NAC (CCA): Cómo corregir errores de certificado en CAM/CAS después de actualizar a 4.1.6

Contenido

Introducción

Este documento describe cómo corregir errores de certificado en Clean Access Manager (CAM)/Clean Access Server (CAS) con la versión 4.1.6.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento del proceso de actualización del dispositivo Cisco Network Admission Control (NAC).

Componentes Utilizados

La información en este documento se basa en la versión 4.1.6 del dispositivo Cisco NAC con CAM/CAS.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos Cisco para obtener más información sobre las convenciones del documento.

Procedimiento

Estos errores de certificado se encuentran en */perfigo/logs/perfigo-redirect.log0.log.0* o */perfigo/logs/perfigo-log0.log.0*.

A continuación se muestra un ejemplo de error de certificado:

```
SEVERE: RMISocketFactory:Creating RMI socket failed to host
        10.1.20.10:sun.security.validator.ValidatorException:
        Certificate chaining error
Aug 1, 2008 1:41:22 PM com.perfigo.wlan.web.admin.ConnectorClient connect
SEVERE: Communication Exception : java.rmi.ConnectIOException: Exception
        creating connection to: 10.1.20.10; nested exception is:
 javax.net.ssl.SSLHandshakeException:
        sun.security.validator.ValidatorException: Certificate chaining error
```

Estos errores son el resultado de las mejoras de seguridad realizadas en 4.1.6. En 4.1.6, CAS y CAM actúan como clientes y servidores entre sí y deben confiar los unos en los otros. Cada uno requiere los certificados raíz e intermedio del otro. Por ejemplo, si el CAS tiene un certificado Verisign y el CAM tiene un certificado Perfigo (temporal), tanto el CAS como el CAM necesitan la cadena Verisign (root e intermediates) y la raíz Perfigo.

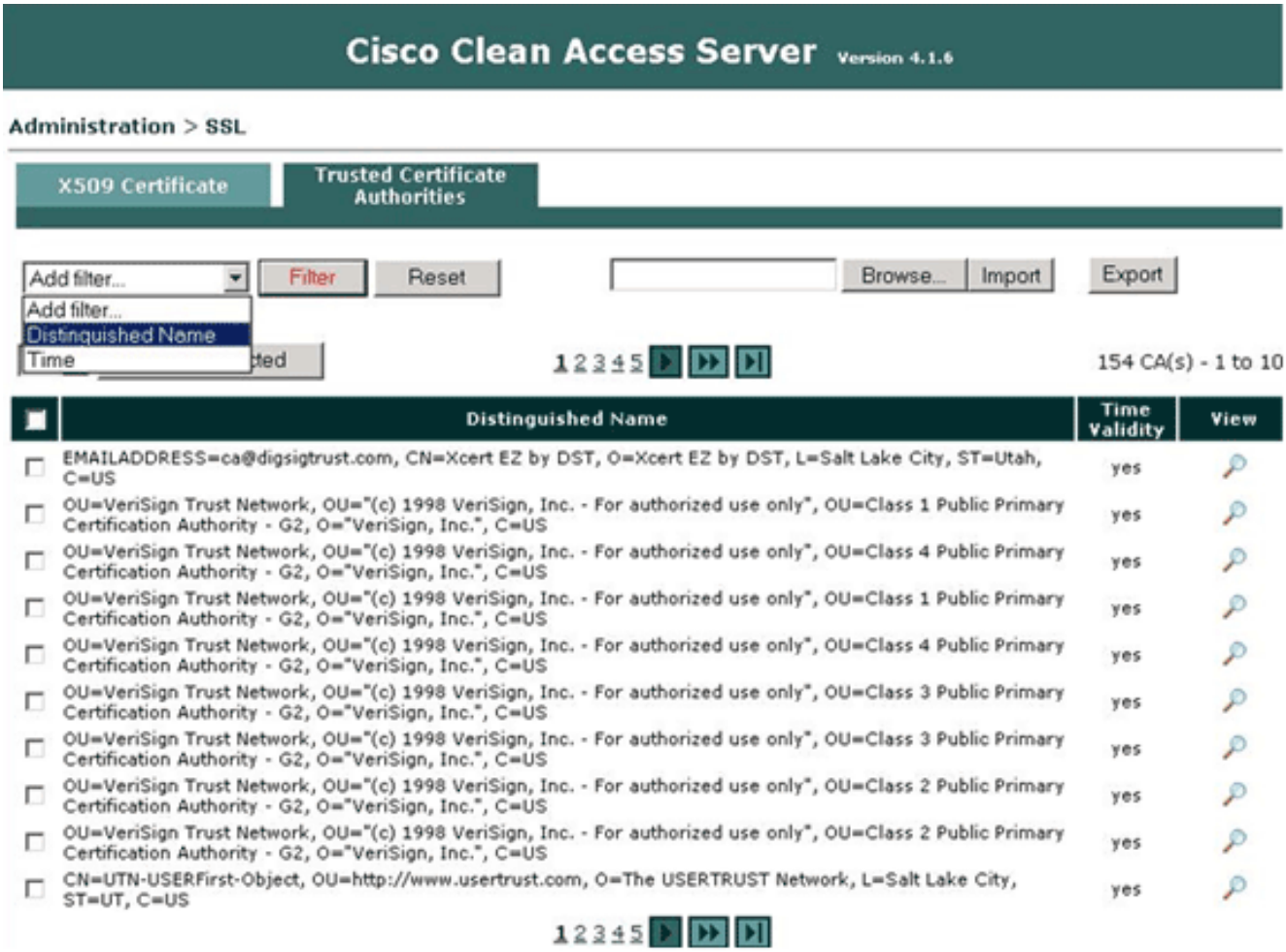
Complete estos pasos para corregir los errores del certificado:

1. Realice una copia de seguridad de los certificados instalados que no sean certificados temporales.En el CAM, abra la interfaz web y vaya a **Administration > CCA Manager > SSL > X509 Certificate**.

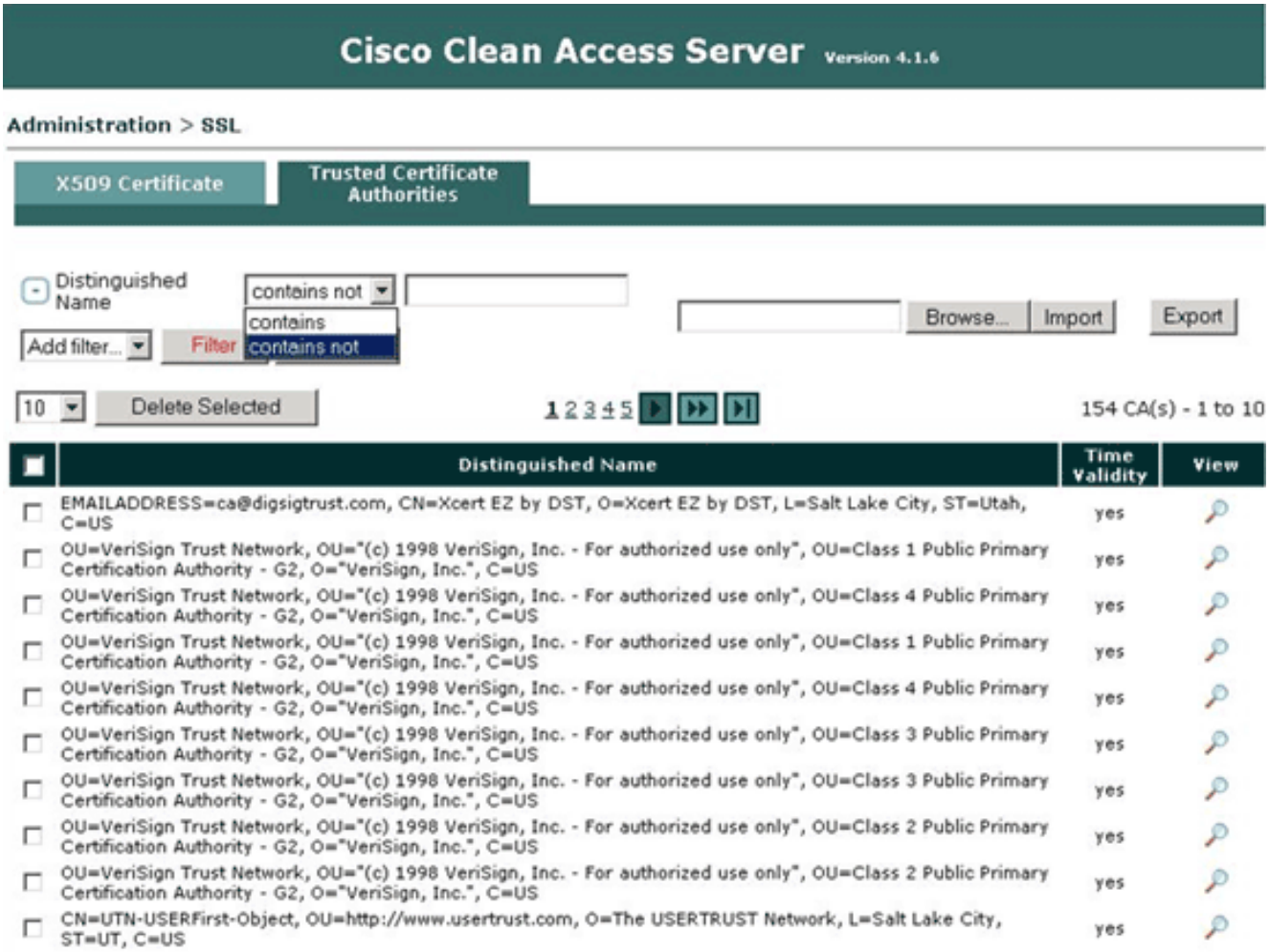
   En el CAS, vaya directamente a la interfaz web a través de https://<CAS IP>/admin, y luego vaya a **Administration > SSL > X509 Certificate**.

Elija **Exportar CSR/Clave privada/Certificado** en la lista desplegable Elegir una acción.Haga clic en **Exportar** junto a Certificado actualmente instalado y guarde este archivo.Haga clic en **Exportar** junto a Clave privada instalada actualmente y guarde este archivo.

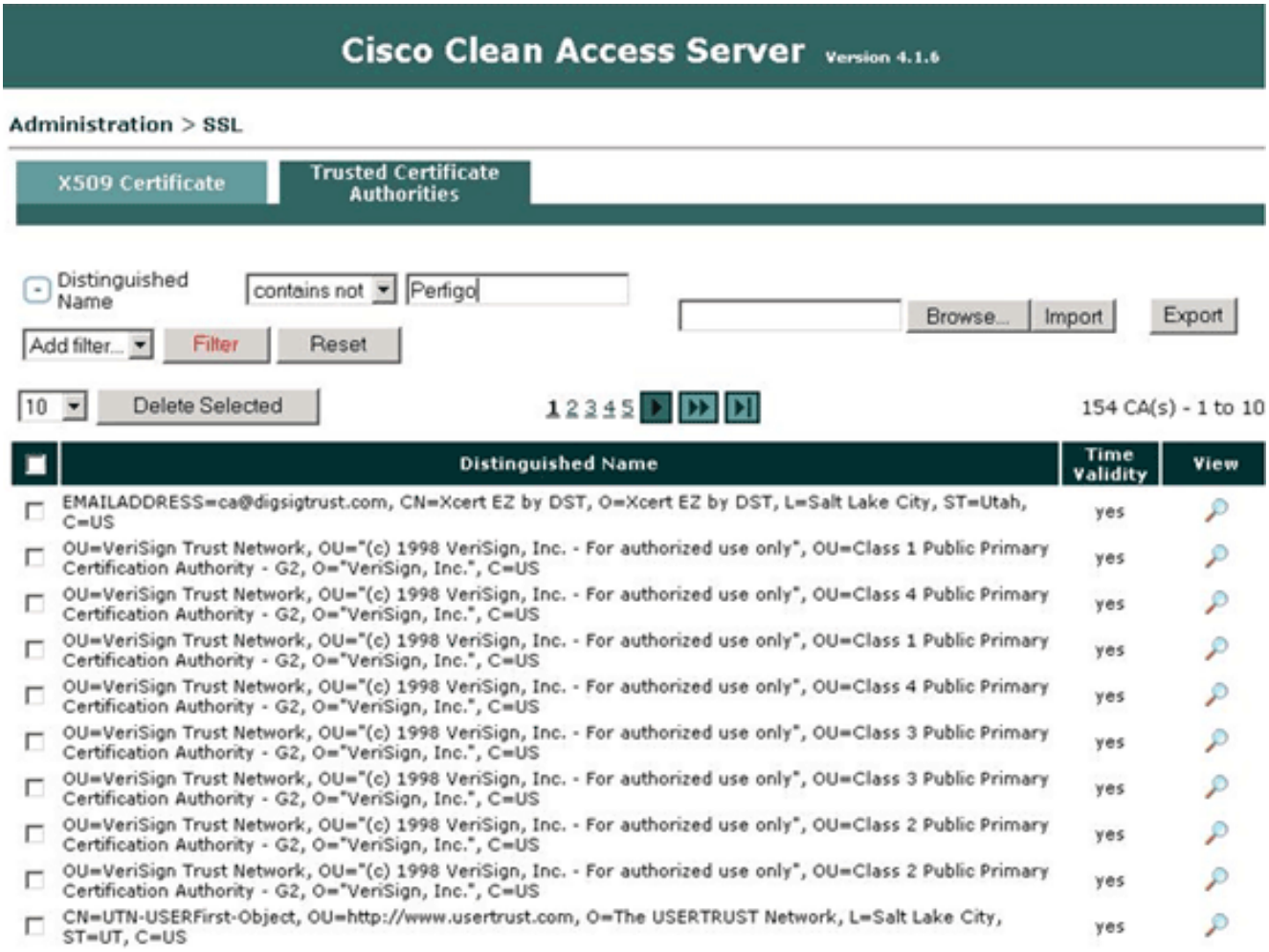
2. Después de la copia de seguridad, si el CAS y el CAM no utilizan ya certificados temporales, genéelos.En el CAM, abra la interfaz web y vaya a **Administration > CCA Manager > SSL > X509 Certificate**.En el CAS, vaya directamente a la interfaz web a través de https://<CAS IP>/admin, y luego vaya a **Administration > SSL > X509 Certificate**.Elija **Generar certificado temporal** en la lista desplegable.Rellene los campos enumerados y haga clic en **Generar**.**Nota:** Esto ya no requiere reiniciar para que surta efecto.
3. Elimine todas las autoridades de certificados de confianza de CAS y CAM. Este paso facilita la gestión y la mejora de la seguridad.En el CAM, vaya a **Administration > CCA Manager > SSL > Trusted Certificate Authorities**.En el CAS, vaya a **Administration > SSL > Trusted Certificate Authorities**.Cree un filtro para excluir el certificado
Perfigo.



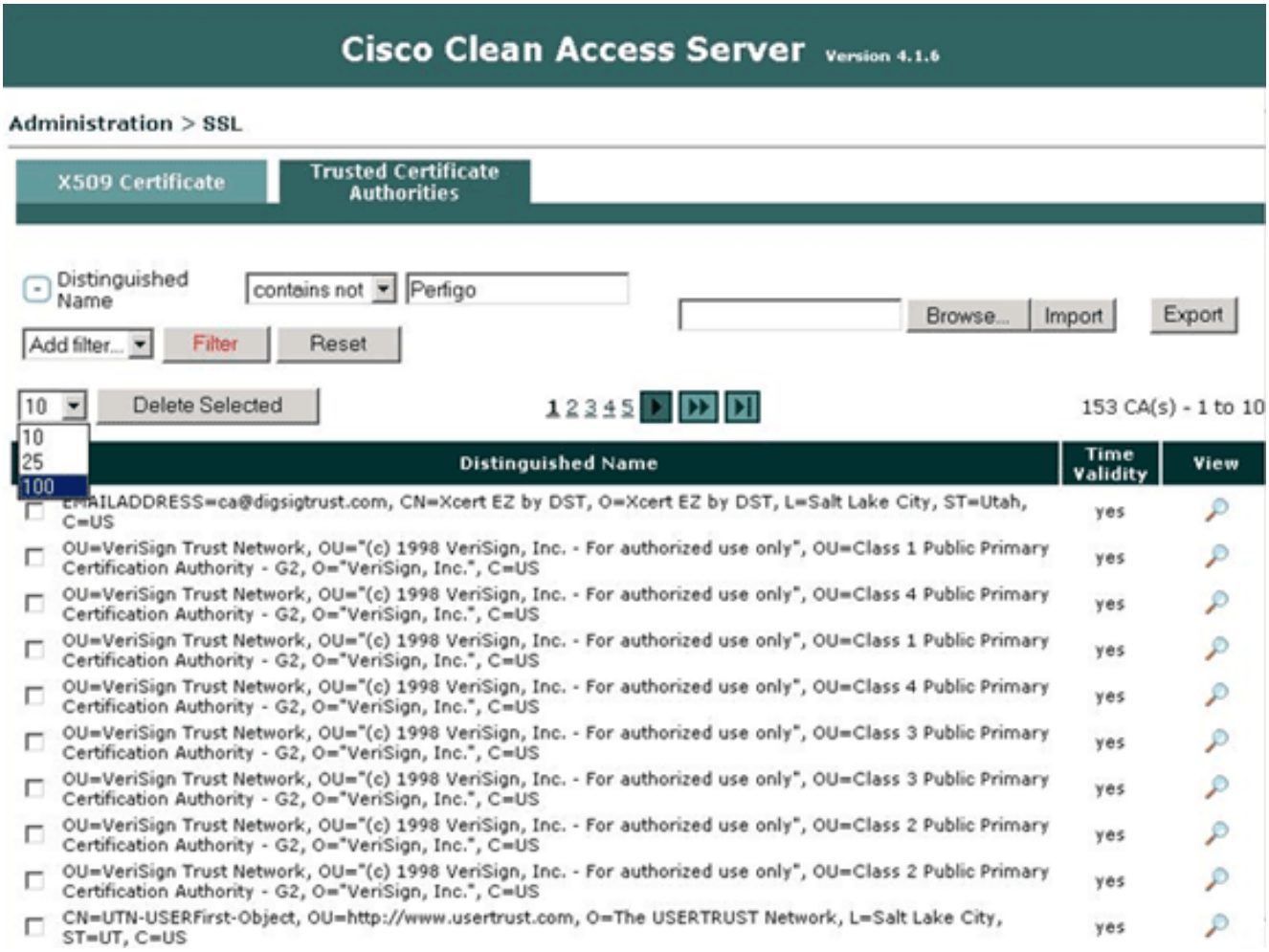
Elija **Nombre distinguido** en la lista desplegable Agregar filtro.



Elija **no contiene** de la lista desplegable que aparece junto a Nombre distinguido.



Escriba Perfigo en el campo de texto y, a continuación, haga clic en **Filtro**.



Elija 100 en la lista desplegable situada junto al botón Eliminar selección.Haga clic en la casilla de verificación debajo de la lista desplegable Eliminar seleccionados para seleccionar todas las autoridades de certificados (CA) de la lista.Haga clic en **Eliminar seleccionados** para eliminar todas las CA de la lista.Continúe haciendo clic en el cuadro y haga clic en **Eliminar seleccionados** hasta que se eliminen todas las CA.

4. Después de quitar todas las CA, se deben importar los certificados raíz e intermedio.En el CAM, vaya a **Administration > CCA Manager > SSL > Trusted Certificate Authorities**.En el CAS, vaya a **Administration > SSL > Trusted Certificate Authorities**.Haga clic en **Examinar**, y elija primero el certificado raíz.**Nota:** El asunto y el emisor deben establecerse en el mismo valor.Haga clic en **Importar** y la CA debe aparecer en la lista siguiente.Realice el mismo procedimiento para cualquier certificado intermedio.
5. Instale los certificados CAS y CAM que realizó la copia de seguridad en el primer paso.En el CAM, abra la interfaz web y vaya a **Administration > CCA Manager > SSL > X509 Certificate**.En el CAS, vaya directamente a la interfaz web a través de https://<CAS IP>/admin, y luego vaya a **Administration > SSL > X509 Certificate**.Elija **Importar certificado** en la lista desplegable.Haga clic en **Examinar** y elija el certificado guardado del paso 1.Haga clic en **Cargar**.Haga clic en **Examinar** de nuevo y elija la clave privada que se guardó del paso 1.Elija **Private Key** en la lista desplegable Tipo de archivo y luego haga clic en **Cargar**.Haga clic en **Verificar e Instalar certificados cargados**.**Nota:** Estos procedimientos no corrigen este mensaje de error:

```
SEVERE: SSLFilter:access deniedCN=cas1.domain.com,
        OU=Information Technologies, O=Company, ST=State,
        C=US:Netscape cert type does not permit use for SSL client
```

Si los registros contienen este mensaje, debe ponerse en contacto con el proveedor de

certificados. El certificado se debe volver a emitir con el campo Tipo de certificado de Netscape establecido tanto en el servidor SSL como en el cliente SSL.

Información Relacionada

- Página de soporte del dispositivo Cisco NAC
- Soporte Técnico y Documentación - Cisco Systems