



# ActivIdentity® ActivID™ Card Management System and Juniper® Secure Access Integration Handbook

Document Version 2.0 | Released | May 2, 2012

## Table of Contents

1.0	Introduction .....	3
1.1	Scope of Document.....	3
1.2	Prerequisites .....	3
2.0	Juniper Secure Access Configuration.....	4
2.1	Procedure 1: Create New Certificate Server Instance .....	4
2.2	Procedure 2: Define Juniper User Role(s) .....	5
2.3	Procedure 3: Define Juniper Authentication Realm .....	6
2.4	Procedure 4: Configure New Juniper Sign-In Page .....	9
2.5	Procedure 5: Juniper Sign-In Policies .....	10
2.6	Procedure 6: Import the CMS Appliance Root CA.....	12
3.0	Authentication with a Smart Card and Client Certificate in the Sign-In Page.....	14

## 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.

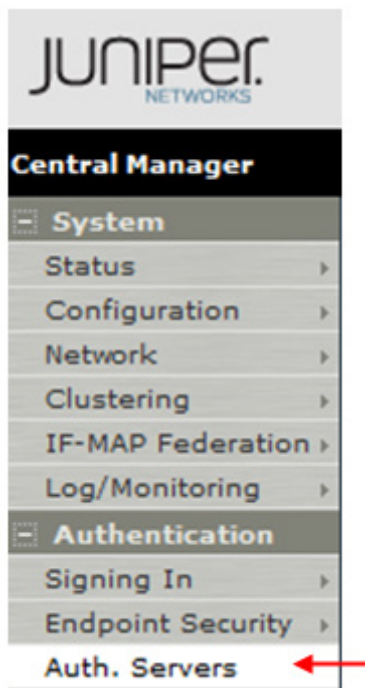
## 2.0 Juniper Secure Access Configuration

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).

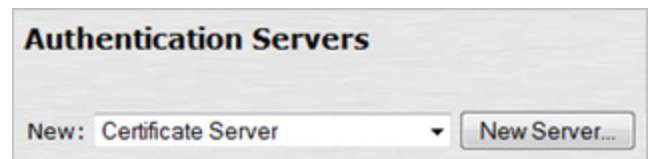
### 2.1 Procedure 1: Create New Certificate Server Instance

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.

**Auth Servers > Cert\_Appliance**

**Settings Users**

**Name:**  Label to reference this server.

**User Name Template:**  Template for constructing user names from certificate attributes.

The template can contain textual characters as well as variables for substitution. Variables are mapped to certificate attributes and policy conditions. All of the certificate variables are available.

Examples:

<certDN.CN>	First CN from the subject DN
<certAttr.serialNumber>	Certificate serial number
<certAttr.altName.xxx>	Where xxx can be:
Email	The Email alternate name
UPN	The Principal Name alternate name
...	etc
<certDNText>	The complete subject DN
cert-<certDN.CN>	The text "cert-" followed by the first CN from the subject DN

**User Record Synchronization**

☐ Enable User Record Synchronization

Logical Auth Server Name:

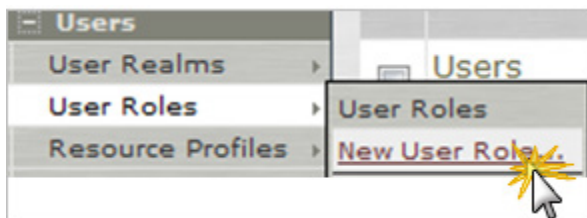
**Save Changes?**

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

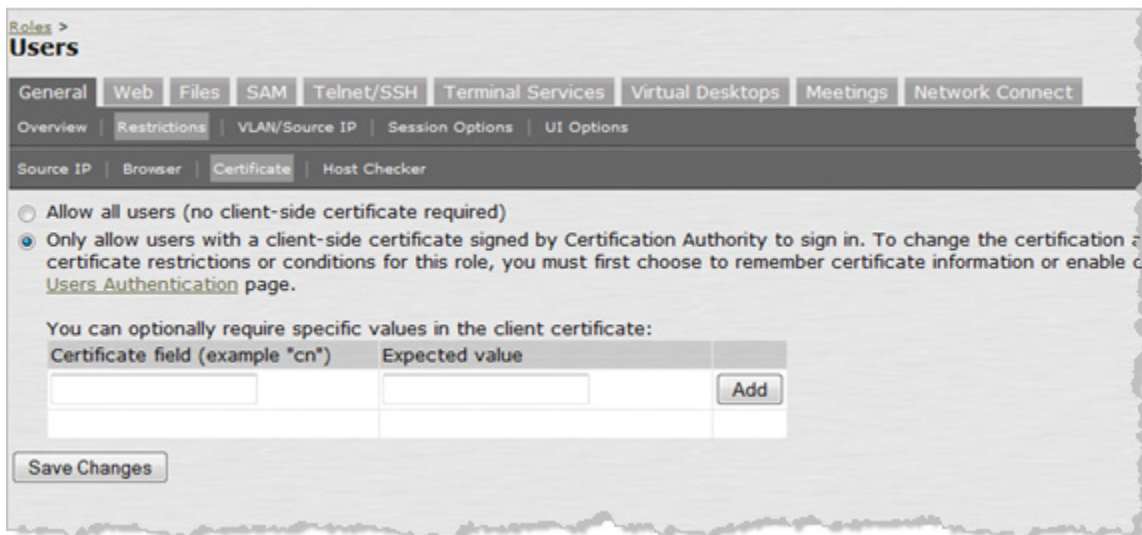
3. Click **Save Changes**.

## 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.



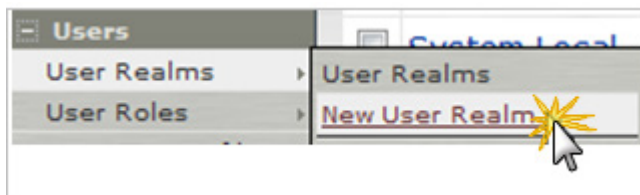
1. From the Admin console, expand the **Users** menu, point to **User Roles**, and then click **New User Role**.
2. Configure the new user role according to your requirements.



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**.

User Authentication Realms >  
**CMSA-Realm**

General | Authentication Policy | Role Mapping

Name: CMSA-Realm  
Description:

☐ When editing, start on the Role Mapping page

**Servers**

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: Cert\_Appliance  
Directory/Attribute: None  
Accounting: None

☐ Additional authentication server

☐ Dynamic policy evaluation

**Other Settings**

Authentication Policy: Certificate restrictions  
Password restrictions

Role Mapping: 1 Rule

**Save changes?**

Save Changes

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.

User Authentication Realms > CMSA-Realm

General Authentication Policy **Role Mapping**

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

New Rule... Duplicate Delete Up Down Save Changes

When users meet these conditions	assign these roles	Rule Name	Stop
1. username is ***	→ Users	All	

When more than one role is assigned to a user:

☒ Merge settings for all assigned roles

☐ User must select from among assigned roles

☐ User must select the sets of merged roles assigned by each rule

Note: Users that do not meet any of the above rules will not be able to sign into this realm.

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

User Authentication Realms > CMSA-Realm

General Authentication Policy **Role Mapping**

Source IP Browser **Certificate** Password Host Checker Limits

☐ Allow all users (no client-side certificate required)

☐ Allow all users and remember certificate information while user is signed in.

☒ Only allow users with a client-side certificate signed by Trusted Client CAs to sign in. To change the certification authority, see the [Trusted Client CA](#) page.

You can optionally require specific values in the client certificate:

Certificate field (example "cn")	Expected value

Add

Save Changes

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**.

Signing In >

### Default Sign-In Page

Name:  Label to reference the sign-in page.

Page Type: ☒ Users/Administrators

**Custom text**

Welcome message:

Portal name:

Submit button:

Instructions:

This text appears on the right-hand side of the sign-in page. You can use <b>, <b>

Username:

Password:

Realm:  This prompt appears when the sign in page supports m

Secondary username:

Secondary password:

☐ Prompt the secondary credentials on the second page

These labels appear when a realm using this sign-in page specifies a secondary au

Sign Out message:  Text appears in message box when user sig

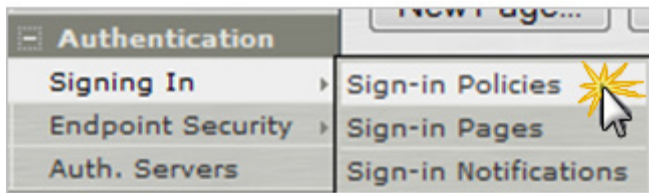
Sign In link text:  Text appears as link to sign in page when us

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**.

### Signing In

**Sign-in Policies** | **Sign-in Pages** | **Sign-in Notifications**

☐ **Restrict access to administrators only**  
Only administrator URLs will be accessible. Note that Administrators can attempt to sign in even if all disabled.

☐ **Enable multiple user sessions**  
Select this check box and enter the maximum number of sessions per user per realm in Users > User Authentication Policy > Limits page. By default, this is 1, or one session per user per realm. If you do not select this option, you limit the user to one session for all realms of this user.

☒ **Display open user session[s] warning notification**  
Check this option to notify users if they have other active session[s] in progress when they attempt to follow the instructions on the warning notification page to proceed or cancel the login.

Select when to display a notification page to users

☒ Always

☐ If the maximum session limit per user for the realm has been reached

New URL... Delete... Enable Disable ↑ ↓

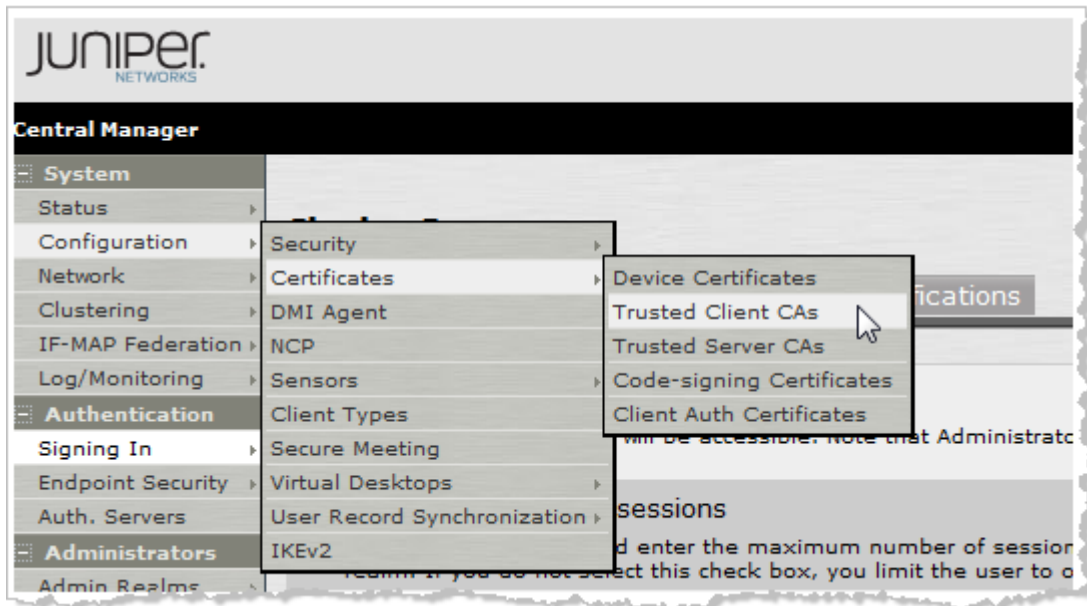
Administrator URLs	Sign-In Page	Authentication
<input type="checkbox"/> <a href="#">*/admin/</a>	<a href="#">Default Sign-In Page</a>	<a href="#">Admin Users</a>

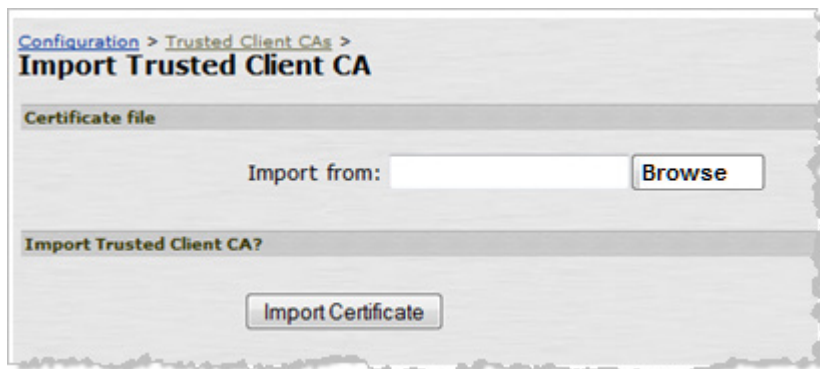
User URLs	Sign-In Page	Authentication
<input type="checkbox"/> <a href="#">*/</a>	<a href="#">Default Sign-In Page</a>	<a href="#">Users</a>
<input type="checkbox"/> <a href="#">*/OOB/</a>	<a href="#">OOB</a>	<a href="#">Users</a>
<input type="checkbox"/> <a href="#">*/VWST/</a>	<a href="#">VisibleWST</a>	<a href="#">Users</a>
<input type="checkbox"/> <a href="#">*/HWST/</a>	<a href="#">HiddenWST</a>	<a href="#">Users</a>
<input type="checkbox"/> <a href="#">*/OOB-AAA/</a>	<a href="#">OOB</a>	<a href="#">Users-AAA</a>
<input type="checkbox"/> <a href="#">*/VWST-AAA/</a>	<a href="#">VWST-AAA</a>	<a href="#">Users-AAA</a>
<input type="checkbox"/> <a href="#">*/HWST-AAA/</a>	<a href="#">HWST-AAA</a>	<a href="#">Users-AAA</a>

- To create a new sign-in policy, click **New URL**.
- 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.
- For **Sign-in Page**, select the sign-in page that you want to associate with the policy.
- For **Authentication realm**, specify which realm(s) map to the policy and how users should pick from amongst realms.
- Click **Save Changes**.

## 2.6 Procedure 6: Import the CMS Appliance Root CA

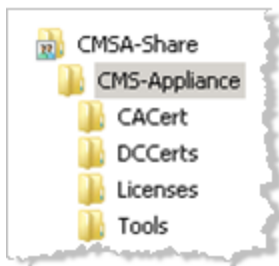


1. Navigate to **Signing In -> Certificates -> Trusted Client CAs**.

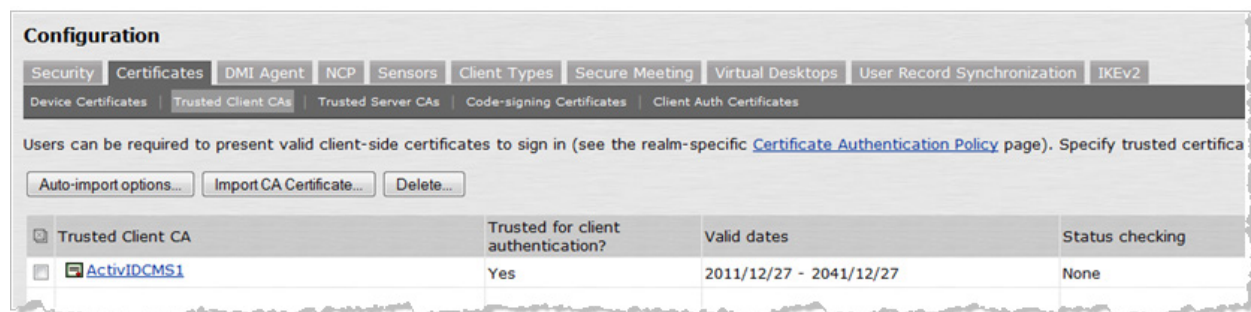
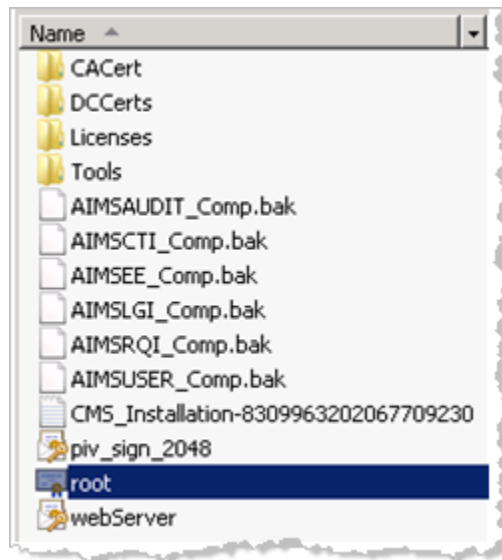


2. In the **Certificate file** section, click the **Browse** button to locate the CMS Appliance Root CA certificate, and then click **Import Certificate**.

The certificate is located as illustrated next:

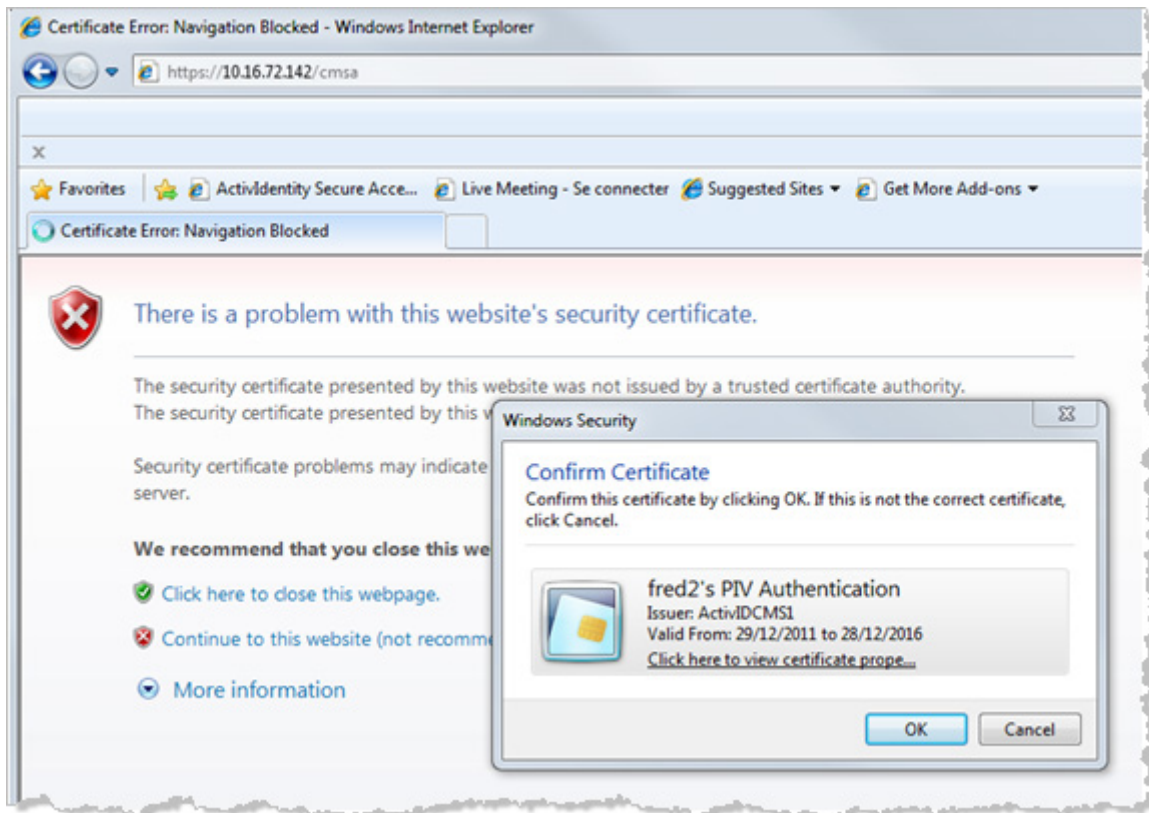


**CMSA-Share -> CMS-Appliance**

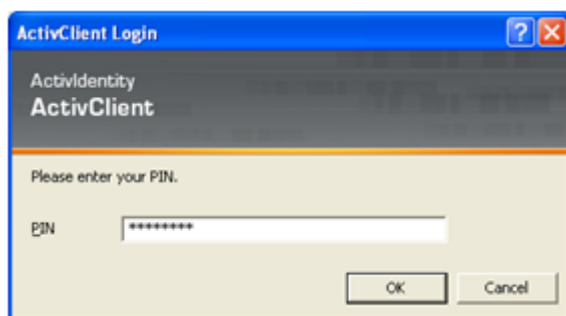


### 3.0 Authentication with a Smart Card and Client Certificate in the Sign-In Page.

1. The user launches the Juniper User Portal.

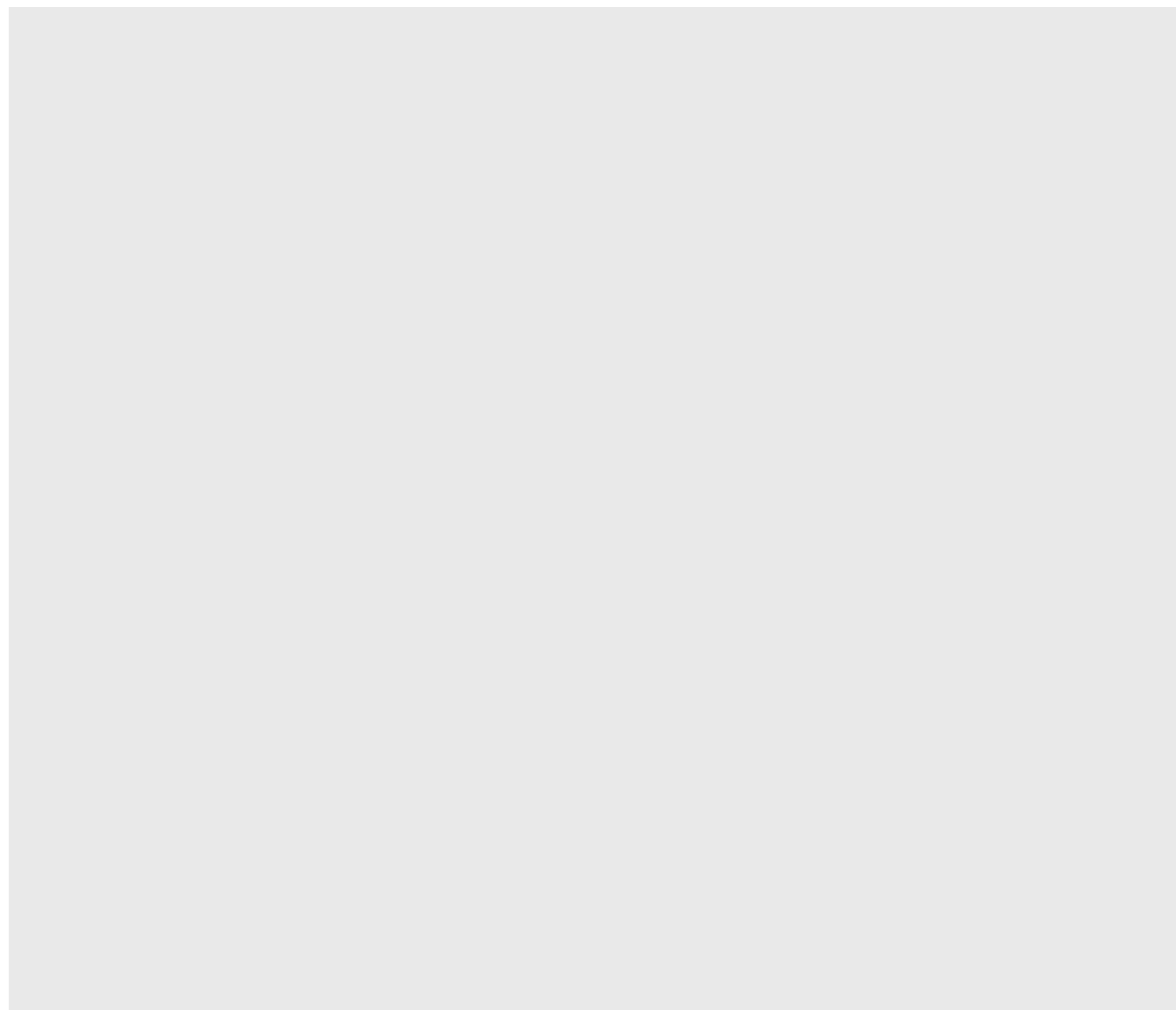


2. The user is prompted to confirm the certificate, and then clicks **OK**.



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





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

### Legal Disclaimer

ActivIdentity, the ActivIdentity (logo), and/or other ActivIdentity products or marks referenced herein are either registered trademarks or trademarks of HID Global Corporation in the United States and/or other countries. The absence of a mark, product, service name or logo from this list does not constitute a waiver of the trademark or other intellectual property rights concerning that name or logo. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The names of other third-party companies, trademarks, trade names, service marks, images and/or products that happen to be mentioned herein are trademarks of their respective owners. Any rights not expressly granted herein are reserved.