ActivIdentity® ActivID™ Card Management System and Juniper® Secure Access

Integration Handbook

Document Version 2.0 | Released | May 2, 2012

ACTIVIDENTITY
part of HID Global

Table of Contents

1.0 Introduction

The Juniper® Networks SA Series SSL VPN Appliances enable remote and mobile employees, customers, and partners to gain secure access to corporate Virtual Private Network resources and applications. Providing secure access via a VPN over existing Internet connections requires strong, two-factor authentication to protect resources. The ActivIdentity solutions that work with Juniper Networks incorporate SSL VPN solutions with versatile, strong authentication that is flexible, scalable, and simple to manage.

1.1 Scope of Document

This document explains how to configure the ActivIdentity® ActivID™ Card Management System Appliance and Juniper Networks Secure Access (SA) Series of appliances to enable client authentication via certificate and smart cards.

1.2 Prerequisites

- ActivIdentity ActivID CMS Appliance installed and Root CA certificate created.
- Juniper SA version 7.1.x installed and configured.
- Users have smart cards issued by the CMSA Appliance.

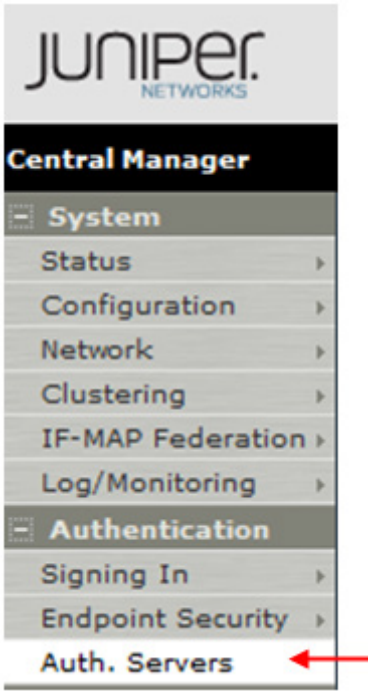
2.0 Juniper Secure Access Configuration

This chapter describes how to configure Juniper Secure Access for use with ActivIdentity CMS. When a user signs into a Juniper SA Series appliance, the user specifies an authentication realm, which is associated with a specific authentication server. The Juniper SA Series appliance forwards the user's credentials to this authentication server to verify the user's identity.

You will create a new authentication server (a certificate server).

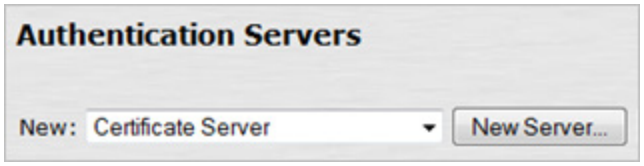
2.1 Procedure 1: Create New Certificate Server Instance

To define a certificate server instance, perform the following steps (this will create a new certificate server instance on the SA Series SSL VPN appliance).



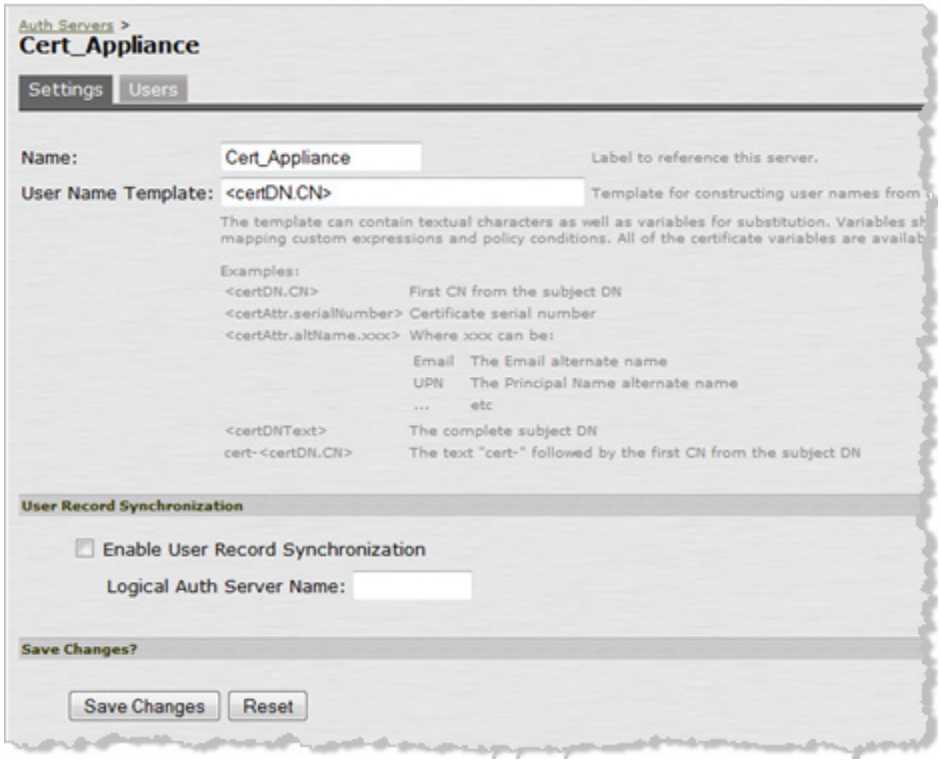
Getting Started

1. In the Admin console, expand the **Authentication** menu, and then click **Auth. Servers**.



2. From the **New** drop-down list, select Certificate Server, and then click **New Server**.

   The following dialog is displayed.

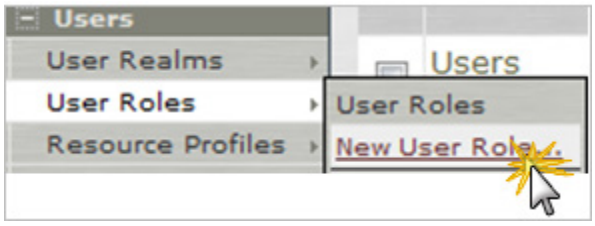


- **Name**—Specify a name to identify the server instance.
- **User Name Template**—Specify the appropriate template for constructing user names.

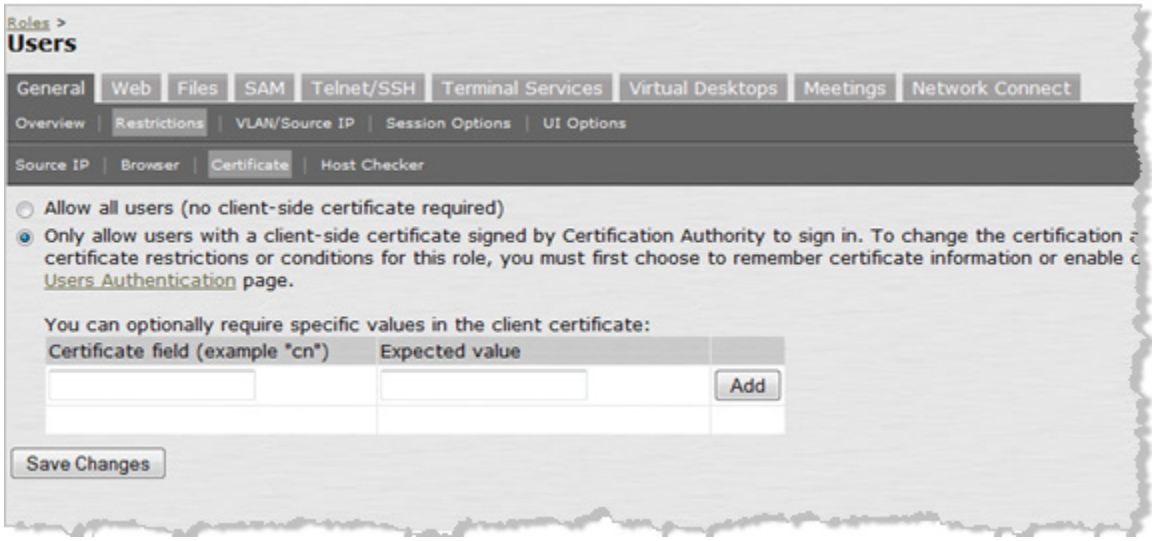
3. Click **Save Changes**.

2.2 Procedure 2: Define Juniper User Role(s)

A user role is an entity that defines user session parameters, personalization settings, and enabled access features.



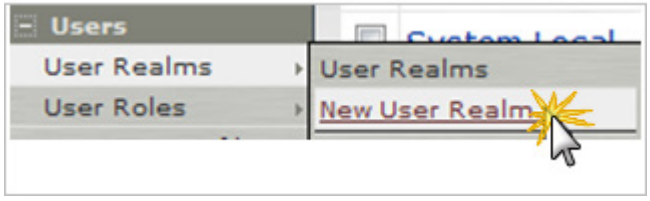
1. From the Admin console, expand the **Users** menu, point to **User Roles**, and then click **New User Role**.
2. Configure the new user role according to your requirements.



3. Use the “certificate” as a restriction. On the **General** tab, click **Restrictions -> Certificate**.
4. Select the option to only allow users with a client-side certificate signed by the CA to sign in.
5. Click **Save Changes**.

2.3 Procedure 3: Define Juniper Authentication Realm

An authentication realm specifies the conditions that users must meet in order to sign in to the SA Series appliance. A realm consists of a grouping of authentication resources.

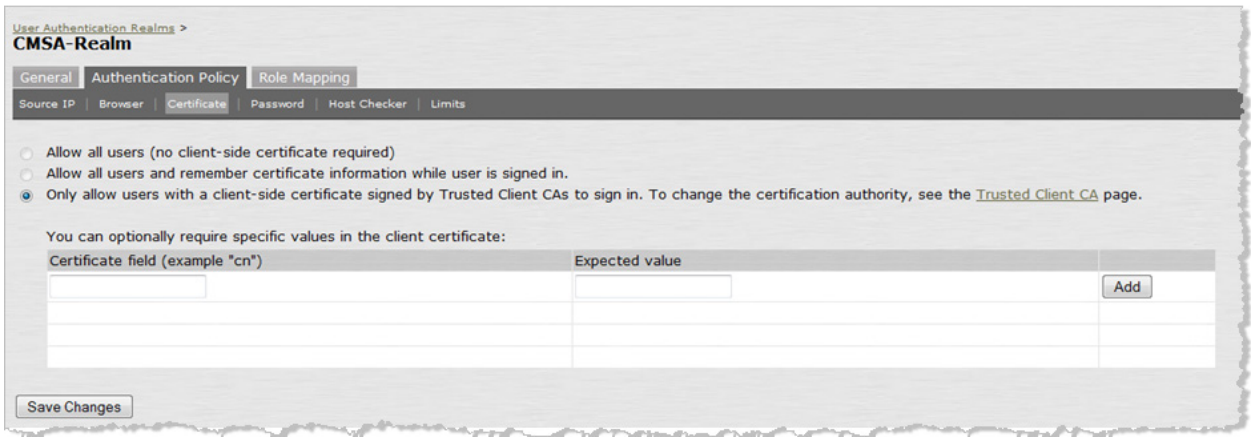


1. From the Admin console, expand the **Users** menu, point to **User Realms**, and then click **New User Realm**.

2. On the **General** tab:
    - **Name**—Enter a name to label this realm.
    - **Description**—Enter a meaningful description.
    - In the **Servers** section:
        - Select an option from the **Authentication** drop-down list to specify an authentication server to use for authenticating users who sign in to this realm (for example, the Cert_Appliance server).
        - Accept the default for **Directory/Attribute**, None.
        - **Accounting**—Accept the default, None.
3. At the bottom of the page, click **Save Changes**.

4. To configure one or more role mapping rules (based on the role defined previously), select the **Role Mapping** tab.

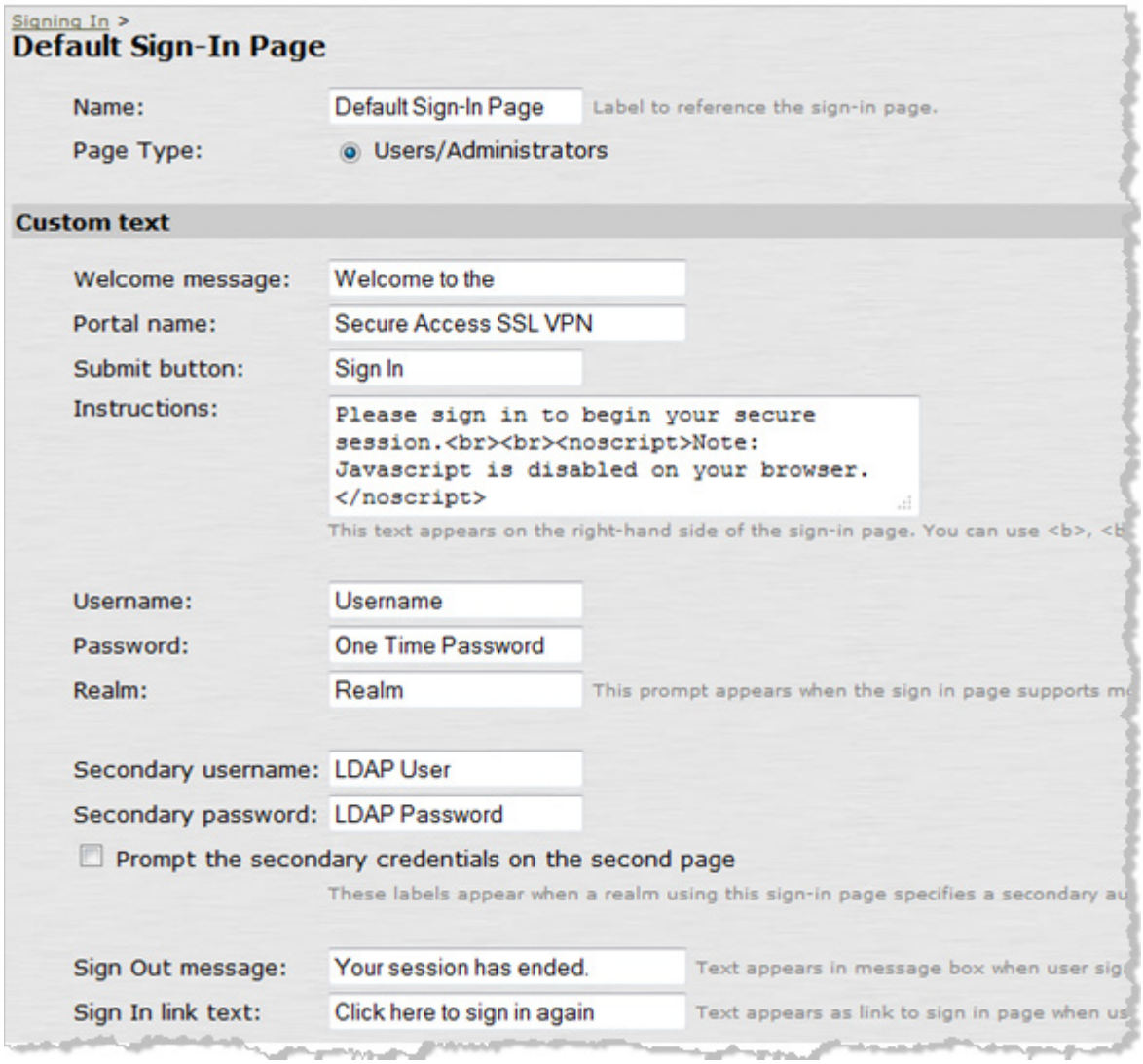
5. Use the certificate as a restriction. Select the **Authentication Policy** tab, and then click **Certificate**.



6. Select the option to only allow users with a client-side certificate signed by a Trusted Client CA to sign in.
7. Click **Save Changes**.

2.4 Procedure 4: Configure New Juniper Sign-In Page

1. From the Admin console, expand the **Authentication** menu, point to **Signing In**, and then click **Sign-in Pages**.



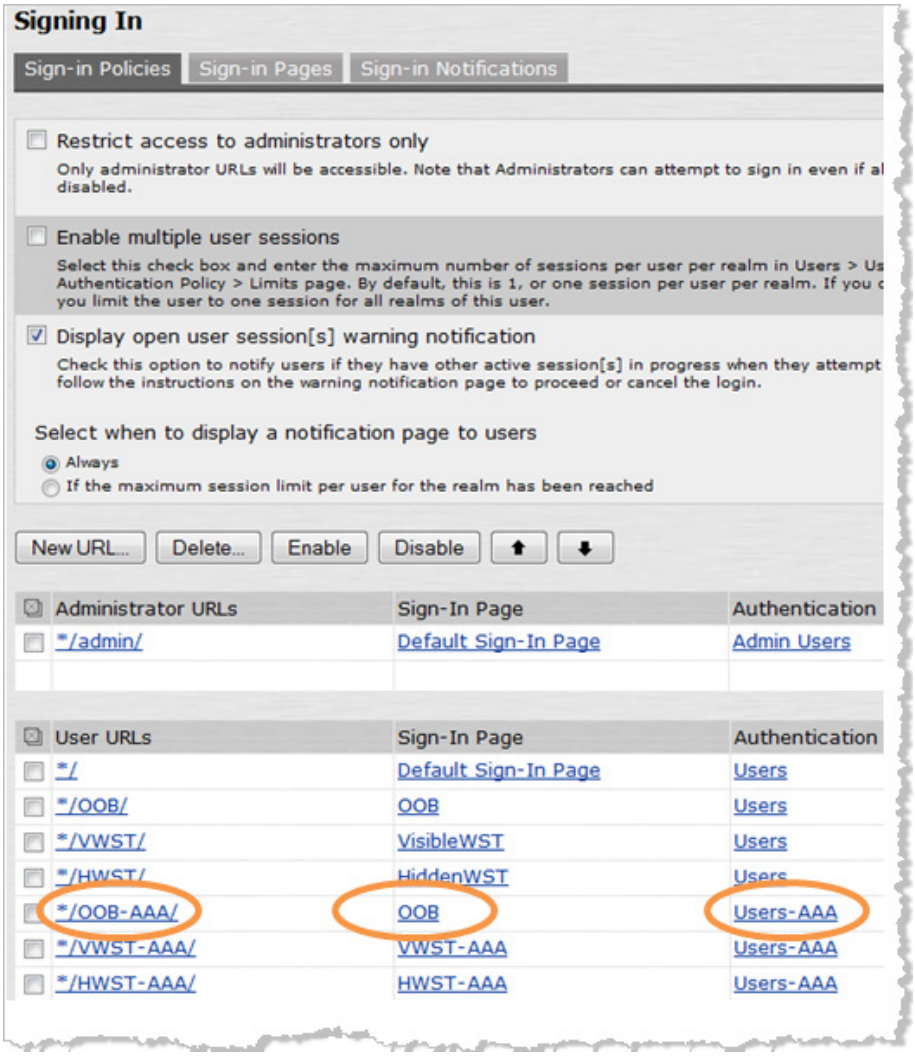
2. Accept the default **Name** and **Page Type**. Accept the defaults in the **Custom text** section of the page.
    - **Welcome message**—The page salutation.

- **Portal name**—Optionally,change this. This will be what comes after *Welcome to the*.
- **Submit button**—The button name.
- **Instructions**—Optionally, change the text you want the user to see on the sign-in page.
- **Username**—This is used by the realm to mask the secondary username on the sign-in page.

2.5 Procedure 5: Juniper Sign-In Policies

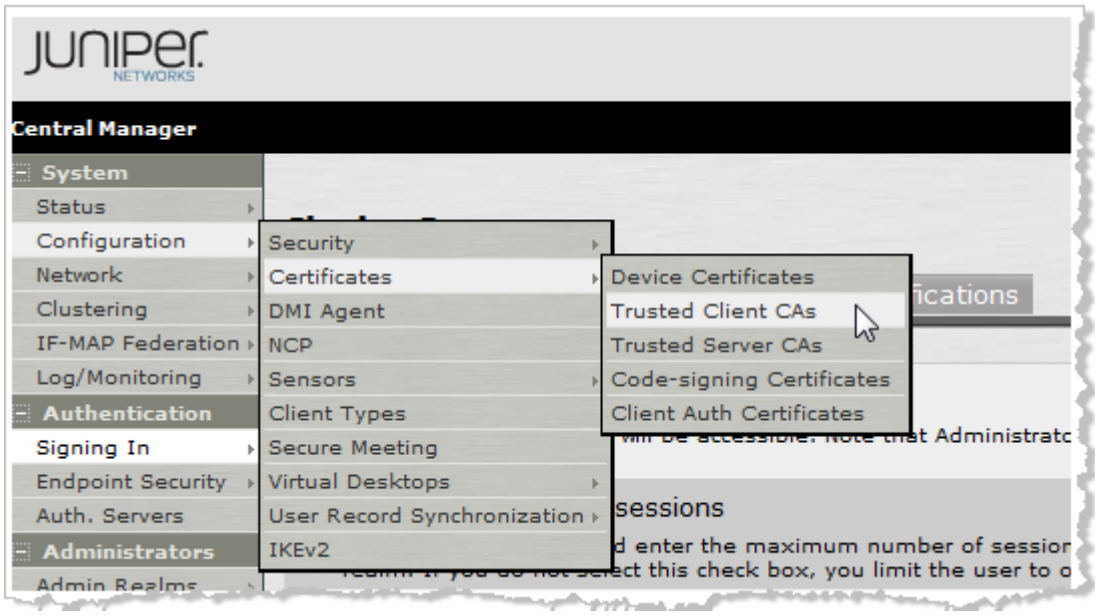
User sign-in policies also determine the realm(s) that users can access.

1. To create or configure user sign-in policies, in the Admin console, expand the **Authentication** menu, point to **Signing In**, and then click **Sign-in Policies**.



2. To create a new sign-in policy, click **New URL**.
3. In the **Sign-in URL** field displayed (not illustrated), enter the URL that you want to associate with the policy. Use the format `<host>/<path>`, where `<host>` is the host name of the Secure Access device and `<path>` is any string you want users to enter.
4. For **Sign-in Page**, select the sign-in page that you want to associate with the policy.
5. For **Authentication realm**, specify which realm(s) map to the policy and how users should pick from amongst realms.
6. Click **Save Changes**.

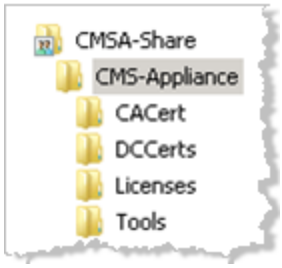
2.6 Procedure 6: Import the CMS Appliance Root CA

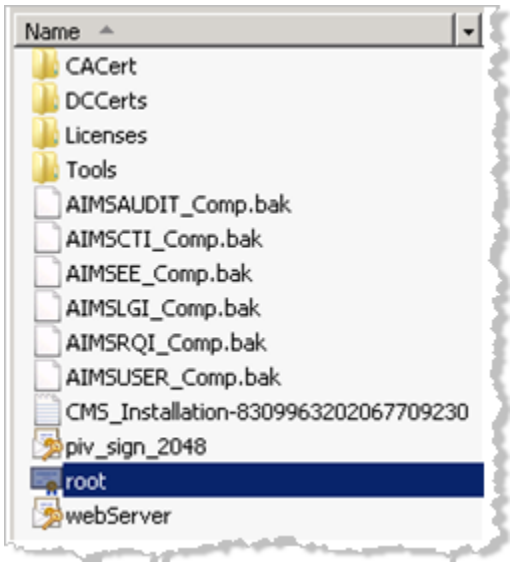


1. Navigate to **Signing In -> Certificates -> Trusted Client CAs**.

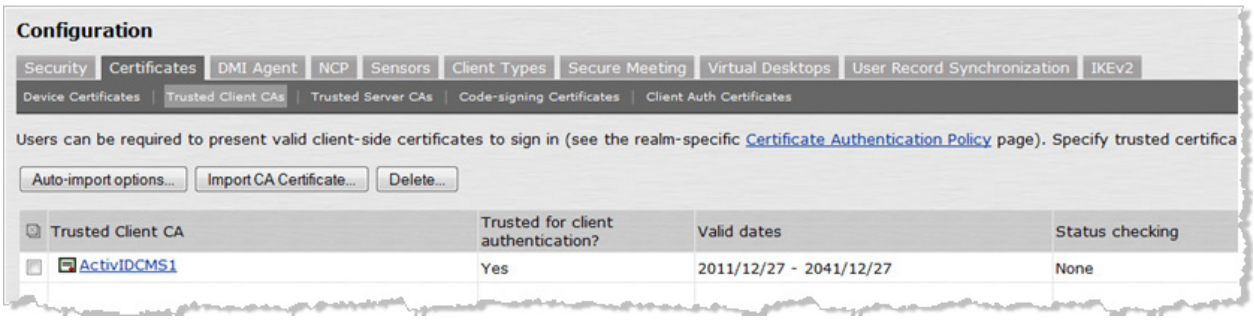
2. In the **Certificate file** section, click the **Browse** button to locate the CMS Appliance Root CA certificate, and then click **Import Certificate**.

   The certificate is located as illustrated next:



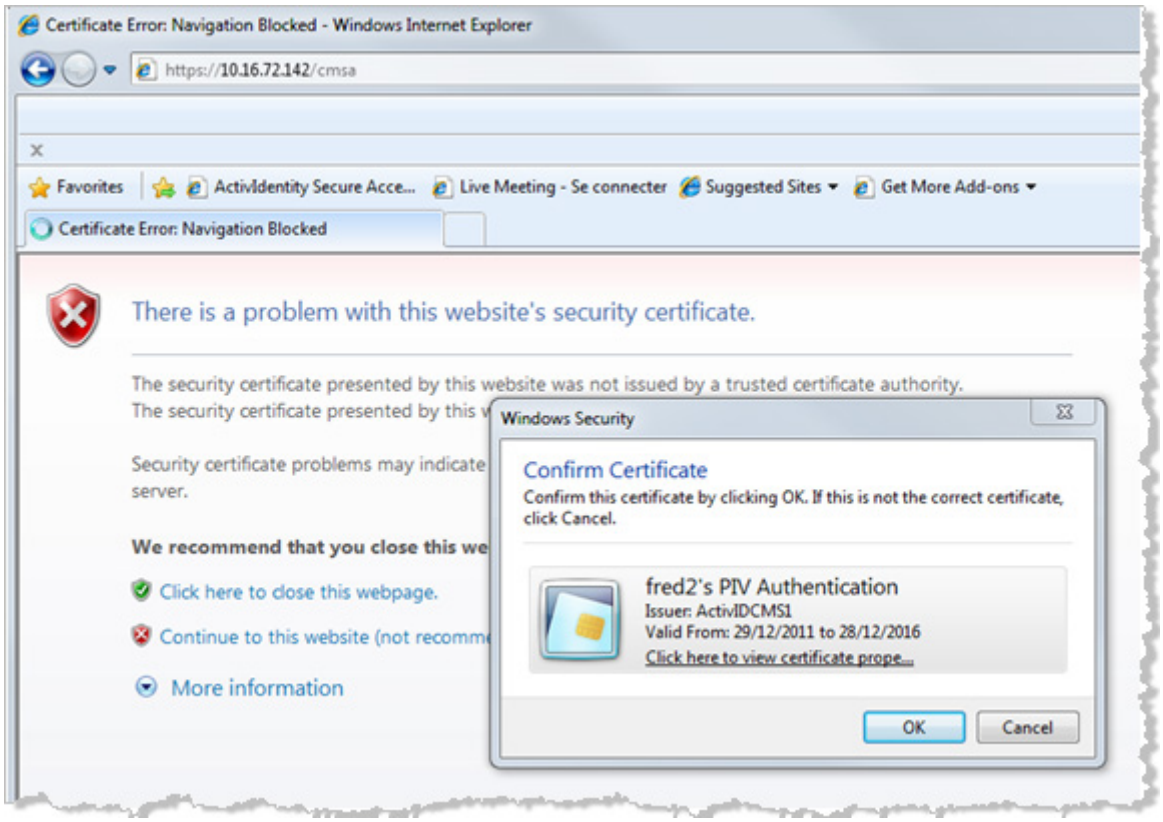


CMSA-Share -> CMS-Appliance

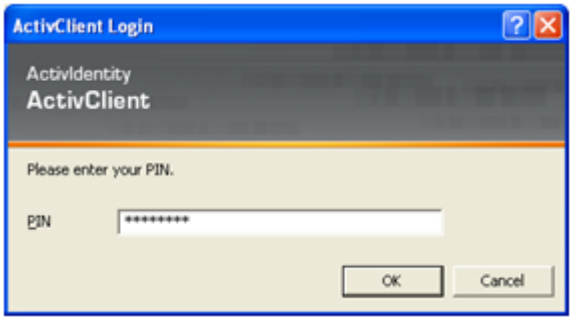


3.0 Authentication with a Smart Card and Client Certificate in the Sign-In Page.

1. The user launches the Juniper User Portal.



2. The user is prompted to confirm the certificate, and then clicks **OK**.



3. The user enters a **PIN**, and then clicks **OK**.

Americas +1 510.574.0100
US Federal +1 571.522.1000
Europe +33 (0) 1.42.04.84.00
Asia Pacific +61 (0) 2.6208.4888
Email info@actividentity.com
Web www.actividentity.com

Legal Disclaimer