Adressage IP ONS15454 avec mode sécurisé activé

Contenu

Introduction:

Le document décrit l'adresse IP de configuration de base attribuée au noeud ONS 15454 avec le mode sécurisé activé dans le contrôleur de transport Cisco (CTC).

Conditions préalables:

Cisco recommande les connaissances de base sur la gestion des réseaux TCP/IP et DCN (Data Communication Network) dans le réseau.

Conditions requises:

Cartes contrôleur OSN15454 pour périphérique ONS

Logiciel système spécifique à la plate-forme ONS

Informations générales:

Si des cartes TCC2P sont installées, l'adressage IP double est disponible en mode sécurisé. Lorsque le mode sécurisé est désactivé (parfois appelé mode répéteur), l'adresse IP entrée dans le champ IP Address s'applique au port LAN du fond de panier ONS 15454 et au port TCP/IP (LAN) TCC2P. Lorsque le mode sécurisé est activé, le champ IP Address affiche l'adresse attribuée au port TCP/IP (LAN) TCC2P et le superutilisateur peut activer ou désactiver l'affichage de l'adresse IP du fond de panier.

Par défaut, les cartes TCC2, TCC2P, TCC3, TNC, TNCE, TSC et TSCE sont en mode répéteur. Dans ce mode, les ports Ethernet (LAN) avant et arrière partagent une adresse MAC et une adresse IP uniques. Les cartes TCC2P, TCC3, TNC, TNCE, TSC et TSCE vous permettent de placer un noeud en mode sécurisé, ce qui empêche un utilisateur de port d'embarcation d'accès frontal d'accéder au réseau local via le port de fond de panier.

Comportement en mode sécurisé :

La modification d'un noeud TCC2P, TCC3, TNC, TNCE, TSC ou TSCE du mode répéteur au mode sécurisé vous permet de provisionner deux adresses IP pour l'ONS 15454 et entraîne

l'attribution de plusieurs adresses MAC aux ports par le noeud. En mode sécurisé, une adresse IP est provisionnée pour le port LAN du fond de panier ONS 15454 et l'autre adresse IP pour le port Ethernet de la carte. Les deux adresses résident sur des sous-réseaux différents, ce qui fournit une couche supplémentaire de séparation entre le port d'accès de l'embarcation et le réseau local ONS 15454. Si le mode sécurisé est activé, les adresses IP provisionnées pour le port LAN du fond de panier et le port Ethernet de la carte doivent respecter les directives générales d'adressage IP et doivent résider sur différents sous-réseaux les uns des autres.

En mode sécurisé, l'adresse IP attribuée au port LAN du fond de panier devient une adresse privée, qui connecte le noeud à un système d'assistance aux opérations (OSS) via un réseau local du bureau central ou d'entreprise privée. Un superutilisateur peut configurer le noeud pour masquer ou révéler l'adresse IP LAN du fond de panier dans les rapports de messages autonomes CTC, de la table de routage ou TL1.

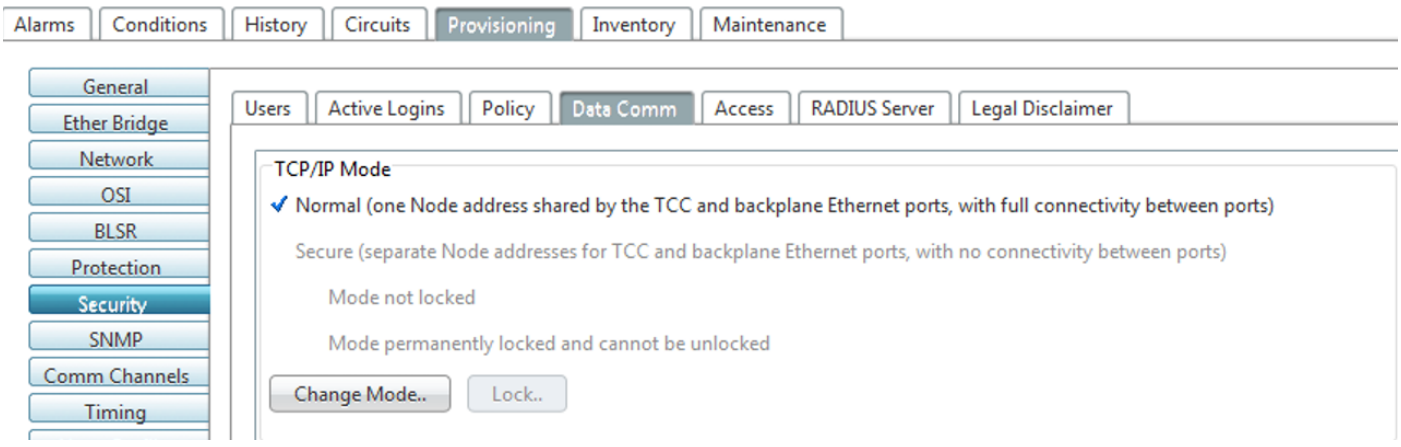
En mode répéteur, un noeud peut être GNE ou ENE. Le fait de placer le noeud en mode sécurisé active automatiquement le proxy SOCKS et attribue par défaut l'état GNE au noeud. Cependant, le noeud peut être reconverti en noeud ENE. En mode répéteur, le proxy SOCKS d'un ENE peut être désactivé (isolant efficacement le noeud au-delà du pare-feu LAN), mais il ne peut pas être désactivé en mode sécurisé. The Net/Subnet Mask Length : saisissez la longueur du masque de sous-réseau (nombre décimal représentant la longueur du masque de sous-réseau en bits) ou cliquez sur les flèches pour ajuster la longueur du masque de sous-réseau. La longueur du masque de sous-réseau est identique pour tous les noeuds ONS 15454 du même sous-réseau. L'adresse MAC (affichage uniquement) affiche l'adresse MAC ONS 15454 IEEE 802.

En mode sécurisé, les ports TCP/IP (LAN) avant et arrière se voient attribuer différentes adresses MAC et les informations du fond de panier peuvent être masquées ou révélées par un superutilisateur.

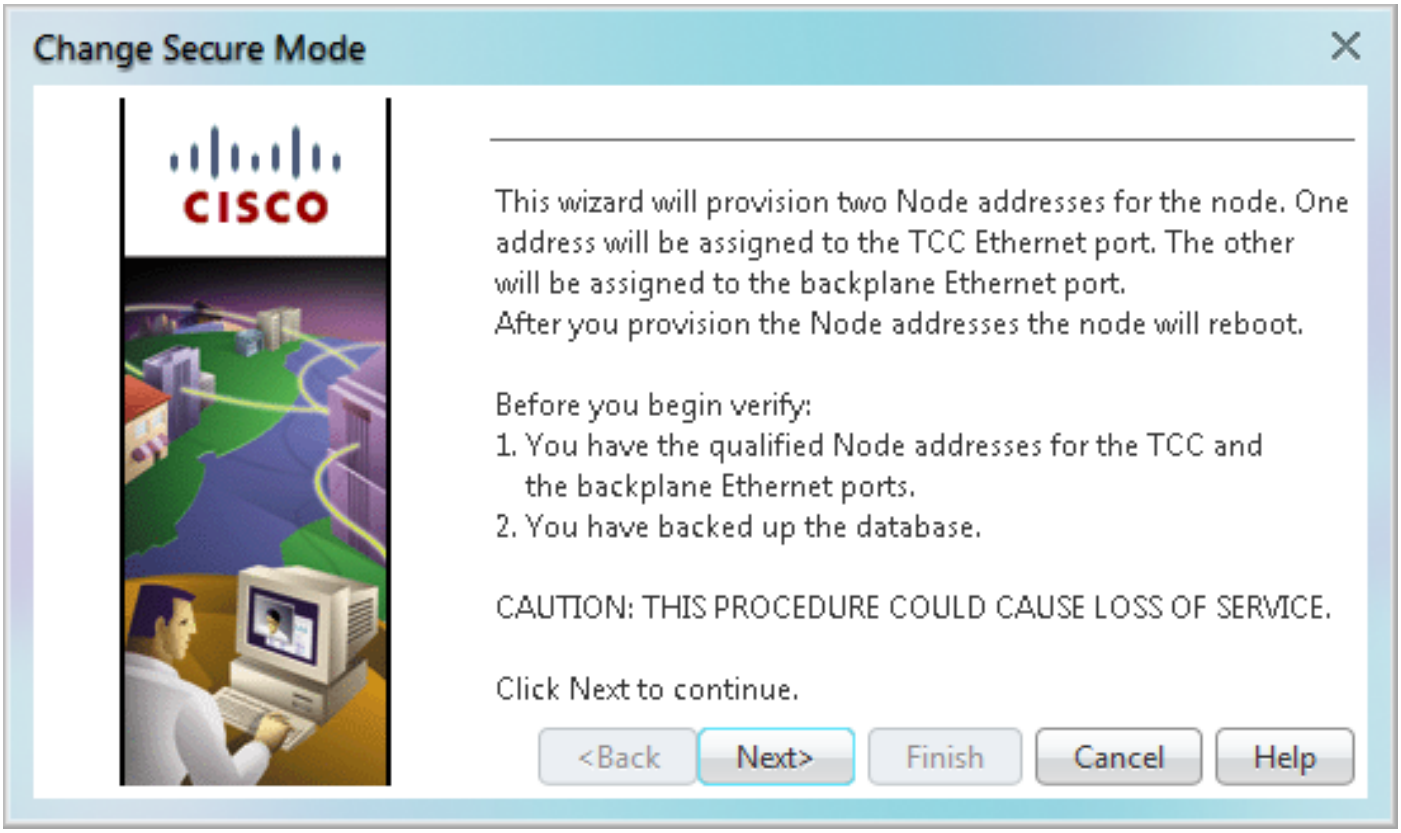
L'adresse IP attribuée au port TCP/IP (LAN) TCC2P doit résider sur un sous-réseau différent du port LAN du fond de panier et du routeur par défaut ONS 15454. Vérifiez que la nouvelle adresse IP TCC2P répond à cette exigence et est compatible avec les adresses IP réseau ONS 15454.

Procédure à suivre pour passer en mode sécurisé via CTC :

Étape 1 Cliquez sur les onglets Provisioning > Security > Data Comm (Provisioning > Sécurité > Data Comm), comme indiqué ci-dessous :

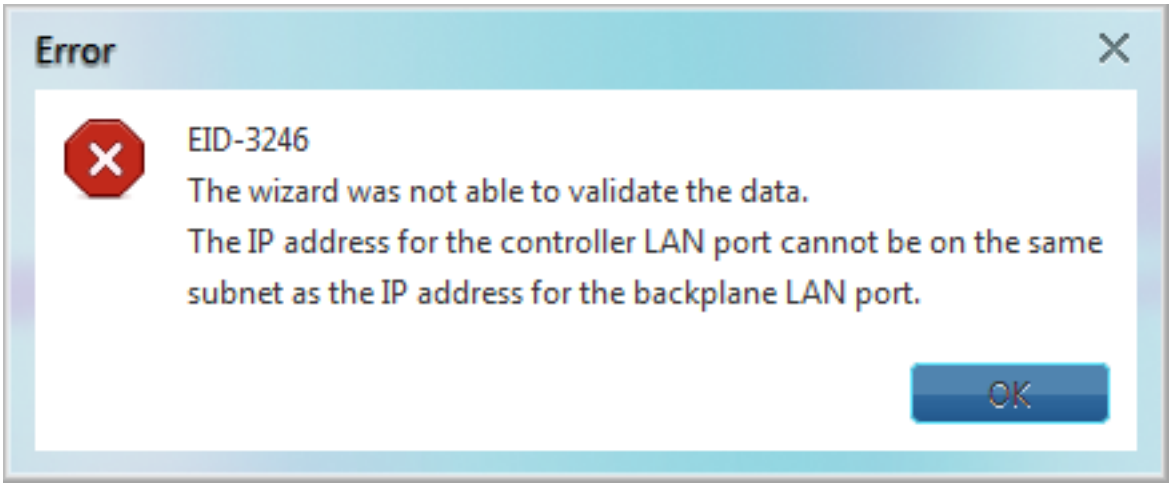


Étape 2 Cliquez sur Modifier le mode.



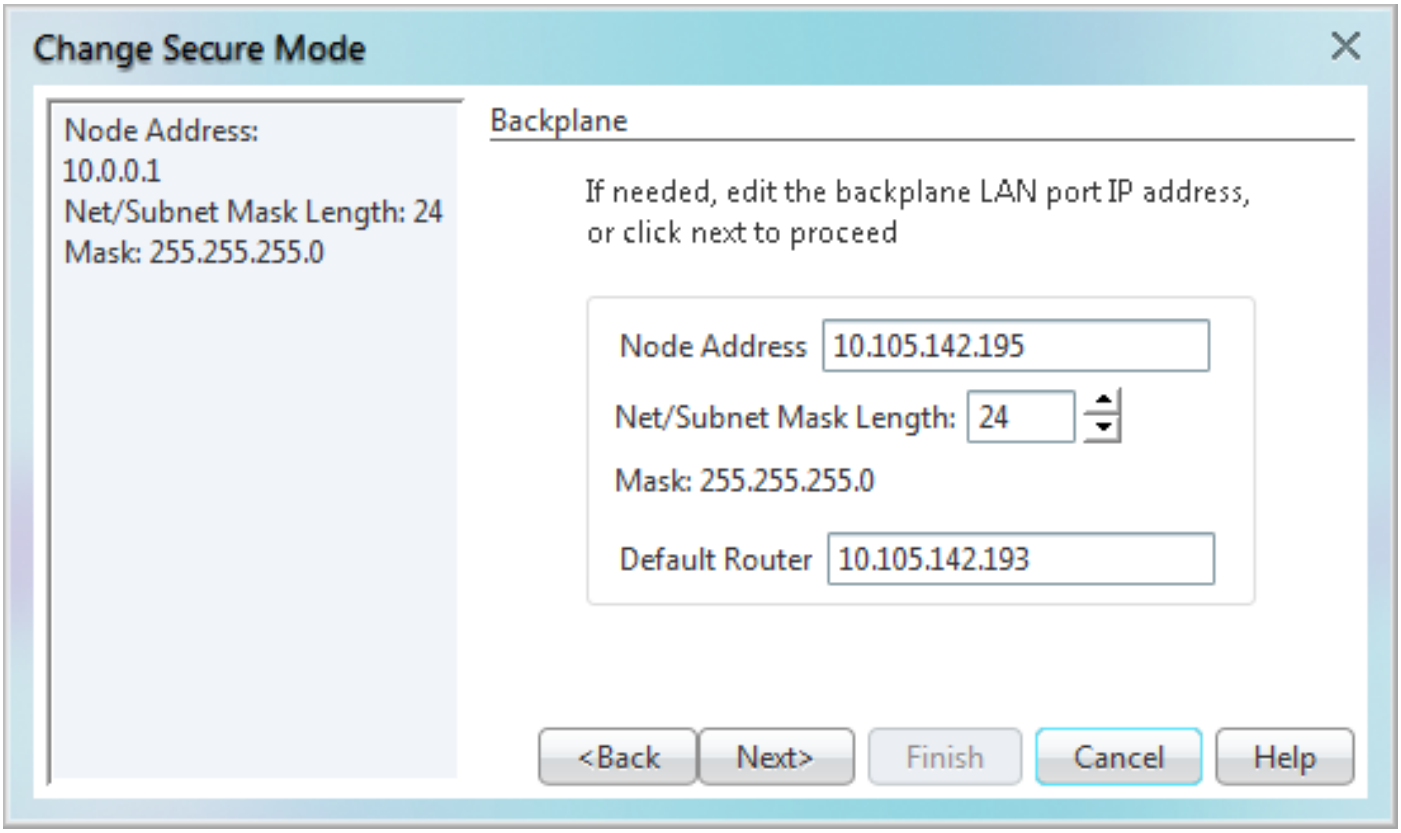
Étape 3 Vérifiez les informations de la page Modifier le mode sécurisé, puis cliquez sur Suivant.

Étape 4 Sur la page TCC Ethernet Port, saisissez l'adresse IP et le masque de sous-réseau du port TCP/IP (LAN) TCC2P. L'adresse IP ne peut pas résider sur le même sous-réseau que le port LAN du fond de panier ou le routeur par défaut ONS 15454 et si ce n'est pas le cas, l'erreur ci-dessous se produira dans CTC.



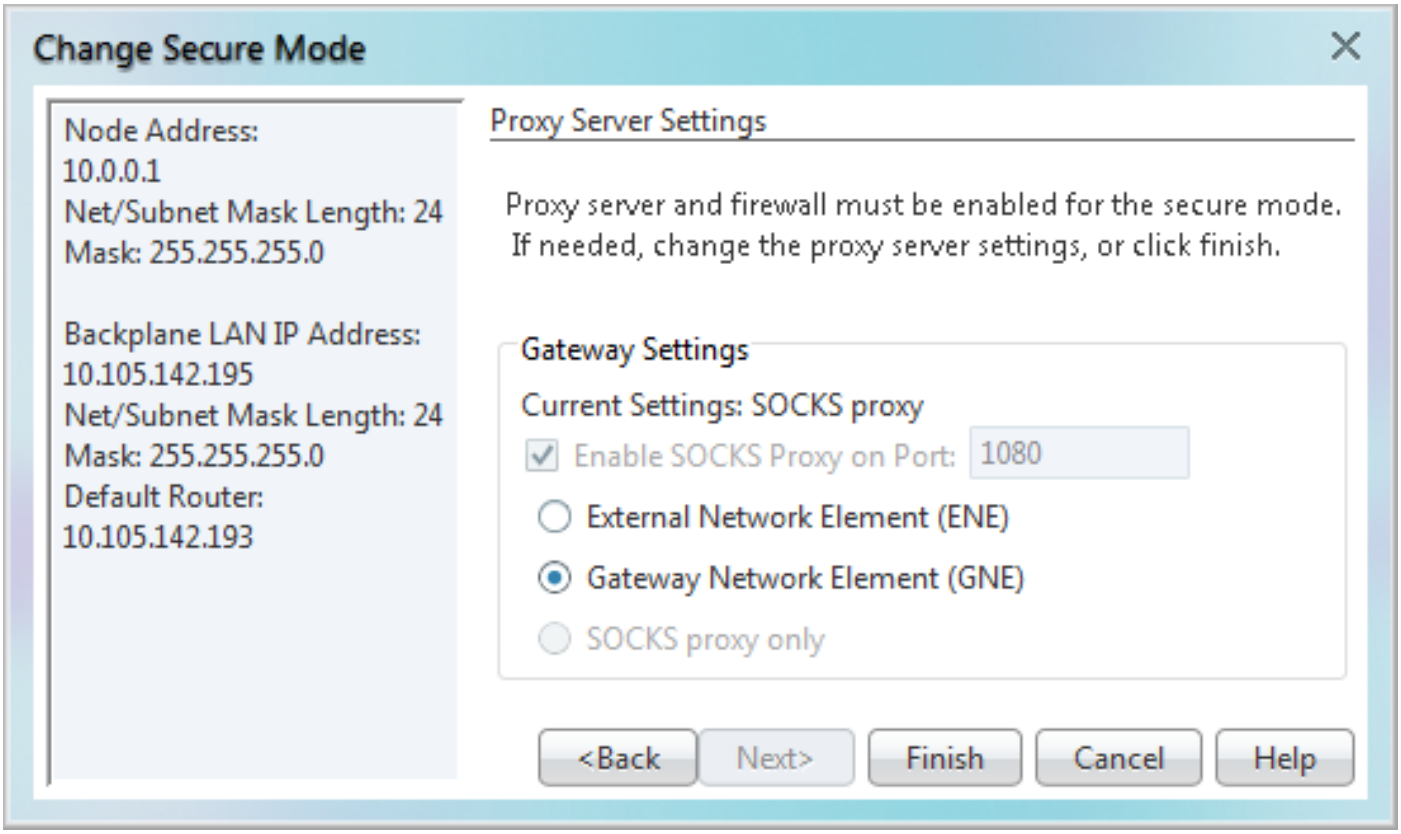
Étape 5 Cliquez sur Suivant après avoir assuré l’étape 4.

Étape 6 Si nécessaire, sur la page Port Ethernet du fond de panier, modifiez l'adresse IP, le masque de sous-réseau et le routeur par défaut du fond de panier. (Normalement, vous ne modifiez pas ces champs si aucun changement de réseau ONS 15454 n'a eu lieu.)



Étape 7 Cliquez sur Suivant.

Étape 8 Sur la page SOCKS Proxy Server Settings, sélectionnez l'une des options suivantes :



- External Network Element (ENE) : si cette option est sélectionnée, l'ordinateur CTC n'est visible que sur l'ONS 15454 où l'ordinateur CTC est connecté. L'ordinateur CTC n'est pas visible pour les noeuds connectés au contrôleur de domaine. En outre, le pare-feu est activé, ce qui signifie que le noeud empêche le trafic IP d'être routé entre le DCC et le port LAN.

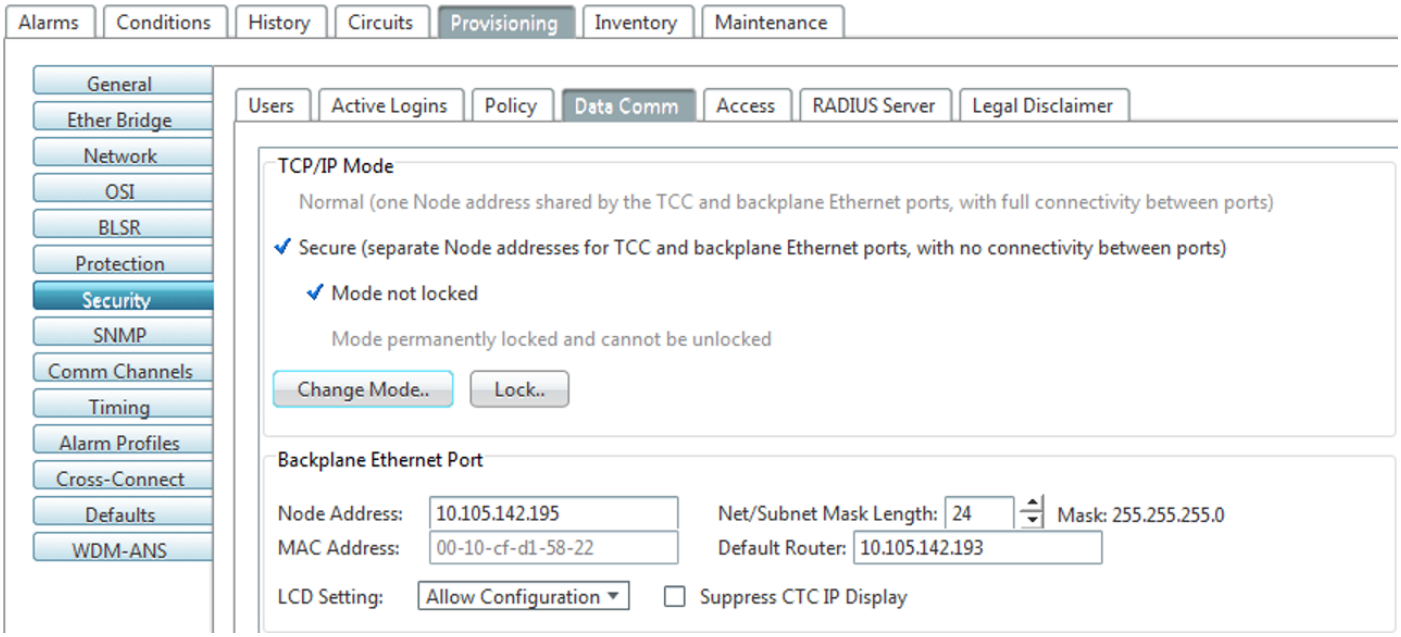
- Gateway Network Element (GNE) : si cette option est sélectionnée, l'ordinateur CTC est visible par les autres noeuds connectés à DCC. Le noeud empêche le trafic IP d'être acheminé entre le DCC et le port LAN.

Note: Le serveur proxy SOCKS est automatiquement activé lorsque vous activez le mode sécurisé.

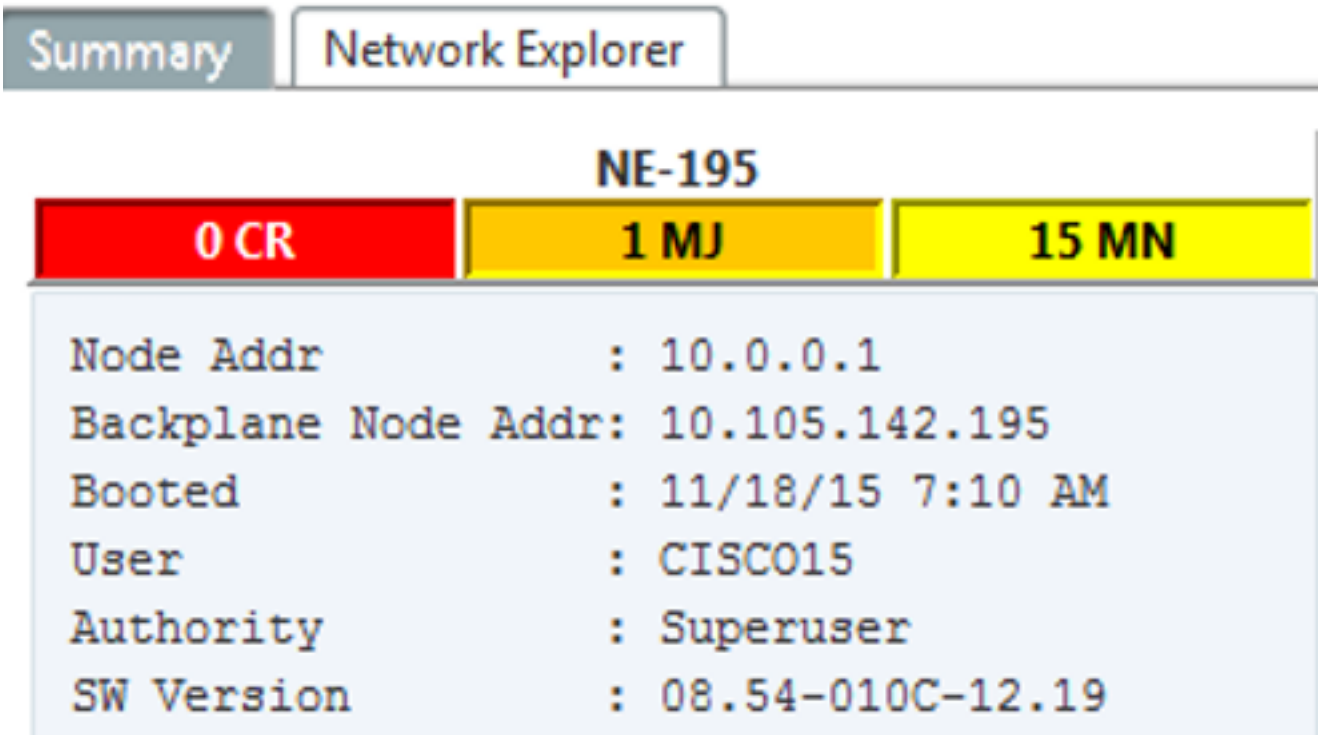
Étape 9 Cliquez sur Terminer.

Dans les 30 à 40 secondes suivantes, les cartes TCC2P redémarrent. La fonction CTC bascule en mode réseau et la boîte de dialogue Alertes CTC apparaît. En mode réseau, le noeud devient gris et une condition DISCONNECTED apparaît dans l'onglet Alarmes.

Après avoir activé le mode sécurisé dans CTC, vérifiez s'ils ont été correctement définis pour le noeud comme indiqué ci-dessous pour un noeud de test.



Vérifiez également les deux adresses IP en mode noeud CTC, comme indiqué ci-dessous.



Comportement verrouillé et déverrouillé du noeud sécurisé :

Le mode sécurisé peut être verrouillé ou déverrouillé sur un noeud fonctionnant en mode sécurisé. L'état par défaut est déverrouillé et seul un superutilisateur peut émettre un verrou. Lorsque le mode sécurisé est verrouillé, la configuration du noeud (y compris l'état du port Ethernet) et l'état du verrouillage ne peuvent être modifiés par aucun utilisateur du réseau. Pour retirer le verrou d'un noeud sécurisé, contactez le support technique de Cisco pour obtenir une autorisation de retour de matériel (RMA) pour l'assemblage de module. L'activation d'un verrou modifie de façon permanente l'EEPROM de l'étagère.

Le verrouillage de configuration d'un noeud est maintenu si la base de données de la carte TCC2P active est rechargée. Par exemple, si vous tentez de charger une base de données de noeud déverrouillée sur la carte TCC2P de secours d'un noeud verrouillé pour transfert vers la carte TCC2P active (action non recommandée), l'état du noeud déverrouillé (via la base de données téléchargée) ne remplacera pas l'état de verrouillage du noeud. Si vous essayez de charger une base de données verrouillée sur la carte TCC2P de secours d'un noeud sécurisé non verrouillé, la carte TCC2P active téléchargera la base de données. Si les valeurs par défaut téléchargées indiquent un état verrouillé, cela entraîne le verrouillage du noeud. Si une charge logicielle a été personnalisée avant l'activation d'un verrou, toutes les fonctions d'approvisionnement verrouillables sont définies de manière permanente sur les valeurs par défaut NE personnalisées fournies dans la charge et ne peuvent être modifiées par aucun utilisateur.

Remarques utiles :

- Si les ports d'accès avant et arrière-plan sont désactivés dans un ENE et que le noeud est isolé de la communication DCC (en raison d'un provisionnement de l'utilisateur ou de défaillances du réseau), les ports avant et arrière-plan sont automatiquement réactivés.
- Le mode sécurisé peut être verrouillé, ce qui empêche la modification du mode.
- L'activation du mode sécurisé entraîne le redémarrage des cartes TCC2P, TCC3, TNC, TNCE, TSC et TSCE ; le redémarrage de la carte affecte le trafic.
- Les options de mode de sécurité ne sont pas disponibles dans CTC si des cartes TCC2 ou un

mélange de cartes TCC2 et TCC2P sont installés.

- L'activation du mode sécurisé entraîne le redémarrage de la carte TCC2P ; un redémarrage de la carte TCC2P affecte le trafic.
- La carte TCC2 ne démarre pas lorsqu'elle est ajoutée en tant que carte de secours à un noeud contenant une carte TCC2P active configurée en mode sécurisé.