Cisco NAC Appliance (Clean Access) Login Issue

Document ID: 91836

Contents

Introduction

This document describes the Cisco NAC Appliance (Clean Access) login prompt issue for multiple users that attempt to log into a public computer system.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Problem 1

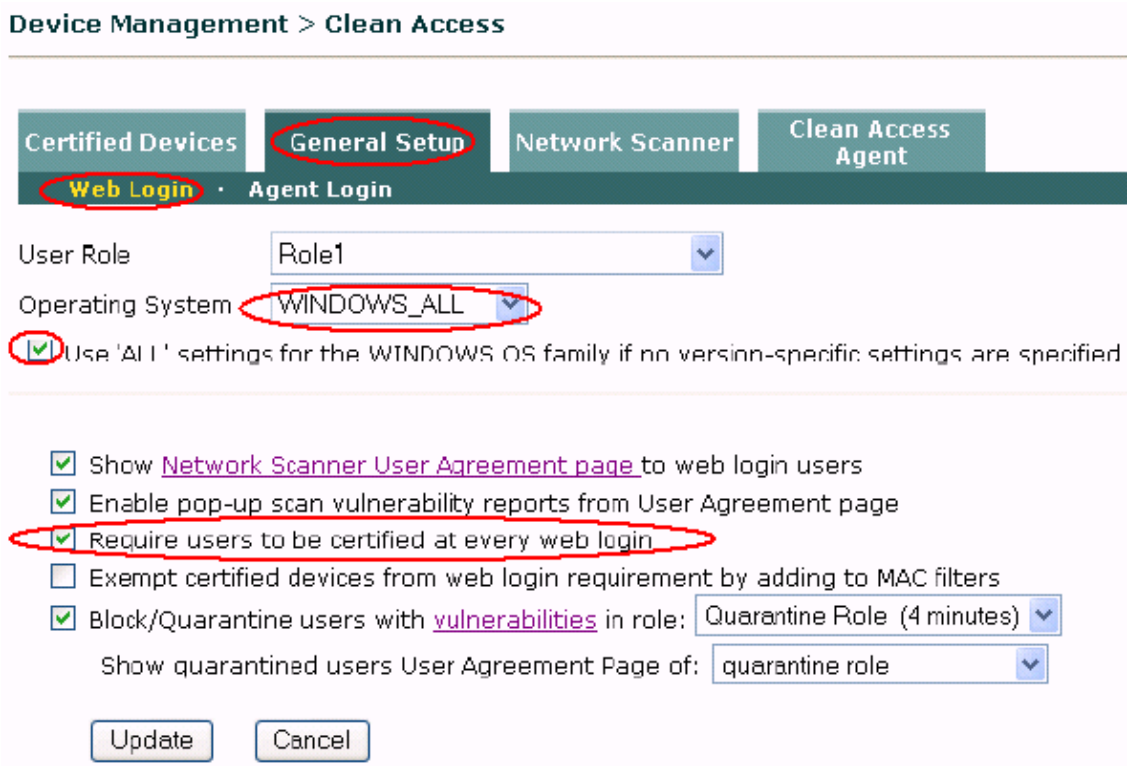
The Clean Access Server (CAS) covers several users who try to get access from a public computer. This issue occurs when a user logs in through a web portal to the CAS and then logs out. When the next user uses the same public computer to login, the prompt does not appear.

Solution

Complete these steps in order to resolve this issue:

1. From your Cisco Clean Access Manager (CAM), choose **Device Management > Clean Access > General Setup**.

2. Click **Web Login**, and choose a user role from the User Role drop−down list. This example uses *Role1*.



3. Make sure that if Operating System is set to **WINDOWS ALL** that you also have **Use ALL settings for the WINDOWS OS family if no version−specific settings are specified** selected.
4. Click the check box for **Require users to be certified at every web login**. This check box forces the user to go through network scanning every time they access the network.

   Note: If disabled (default), users only need to be certified the first time they access the network, or until their MAC address is cleared from the Certified List.
5. Click **Update**.

Problem 2

You might receive this error when you access the CAS through 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.
```

Solution

You can reissue the certificates on CAS and CAM in order to resolve this issue.

Problem 3

Refer to the information in the solution section if you receive this error:

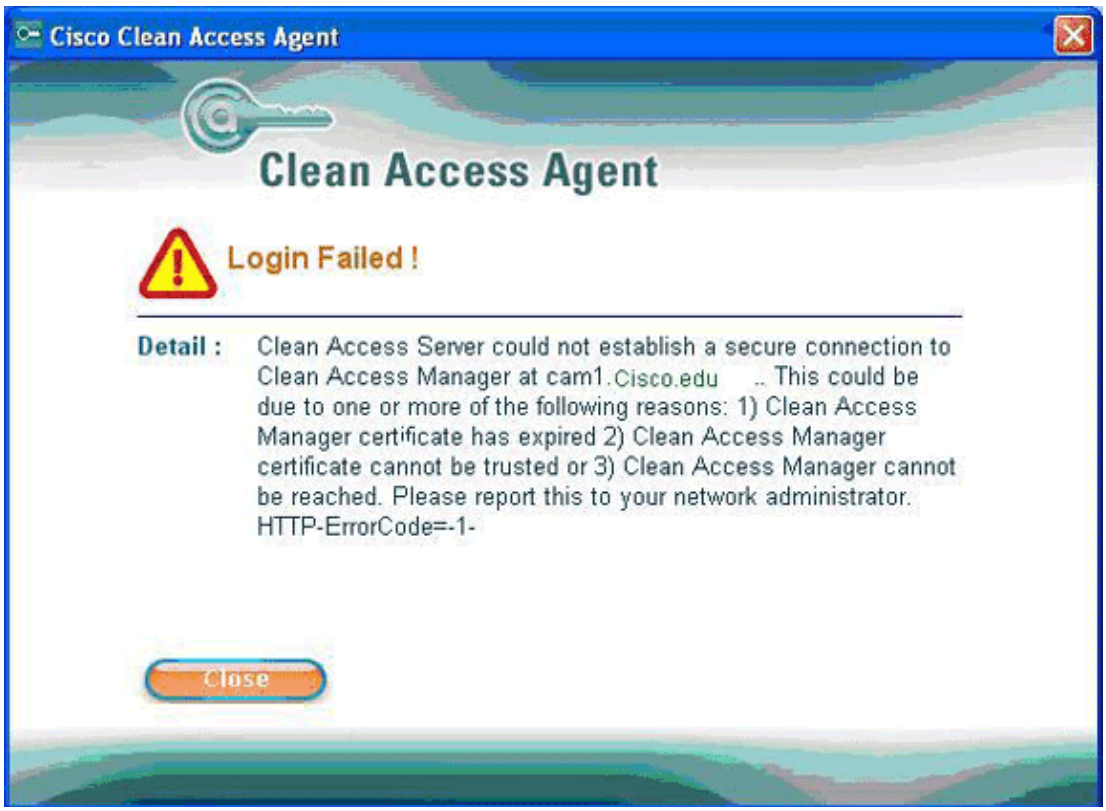
```
Cisco Clean Access Agent is having problem communicate with NAC appliance server.
This could be course by the SSL. Please make sure the certificate on the NAC appliance
server is valid (use Domain name and date/time Must not expire). If the NAC Appliance
uses the temporary certificate, you have to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

Solution

This error is seen on Mac OS specifically. The root cause for the issue is that the CAS certificate needs to be issued to a fully qualified domain or host name in order to be validated in Mac OS X, and the client needs to have a proper root certificate.

Problem 4

You might receive this error:



Solution

The cause for this error message is SSL certificate issued by CAM to a host name that the CAS could not resolve. You can change it to the IP address in order to resolve the issue.

Problem 5

NAC might automatically log out users after a few minutes.

Solution

The CAS logs out the user if it does not receive any packets from the user for the duration of the heartbeat timer. In order to make the CAS wait a longer period of time before it logs out the user, you can set the *heartbeat timer* to a higher value. In order to increase the vale of the heartbeat timer, go to **CAS > Miscellaneous > Heartbeat Timer**.

Problem 6

You might receive this error:

Network Error! Detail: The server response could not be parsed.[12152]

Solution

Complete these steps in order to resolve this issue:

1. Open Internet Explorer.
2. Click **Tools**.
3. Choose **Internet Options**.
4. Click the **Content** tab.
5. Click **Clear SSL State**.

   This step clears the certificate for Internet Explorer.
6. Close and reopen Internet Explorer, and then try to log in again.

Related Information

- **Cisco NAC Appliance (Clean Access)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jun 13, 2007 Document ID: 91836