

Configuración de las credenciales del dispositivo en el panel empresarial de Cisco

Introducción

Cisco Business Dashboard proporciona herramientas que le ayudan a supervisar, administrar y configurar fácilmente los dispositivos Cisco Business, como switches, routers y puntos de acceso inalámbricos (WAP), mediante el explorador web. También le notifica sobre el dispositivo y las notificaciones de soporte de Cisco, como la disponibilidad de nuevo firmware, el estado del dispositivo, las actualizaciones de la configuración de red y cualquier dispositivo Cisco conectado que ya no esté en garantía o cubierto por un contrato de soporte.

Cisco Business Dashboard Network Management es una aplicación distribuida que consta de dos componentes o interfaces independientes: una o varias sondas denominadas sonda del panel empresarial de Cisco y un único panel denominado panel empresarial de Cisco.

Una instancia de Cisco Business Dashboard Probe instalada en cada sitio de la red realiza la detección de red y se comunica directamente con cada dispositivo de Cisco. En una red de un solo sitio, puede optar por ejecutar una instancia independiente de Cisco Business Dashboard Probe. Sin embargo, si su red está compuesta por varios sitios, puede instalar Cisco Business Dashboard en una ubicación conveniente y asociar cada sonda al panel. Desde la interfaz del administrador, puede obtener una vista de alto nivel del estado de todos los sitios de la red y conectarse a la sonda instalada en un sitio determinado cuando desee ver información detallada para ese sitio.

Para que Cisco Business Dashboard Network detecte y gestione completamente la red, la sonda de Cisco Business Dashboard debe tener credenciales para la autenticación con los dispositivos de red. Cuando se descubre un dispositivo por primera vez, la sonda intentará autenticarse con el dispositivo mediante el nombre de usuario y la contraseña predeterminados y la comunidad SNMP (protocolo simple de administración de red). Si las credenciales del dispositivo se han cambiado del valor predeterminado, será necesario que proporcione las credenciales correctas a Cisco Business Dashboard. Si este intento falla, se generará un mensaje de notificación y el usuario deberá proporcionar credenciales válidas.

Objetivo

El objetivo de este documento es mostrarle cómo configurar las credenciales del dispositivo en la sonda de Cisco.

Dispositivos aplicables | Versión de software

- Panel empresarial de Cisco | 2,2

Configurar las credenciales del dispositivo

Agregar nuevas credenciales

Introduzca uno o varios conjuntos de credenciales en los campos siguientes. Cuando se aplica, cada credencial se probará con cualquier dispositivo del tipo adecuado para el que no estén

disponibles las credenciales de trabajo. Un conjunto de credenciales puede ser una combinación de nombre de usuario/contraseña, una comunidad SNMPv2 o credenciales SNMPv3.

Paso 1. Inicie sesión en la GUI de Cisco Business Dashboard y elija **Administration > Device Credentials**.

Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log

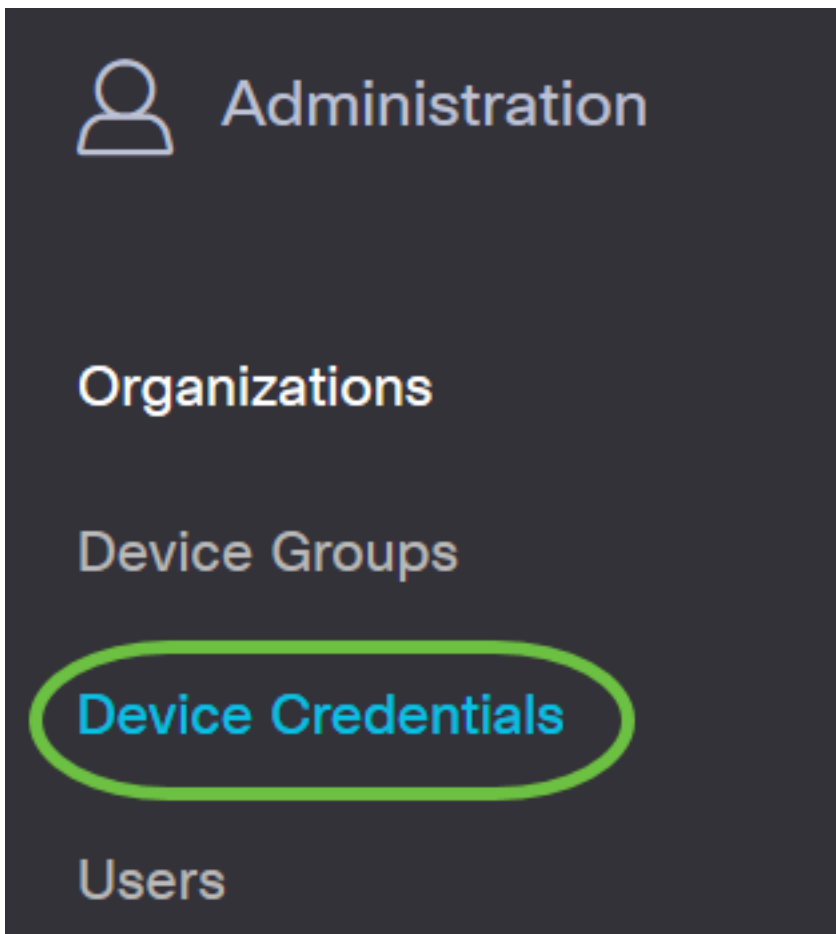


Reports



Administration





Paso 2. En el área Agregar nuevas credenciales, introduzca un nombre de usuario que se aplicará a los dispositivos de la red en el campo *Nombre de usuario*. El nombre de usuario y la contraseña predeterminados son cisco.

Nota: En este ejemplo, se utiliza cisco.

Add New Credentials

Enter one or more sets of credentials in the fields below. When applied, each credential will be tested against any devices of credentials may be either a username/password combination, an SNMPv2 community or SNMPv3 credentials.

cisco	●●●●●●●●	🗑️ +
cisco		🗑️

Paso 3. En el campo *password*, ingrese una contraseña.

Add New Credentials

Enter one or more sets of credentials in the fields below. When applied, each credential will be tested against any devices of credentials may be either a username/password combination, an SNMPv2 community or SNMPv3 credentials.

cisco	●●●●●●●●	🗑️ +
cisco		🗑️

Paso 4. En el campo *Comunidad SNMP*, ingrese el nombre de la comunidad. Es la cadena de comunidad de sólo lectura para autenticar el comando SNMP Get. El nombre de comunidad se utiliza para recuperar la información del dispositivo SNMP. El nombre predeterminado de la comunidad SNMP es Public.

Nota: En este ejemplo, se utiliza Public.

The screenshot shows a configuration form for SNMPv3. At the top, there are two input fields: one containing 'cisco' and another with masked characters. Below these are two rows of 'Community' entries, each with a checkmark and a trash icon. The first 'Community' entry, containing 'public', is highlighted with a green oval. Below the communities are two authentication/encryption options: 'SHA' and 'AES', each with a dropdown arrow and a corresponding masked password field.

Paso 5. En el campo *SNMPv3 User Name*, ingrese un nombre de usuario que se utilizará en el SNMPv3

Nota: En este ejemplo, se utiliza Public.

The screenshot shows the same configuration form as in Step 4. The 'User Name' field is highlighted with a green oval and contains 'public'. The 'Authentication' dropdown is set to 'SHA' and the 'Encryption' dropdown is set to 'AES'. Both dropdowns have corresponding password fields with masked characters.

Paso 6. En el menú desplegable *Authentication*, elija un tipo de autenticación que SNMPv3 utilizará. Las opciones son:

- Ninguno: no se utiliza autenticación de usuario. Este es el valor predeterminado. Si elige esta opción, vaya directamente al [Paso 11](#).
- MD5: utiliza el método de encriptación de 128 bits. El algoritmo MD5 utiliza un criptosistema público para cifrar datos. Si selecciona esta opción, se le solicitará que introduzca una frase de paso de autenticación.
- SHA: el algoritmo hash seguro (SHA) es un algoritmo de hash unidireccional que produce un resumen de 160 bits. SHA calcula más lentamente que MD5, pero es más seguro que MD5. Si selecciona esta opción, se le solicitará que introduzca una frase de paso de autenticación y elija un protocolo de cifrado.

Nota: En este ejemplo, se utiliza SHA.

public ✓

public ✓

SHA

None

MD5

SHA

Paso 7. En el campo *Frase de Paso de Autenticación*, ingrese una contraseña para ser utilizada por SNMPv3.

public ✓

public ✓

SHA

AES

Paso 8. En el menú desplegable Tipo de cifrado, elija un método de cifrado para cifrar las solicitudes SNMPv3. Las opciones son:

- Ninguno: no se requiere ningún método de encriptación.
- DES: el estándar de cifrado de datos (DES) es un cifrado de bloque simétrico que utiliza una clave secreta compartida de 64 bits.
- AES128 - Estándar de cifrado avanzado que utiliza una clave de 128 bits.


Nota: En este ejemplo, se elige AES.



The image shows a configuration interface with several rows. The first two rows are labeled 'public' and have a green checkmark. The third row has a dropdown menu set to 'SHA' and a field of 20 dots. The fourth row has a dropdown menu set to 'AES' (highlighted with a green circle) and a field of 20 dots. The fifth row has a dropdown menu set to 'None' and a trash icon. The sixth row has a dropdown menu set to 'DES' and a field of 20 dots. The seventh row has a dropdown menu set to 'AES' (highlighted with a green circle) and a field of 20 dots. The eighth row has a dropdown menu set to 'None' and a field of 20 dots. The ninth row has a dropdown menu set to 'None' and a field of 20 dots.


Paso 9. En el campo *Encryption Pass Phrase (Frase de paso de cifrado)*, ingrese una clave de 128 bits que SNMP utilizará para el cifrado.

The image shows a configuration interface similar to the one above. The first two rows are labeled 'public' and have a green checkmark. The third row has a dropdown menu set to 'SHA' and a field of 20 dots. The fourth row has a dropdown menu set to 'AES' (highlighted with a green circle) and a field of 20 dots. The fifth row has a dropdown menu set to 'None' and a trash icon. The sixth row has a dropdown menu set to 'DES' and a field of 20 dots. The seventh row has a dropdown menu set to 'AES' (highlighted with a green circle) and a field of 20 dots. The eighth row has a dropdown menu set to 'None' and a field of 20 dots. The ninth row has a dropdown menu set to 'None' and a field of 20 dots.

Paso 10. (Opcional) Haga clic en el botón para crear una nueva entrada para el nombre de usuario y el título. Puede agregar hasta una o dos entradas adicionales, dependiendo del tipo de credenciales.



 



 



SHA

AES

Paso 11. Haga clic en Apply (Aplicar).


 

SHA










AES



Ahora debería haber configurado correctamente las credenciales del dispositivo en la sonda de Cisco Business Dashboard.

Ver dispositivos en la red

En la tabla siguiente se muestran los dispositivos detectados por la sonda de Cisco Business Dashboard.

Device	Type	Organization	Network	Credential	Status	Last Used	Last Used Successfully	Action
SG300-10PP	Switch	Branch Offices	Branch 1	SNMPv2/*****	N/A	Aug 5 2020 10:47:33	Aug 5 2020 10:47:33	  
SG300-10PP	Switch	Branch Offices	Branch 1	cisco/*****	N/A	Aug 4 2020 13:42:48	Aug 4 2020 13:42:48	  
switch0294f9	Switch	Branch Offices	Branch 1	SNMPv2/*****	N/A	Aug 5 2020 10:47:30	Aug 4 2020 13:12:12	  

Nota: Se recomienda habilitar SNMP en el dispositivo para que tenga una topología de red más precisa.

Ahora debería haber visto correctamente la identidad de los dispositivos de la red y su tipo de credencial correspondiente.