros de port sont divisés en trois plages : Ports réservés, ports enregistrés, et ports dynamiques et/ou privés. Les ports réservés sont ceux qui vont de 0 à 1023. Les ports enregistrés sont ceux qui vont de 1024 à 49151. Les ports dynamiques et/ou privés sont ceux qui vont de 49152 à 65535.

Les ports réservés sont affectés par l'IANA et, sur la plupart des systèmes, ils ne peuvent être utilisés que par des processus de système ou des programmes exécutés par des utilisateurs possédant les droits nécessaires. Le tableau ci-dessous montre certains des numéros de port réservés. Pour plus de détails, veuillez visiter le site web IANA : http://www.iana.org/assignments/port-numbers.

Numéro de port	Protocole	TCP/UDP
21	FTP (File Transfer Protocol)	TCP
22	SSH (Shell sécurisé)	TCP
23	Telnet	TCP
25	SMTP (Simple Mail Transfer Protocol)	TCP
37	Heure	TCP, UDP
39	RLP (Resource Location Protocol)	UDP
49	TACACS, TACACS+	UDP
53	DNS	UDP
67	serveur BOOTP	UDP
68	client BOOTP	UDP
69	TFTP	UDP
70	Gopher	TCP
79	Finger	TCP
80	HTTP	TCP
110	POP3	TCP
119	NNTP (Network News Transfer Protocol)	TCP
161/162	SNMP	UDP
443	HTTPS	TCP

BOOTP (Bootstrap Protocol)
Semblable au DHCP, mais pour de plus petits réseaux. Attribue l'adresse IP pendant une durée de temps spécifique.

CHAP (Challenge Handshake Authentication Protocol)
Un protocole sécurisé pour la connexion à un système ; il est plus sécurisé que le PAP.

DHCP (Dynamic Host Configuration Protocol)
Protocole Internet pour automatiser la configuration des ordinateurs qui utilisent TCP/IP.

DNS = serveur de nom de domaine.
Un système qui permet à un serveur de nom de réseau de traduire des noms d'hôte de texte en adresses IP numériques.

Kerberos
Un protocole d'authentification de réseau qui fournit l'authentification stricte pour les applications client/serveur à l'aide la cryptographie par clé secrète.

LDAP (Lightweight Directory Access Protocol)
Un protocole pour accéder aux informations de répertoire.

NAT (Network Address Translation)
Un standard Internet qui permet à un LAN d'utiliser un jeu d'adresses IP pour le trafic interne et un deuxième jeu d'adresses pour le trafic externe. Ceci permet à une entreprise de protéger a interne de l'internet public.

NFS (Network File System)
Un protocole qui permet le partage de fichier à travers un réseau. Les utilisateurs peuvent voir, enregistrer, et mettre à jour des fichiers sur un ordinateur distant. Vous pouvez utiliser NFS pour monter tout, ou une partie d'un système de fichiers. Les usagers peuvent accéder la partie montée avec les mêmes privilèges que l'accès utilisateur à chaque fichier.

NIS (Network Information System)
Système développé par Sun Microsystems pour distribuer des données de système telles que les noms d'utilisateur et d'hôtes parmi les ordinateurs d'un réseau.

NMS (Network Management System)
NMS sert de serveur central, qui demande et reçoit des informations de type SNMP à partir de tout ordinateur qui utilise SNMP.

NTP (Network Time Protocol)
Un protocole utilisé pour synchroniser l'heure sur les ordinateurs en réseau et le matériel.

PAP (Password Authentication Protocol)
Une méthode d'authentification de l'utilisateur dans laquelle le nom d'utilisateur et le mot de passe sont transmis via un réseau et comparés à un tableau des paires de nom et mot de passe.

PPP (Point-to-Point Protocol)
Un protocole pour créer et exécuter l'IP et d'autres protocoles réseau via une liaison série.

RADIUS (Remote Authentication Dial-In User Service)
Un protocole d'authentification et de comptabilité. Permet à des serveurs d'accès distant de communiquer avec un serveur central pour authentifier des utilisateurs des appels entrants et leur autorisation d'accès. Une entreprise stocke des profils d'utilisateur dans une base de données centrale que tous les serveurs distants peuvent partager.

SNMP (Simple Network Management Protocol)
Un protocole que les administrateurs de système utilisent pour surveiller des réseaux et des périphériques connectés et pour répondre aux questions d'autres hôtes de réseau.

SMTP (Simple Mail Transfer Protocol)
Protocole TCP/IP pour envoyer des e-mails entre un serveur et l'autre.

SSL (Secure Sockets Layer)
Un protocole qui fournit des services d'authentification et de cryptage entre un serveur web et un navigateur web.

SSH (Shell sécurisé)
Un protocole de transport sécurisé basé sur la cryptographie de touche publique.

TACACS+ (Terminal Access Controller Access Control System)
Une méthode d'authentification utilisée dans des réseaux d'UNIX. Il permet à un serveur d'accès distant de communiquer avec un serveur d'authentification pour déterminer si l'usager a accès au réseau.

Telnet
Un protocole terminal qui fournit une méthode conviviale de création des connections de terminal à un hôte de réseau.

Le serveur de console supporte la configuration de la page web (https). Il existe deux types de fichiers de certificat pour l'authentification du côté serveur.

- Auto-signé : Les utilisateurs peuvent créer les fichiers de certificat tous seuls. Le côté négatif est que le client sera invité à accepter un certificat signé par une autorité que le navigateur ne connaît pas. Habituellement le navigateur client devra recevoir le certificat une seule fois et il ne sera plus invité à le faire.
- Signé par une autorité de certification : Les usagers créent des fichiers CA et les envoient à un CA pour la signature. L'avantage principal est que l'utilisateur ne sera pas invité à accepter un certificat.

Les utilisateurs ont besoin d'installer la boîte à outils d'openSSL avant de créer les fichiers CA mentionnés ci-dessus. Nous expliquons ici comment générer le certificat du serveur web du serveur de console qui utilisent l'openSSL et la shell de Linux. Pour la boîte à outils d'openSSL, vous pouvez la télécharger de : http://www.openssl.org/.

1. CA autosigné:

i) Créez une clé et un certificat X.509 :

sous l'invite de commande de Linux :

openssl req -x509 -newkey rsa:1024 -days 1024 -keyout cakey.pem -out cacert.pem

Les options qui peuvent être changées ici sont :

* l'algorithme du PK peut être modifié de rsa en dsa ainsi que la longueur de la clé en morceaux (512, 1024, 2048, 4096).

* période de temps pour la validité de certificat ; nous la définissons à 1024 jours, c'est-à-dire moins de 3 ans.

Vous pouvez également définir la date initiale ou finale pour la validité du certificat. Vous serez invité à entrer le mot de passe PEM deux fois pour la clé puis à entrer des informations nécessaires pour le certificat :

Voici un exemple d'invitation :

Nom de pays	<US>
Nom de l'état ou de la province	<YourState>
Ville ou localité	<Anchorage>
Nom d'entreprise	<Your business name>
Unité organisationnelle Prolix	<R & D>
Nom commun (SERVER HOST NAME)	<IPCS>
Adresse e-mail de l'administrateur serveur	<you@yourdomain.dom>

ii) mot de passe en bande :

openssl rsa -in cakey.pem -out cakey-nopassword.pem

iii) Combinez les clés et les fichiers de certificat X.509 en server.pem :

cat cakey-nopassword.pem cacert.pem > server.pem

iv) Collectez les 3 fichiers PEM et préparez vous pour télécharger sur le serveur IPCS :

server.pem , cacert.pem , cakey.pem

2. Signé par CA digne de confiance :

i) Préparez la clé privée **cakey.pem:**

openssl genrsa –des3 –out cakey.pem 1024

signification des paramètres :

genrsa : générez la clé privée RSA

des3 : Cryptez le certificat par DES3

1024 : la taille de la clé est 1024 bits

ii) Préparez une demande de signature de certificat :

openssl req –new –key cakey.pem –out server.csr

la boîte à outils d'openSSL invitera l'utilisateur avec un message pour l'aider à remplir un formulaire d'inscription. Une fois qu'il est rempli, les utilisateurs peuvent soumettre le fichier CSR à www.verisign.com pour le test ou se reporter à http://www.hitrust.com.tw/hitrustexe/frontend/default_tw.asp (situé à Taiwan) pour appliquer un certificat signé. Obtenez le certificat et nommez le fichier ainsi « cacert.pem »..

iii) mot de passe en bande :

openssl rsa –in cakey.pem –out cakey-nopassword.pem

iv) Combinez les clés et les fichiers de certificat X.509 en server.pem :

cat cakey-nopassword.pem cacert.pem > server.pem

v) Rassemblez les 3 fichiers PEM pour le téléchargement :

server.pem , cacert.pem , cakey.pem

Déclaration FCC

DÉCLARATION DE CONFORMITÉ À LA RÉGLEMENTATION FCC EN MATIÈRE DE COMPATIBILITÉ ÉLECTROMAGNÉTIQUE

Nous, Belkin International, Inc., sis au 501 West Walnut Street, Compton CA, 90220, États-Unis, déclarons sous notre seule responsabilité que le produit F1DU, auquel se réfère la présente déclaration :

est conforme aux normes énoncées à l'alinéa 15 de la réglementation FCC. Le fonctionnement est sujet aux deux conditions suivantes :

(1) cet appareil ne peut pas provoquer d'interférences nuisibles et (2) cet appareil doit accepter toute interférence reçue, y compris les interférences pouvant entraîner un fonctionnement non désiré.

L'appareil a été testé et satisfait aux limites de la classe A des appareils numériques, conformément à l'alinéa 15 de la réglementation de la FCC. Ces limites sont conçues pour assurer la protection raisonnable contre l'interférence nuisible quand le matériel est actionné dans un environnement commercial. L'appareil génère, utilise et peut irradier une énergie de fréquence radio. S'il n'est pas installé et utilisé conformément aux instructions, il peut causer des interférences nuisibles sur le plan de la réception radio ou télévision. Le fonctionnement de ce matériel dans des zones résidentielles est susceptible d'entraîner l'interférence nuisible dans ce cas l'usager sera requis de rectifier l'interférence à ses frais.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.

Déclaration de conformité CE

Nous, Belkin International, Inc., déclarons que le produit F1DP116S, auquel se rapporte la présente déclaration, a été élaboré dans le respect des normes d'émissions EN55022 ainsi que des normes d'immunité EN55024, LVP EN61000-3-2 et EN61000-3-3 en vigueur.

ICES

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Garantie produit limitée de 2 ans de Belkin International, Inc.

Couverture offerte par la garantie

Belkin International, Inc. (« Belkin ») garantit à l'acheteur initial de ce produit Belkin que le produit est exempt de défauts de conception, de montage, de matériau et de fabrication.

Période de couverture

Belkin Corporation garantit ce produit Belkin pour une période de deux ans.

En cas de problème

Garantie du produit
Belkin s'engage à réparer ou à remplacer gratuitement, à sa convenance, tout produit défectueux (sans intervention dans les frais d'expédition du produit).

Limites de la couverture offerte par la garantie

Toutes les garanties précitées sont nulles et non avenues si le produit Belkin n'est pas retourné à Belkin, à la demande expresse de celui-ci, l'acheteur étant responsable de l'acquittement des frais d'expédition, ou si Belkin détermine que le produit Belkin a été installé de façon inappropriée ou modifié d'une quelconque manière. La garantie du produit Belkin ne protège pas contre des calamités naturelles comme les inondations, les tremblements de terre, la foudre, la guerre, le vandalisme, le vol, l'usure normale, l'érosion, l'épuisement, l'obsolescence, l'abus, les dommages provoqués par des perturbations de basse tension (baisses ou affaissements de tension, par exemple), un programme non autorisé ou une modification de l'équipement du système.

Pour une demande d'intervention

Procédez comme suit pour obtenir une réparation de votre produit Belkin :

1. Contactez Belkin International, Inc. au 501 W. Walnut St., Compton CA 90220, U.S.A. À l'attention de : Customer Service (service clientèle) ou appelez le (800)-223-5546 dans un délai de 15 jours suivant l'apparition du problème. Préparez-vous à fournir les informations suivantes :
    a. Le numéro de référence du produit Belkin.
    b. Lieu d'achat du produit.
    c. Date d'achat du produit.
    d. Une copie de la facture originale.

2. Le représentant du service client Belkin vous indiquera alors comment envoyer votre facture et le produit Belkin, et comment présenter votre réclamation.

Belkin se réserve le droit d'examiner le produit Belkin endommagé. Tous les frais d'expédition du produit Belkin à l'adresse de Belkin en vue de son inspection seront entièrement à la charge de l'acheteur. Si Belkin détermine, à son entière discrétion, qu'il serait impossible d'expédier l'équipement endommagé à Belkin, Belkin peut désigner un atelier de réparation de son choix pour l'inspection du produit et l'établissement d'un devis de réparation. Les coûts, s'il en est, pour l'expédition de l'équipement jusqu'à l'atelier de réparation et le retour, et pour l'estimation, seront entièrement assumés par l'acheteur. L'équipement endommagé doit être disponible pour inspection jusqu'à ce que la demande de réclamation soit réglée. Lorsqu'un règlement intervient, Belkin se réserve le droit d'un recours en subrogation sous toute autre police d'assurance détenue par l'acheteur.

La loi nationale face à la garantie.
CETTE GARANTIE NE COMPREND QUE LA GARANTIE BELKIN. BELKIN REJETTE PAR LE PRÉSENT DOCUMENT TOUTES LES AUTRES GARANTIES, EXPLICITES OU IMPLICITES, SAUF EXCEPTIONS PRÉVUES PAR LA LOI, Y COMPRIS MAIS SANS S'Y LIMITER, LES GARANTIES IMPLICITES AFFÉRENTES À LA QUALITÉ LOYALE ET MARCHANDE ET À L'ADÉQUATION À UNE FINALITÉ DONNÉE. CES GARANTIES IMPLICITES, LE CAS ÉCHÉANT, SONT D'UNE DURÉE LIMITÉE AUX CONDITIONS DE LA PRÉSENTE GARANTIE.

Certains pays ne permettent pas d'imposer de limite à la durée de validité des garanties implicites. Il se peut donc que les limites ci-dessus ne s'appliquent pas dans votre cas.

BELKIN NE PEUT EN AUCUN CAS ÊTRE TENU RESPONSABLE DE DOMMAGES ACCESSOIRES, DIRECTS, INDIRECTS OU MULTIPLES, Y COMPRIS, MAIS SANS S'Y LIMITER, LA PERTE DE REVENUS OU D'AFFAIRES DÉCOULANT DE LA VENTE OU DE L'UTILISATION DE TOUT PRODUIT BELKIN, MÊME LORSQU'IL A ÉTÉ AVISÉ DE LA PROBABILITÉ DES DITS DOMMAGES.

La garantie vous confère des droits légaux spécifiques. Vous pouvez également bénéficier d'autres droits qui varient d'un pays à l'autre. Certains pays ne permettent pas d'exclure ou de limiter les dommages accidentels, consécutifs ou autres, de sorte que les limitations d'exclusions précitées peuvent ne pas s'appliquer dans votre cas.

BELKIN®

OmniView® Serveur de console série

Assistance technique gratuite*

Vous trouverez des informations techniques sur le site www.belkin.com dans la zone d'assistance technique. Pour contacter le service d'assistance technique par téléphone, veuillez composer le numéro correspondant dans la liste ci-dessous*.

*Hors coût de communication locale

Pays	Numéro	Adresse Internet
AUTRICHE	0820 200766	http://www.belkin.com/uk/support/
BELGIQUE	07 07 00 073	http://www.belkin.com/nl/support/
RÉPUBLIQUE TCHÈQUE	239 000 406	http://www.belkin.com/uk/support/
DANEMARK	701 22 403	http://www.belkin.com/uk/support/
FINLANDE	00800 - 22 35 54 60	http://www.belkin.com/uk/support/
FRANCE	08 - 25 54 00 26	http://www.belkin.com/fr/support/
ALLEMAGNE	0180 - 500 57 09	http://www.belkin.com/de/support/
GRÈCE	00800 - 44 14 23 90	http://www.belkin.com/uk/support/
HONGRIE	06 - 17 77 49 06	http://www.belkin.com/uk/support/
ISLANDE	800 8534	http://www.belkin.com/uk/support/
IRLANDE	0818 55 50 06	http://www.belkin.com/uk/support/
ITALIE	02 - 69 43 02 51	http://www.belkin.com/it/ support
LUXEMBOURG	34 20 80 85 60	http://www.belkin.com/uk/support/
PAYS-BAS	0900 - 040 07 90 0,10 € par minute	http://www.belkin.com/nl/support/
NORVÈGE	81 50 0287	http://www.belkin.com/uk/support/
POLOGNE	00800 - 441 17 37	http://www.belkin.com/uk/support/
PORTUGAL	707 200 676	http://www.belkin.com/uk/support/
RUSSIE	495 580 9541	http://www.belkin.com/uk/support/
AFRIQUE DU SUD	0800 - 99 15 21	http://www.belkin.com/uk/support/
ESPAGNE	902 - 02 43 66	http://www.belkin.com/es/support/
SUÈDE	07 - 71 40 04 53	http://www.belkin.com/uk/support/
SUISSE	08 - 48 00 02 19	http://www.belkin.com/uk/support/
ROYAUME-UNI	0845 - 607 77 87	http://www.belkin.com/uk/support/
AUTRES PAYS	+44 - 1933 35 20 00	

BELKIN®

www.belkin.com

Belkin Ltd.
Express Business Park
Shipton Way, Rushden
NN10 6GL, Royaume-Uni

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk
Pays-Bas

Belkin GmbH
Hanebergstraße 2
80637 Munich
Allemagne

Belkin SAS
130 rue de Silly
92100 Boulogne-Billancourt
France

Belkin Iberia
Avda. Cerro del Aguila 3
28700 San Sebastián de los Reyes
Espagne

Belkin Suède
Knarrarnäsgatan 7
164 40 Kista
Suède

P75598ea