

Problema del login del Cisco NAC Appliance (Clean Access)

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Problema 1](#)

[Solución](#)

[Problema 2](#)

[Solución](#)

[Problema 3](#)

[Solución](#)

[Problema 4](#)

[Solución](#)

[Problema 5](#)

[Solución](#)

[Problema 6](#)

[Solución](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe el problema del prompt de inicio de sesión del Cisco NAC Appliance (Clean Access) para los usuarios múltiples que intentan registrar en un sistema informático de computadoras de uso público.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

Problema 1

El servidor de acceso limpio (CAS) cubre a varios usuarios que intenten conseguir el acceso de las computadoras de uso público. Este problema ocurre cuando un usuario abre una sesión a través de un portal web a CAS y después termina la sesión. Cuando el usuario siguiente utiliza las mismas computadoras de uso público para iniciar sesión, el prompt no aparece.

Solución

Complete estos pasos para resolver este problema:

1. De su Access Manager limpio de Cisco (CAM), elija la **Administración de dispositivos** >



limpian el acceso > configuración general.

2. Haga clic el **login de la red**, y elija un rol del usuario del rol del usuario de la lista desplegable. Este ejemplo utiliza *Role1*.

Device Management > Clean Access

Device Management > Clean Access

Certified Devices **General Setup** Network Scanner Clean Access Agent

Web Login · Agent Login

User Role

Operating System

Use 'All' settings for the WINDOWS OS family if no version-specific settings are specified

Show [Network Scanner User Agreement page](#) to web login users

Enable pop-up scan vulnerability reports from User Agreement page

Require users to be certified at every web login

Exempt certified devices from web login requirement by adding to MAC filters

Block/Quarantine users with [vulnerabilities](#) in role:

Show quarantined users User Agreement Page of:

3. Asegurese que si el sistema operativo se fija al **WINDOWS ALL** que usted también tiene **uso TODAS LAS configuraciones para la familia del OS (SISTEMA OPERATIVO) WINDOWS si no se especifica ningunas configuraciones versión-específicas** seleccionó.
4. Haga clic la casilla de verificación para que los **usuarios Require sean certificados en cada login de la red**. Esta casilla de verificación fuerza al usuario a pasar con la exploración de la red cada vez que acceden la red. **Nota:** Si están inhabilitados (valor por defecto), los usuarios necesitan solamente ser certificados la primera vez que acceden la red, o hasta que su dirección MAC se borra de la lista certificada.
5. Haga clic en **Update** (Actualizar).

Problema 2

Usted puede ser que reciba este error cuando usted accede CAS a través del webconsole (https):

The link that you requested is not present on this Clean Access System. If you reached this page by following a link from the user interface of the Clean Access Manager or Server, then please report this as a bug.

Solución

Usted puede reeditar los Certificados en CAS y el CAM para resolver este problema.

Problema 3

Refiera a la información en la [sección de soluciones](#) si usted recibe este error:

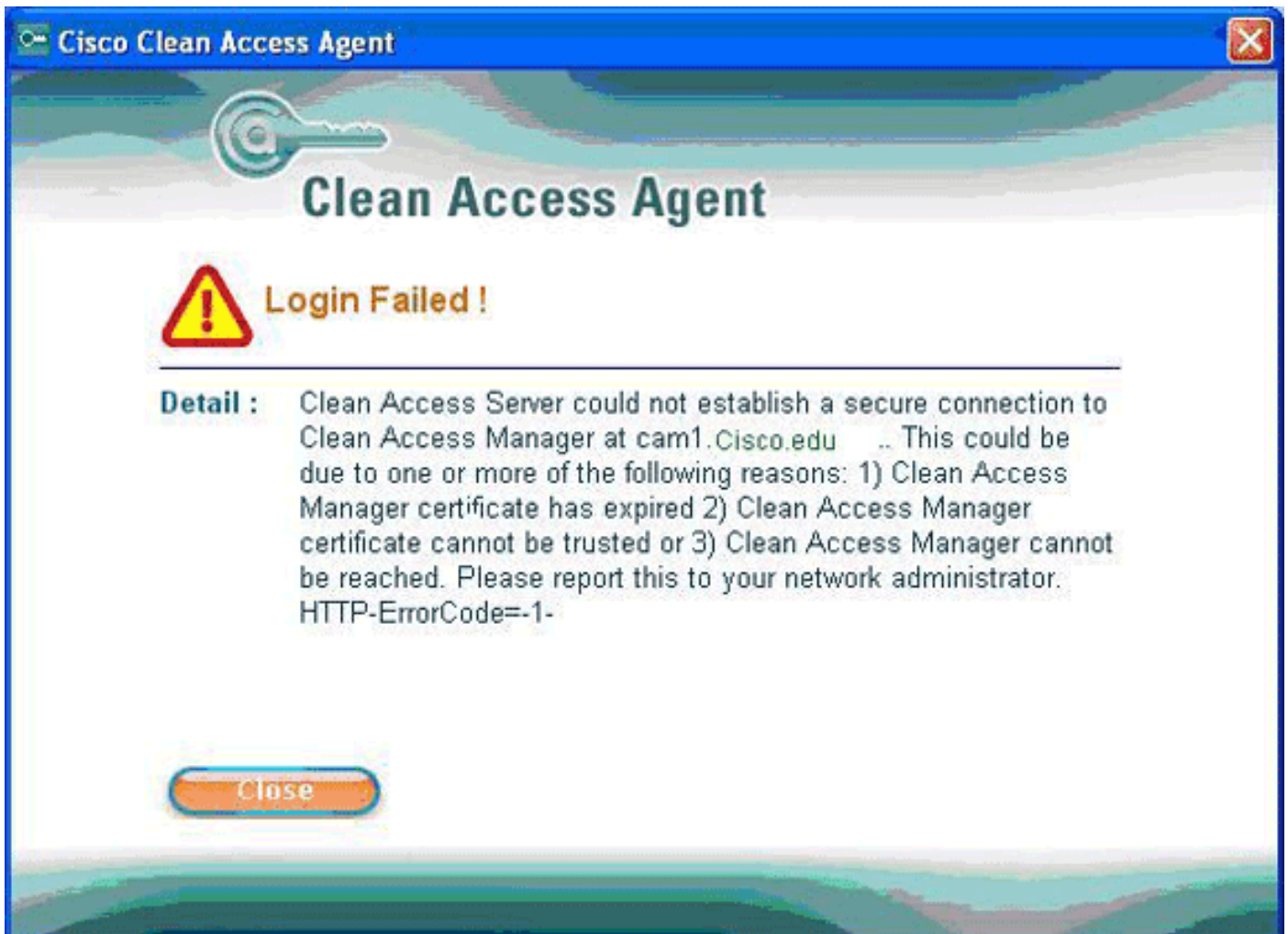
Cisco Clean Access Agent is having problem communicate with NAC appliance server. This could be course by the SSL. Please make sure the certificate on the NAC appliance server is valid (use Domain name and date/time Must not expire). If the NAC Appliance uses the temporary certificate, you have to install the root certificate into the certificate keyChains

Solución

Este error se considera en el Mac OS específicamente. La causa raíz para el problema es que el certificado de CAS necesita ser publicado a un dominio o a un nombre del host calificado completamente para ser validado en Mac OS X, y el cliente necesita tener un certificado raíz apropiado.

Problema 4

Usted puede ser que reciba este error:



Solución

La causa para este mensaje de error es certificado SSL publicado por el CAM a un nombre del host que CAS no podría resolver. Usted puede cambiarla a la dirección IP para resolver el problema.

Problema 5

El NAC pudo automáticamente los Logout user después de algunos minutos.

Solución

CAS termina la sesión al usuario si no recibe ninguna paquetes del usuario para la duración del temporizador Heartbeat (de latido). Para hacer CAS espere un período de tiempo más largo antes de que termine la sesión al usuario, usted puede fijar el *temporizador Heartbeat (de latido)* a un valor más alto. Para aumentar el valle del temporizador Heartbeat (de latido), vaya a **CAS > diverso > temporizador Heartbeat (de latido)**.

Problema 6

Usted puede ser que reciba este error:

¡Error de red! Detalle: La respuesta del servidor no podía ser parsed.[12152]

Solución

Complete estos pasos para resolver este problema:

1. Abra al Internet Explorer.
2. Haga clic las **herramientas**.
3. Elija las **opciones de Internet**.
4. Haga clic la lengüeta **contenta**.
5. Haga clic el **estado claro SSL**. Este paso borra el certificado para el Internet Explorer.
6. Cierre y abra de nuevo al Internet Explorer, y después intente iniciar sesión otra vez.

Información Relacionada

- [Cisco NAC Appliance \(Clean Access\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)