# RSA SecurID Access SAML Configuration for Dell SonicWALL E-Class

**Last Modified:** May 11, 2016

Dell SonicWALL E-Class is a secure access gateway to network resources allowing administrator to have tight control of the endpoint.

**Before You Begin**

- Acquire an administrator account to RSA SecurID Access.
- Install the Dell SonicWALL E-Class Appliance.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

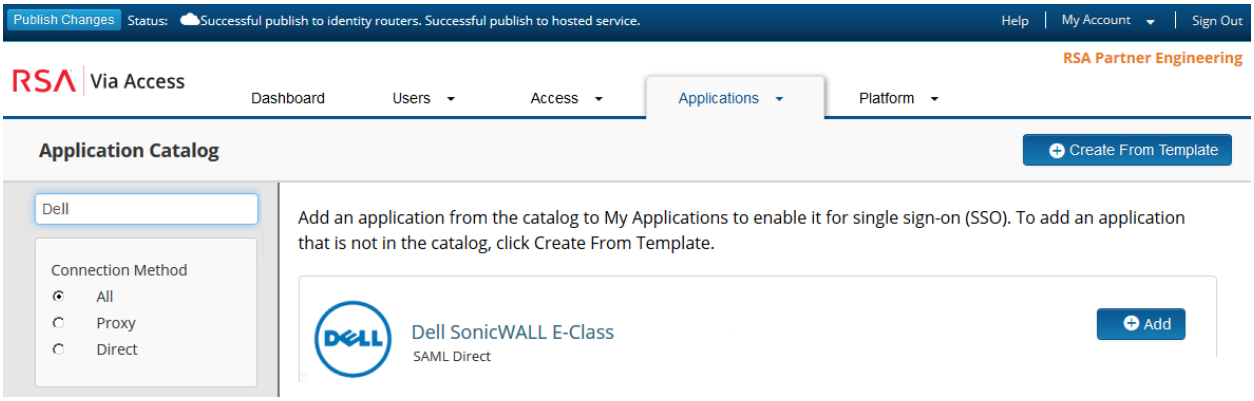
**Procedure**

1. Add the Application in RSA SecurID Access
2. Configure Dell SonicWALL E-Class to Use RSA SecurID Access as an Identity Provider

## Add the Application in RSA SecurID Access

**Procedure**

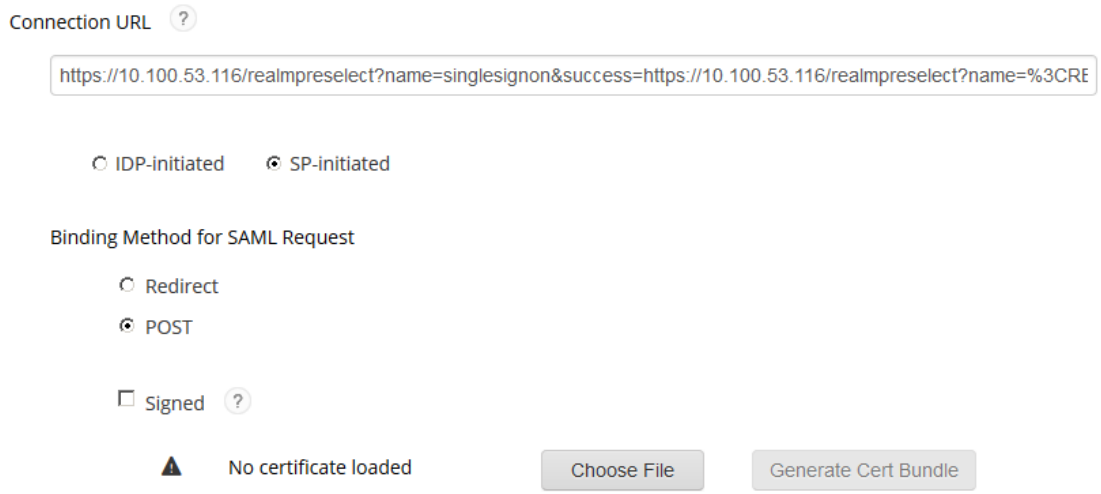
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for the SAML application that you wish to add.



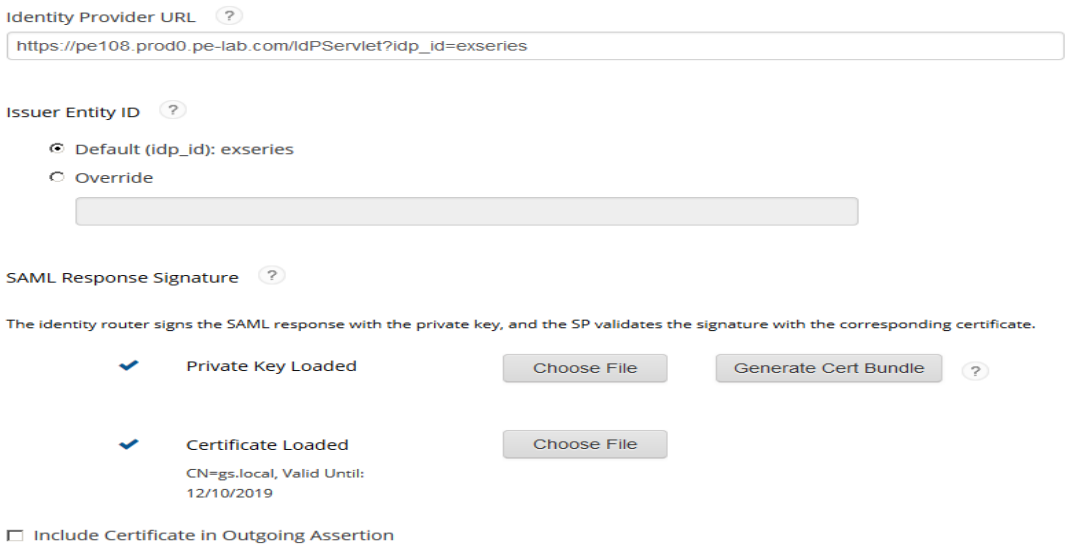
3. On the Basic Information page, specify the application name and click **Next Step**.

**Note: The following SP-initiated configuration works for both SP-initiated and IDP- initiated connections.**

4. On the Connection Profile page, choose **SP–initiated.**
5. Modify the Connection URL. Replace the 2 instances of **<FQDN>** with the full qualified domain name of the SonicWALL. Replace **<REALM>** with the name of the single sign-on realm found on page 10 step 20.
   In this example the SonicWALL address is 10.100.53.116 and the realm name singlesignon.
   https://<FQDN>/realmpreselect?name=<REALM>&success=https://<FQDN>/realmpreselect?name=%3CREALM-NAME%3E&success=/workplace/access/home




6. Scroll down to the **SAML Identity Provider (Issuer)** section.

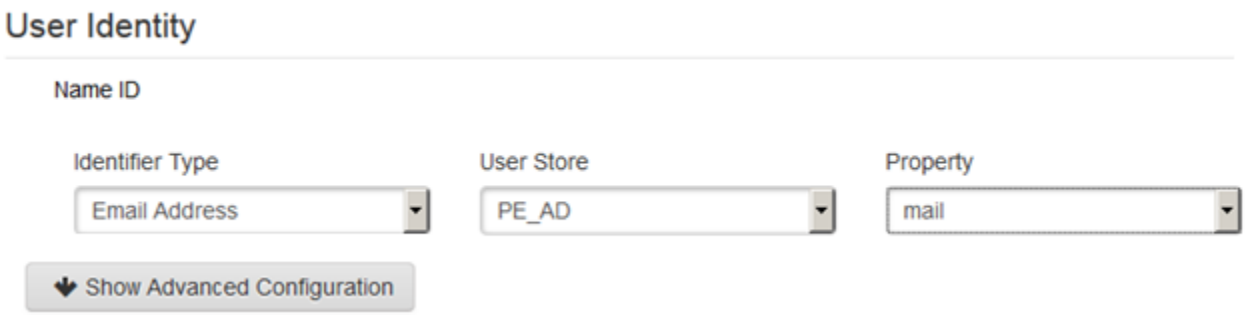



   a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure the SonicWALL E-Class.
   b. Select **Choose File** and upload the private key.
   c. Select **Choose File** and upload the public certificate.

7. Scroll down to the **Service Provider** section.

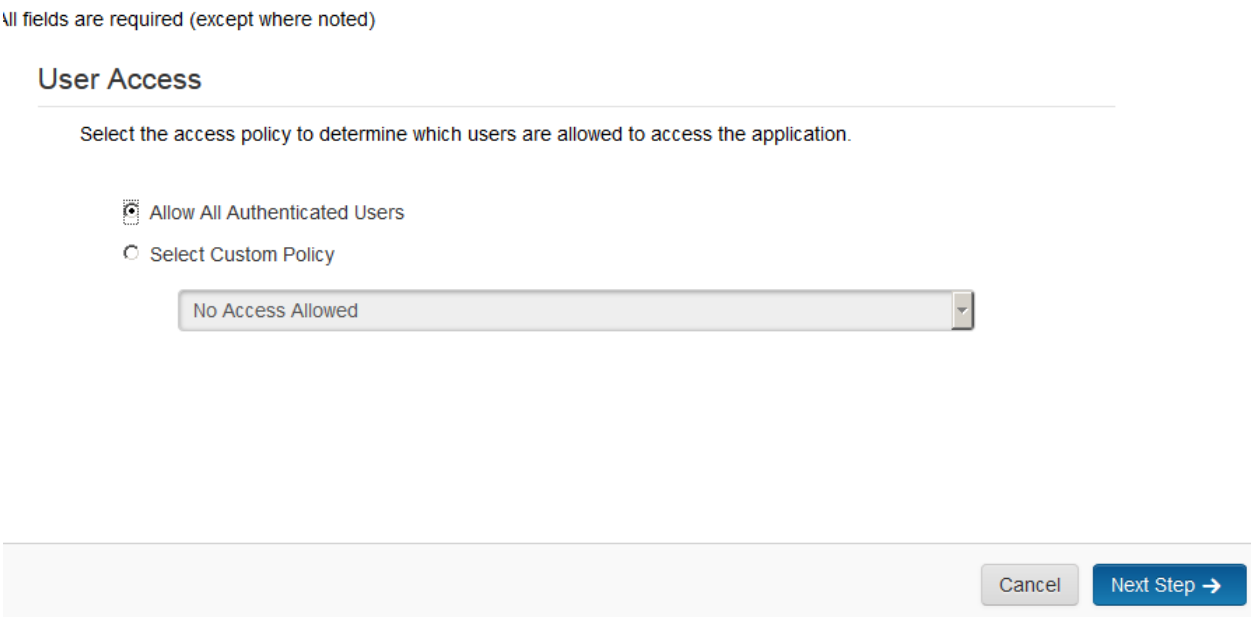

   a. In the **Assertion Consumer Service (ACS) URL** field replace **<FQDN>** with the IP address of your SonicWALL. Example **https://10.100.53.116/saml2ssoconsumer**
   b. In the **Audience (Service Provider Entity ID)** field replace **<SP_Entity_ID>** with the value from page 7 step 11.

8. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email** and **Property** to **mail**.

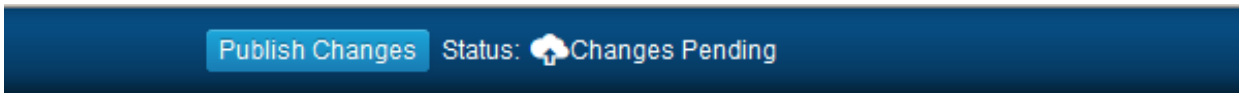



9. Click **Next Step**.

10. On the **User Access** page, select the desired user policy from the drop down list.




11. Click **Next Step**.
12. On the **Portal Display** page, select **Display in Portal**.
13. Click **Save and Finish**.
14. Click **Publish Changes**. Your application is now enabled for SSO.



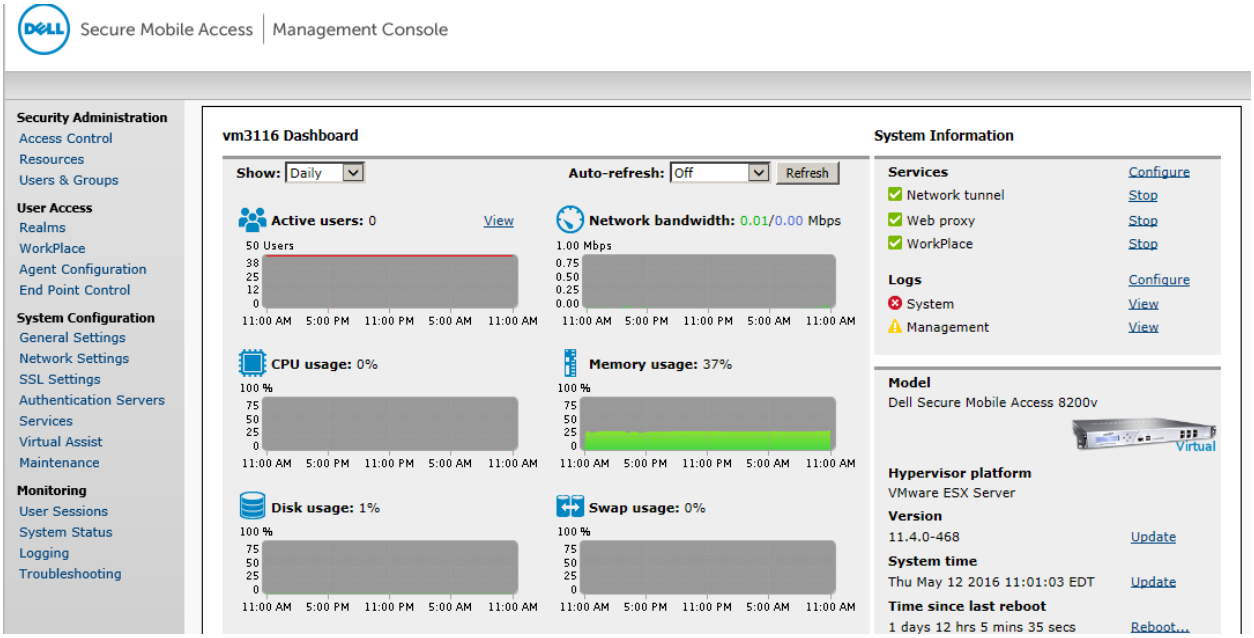

**Next Steps**

[Configure Dell SonicWALL E-Class to Use RSA SecurID Access as an Identity Provider]

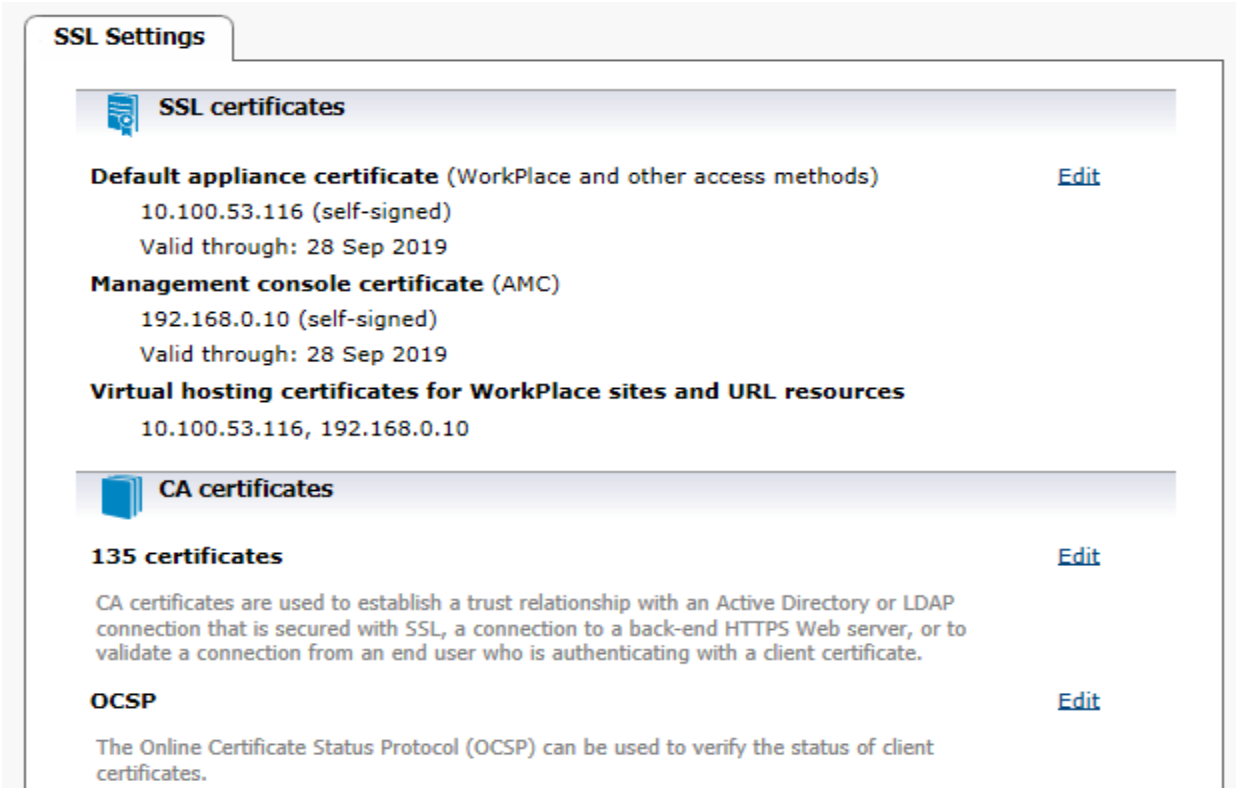
## Configure Dell SonicWALL E-Class to Use RSA SecurID Access as an Identity Provider

**Procedure**

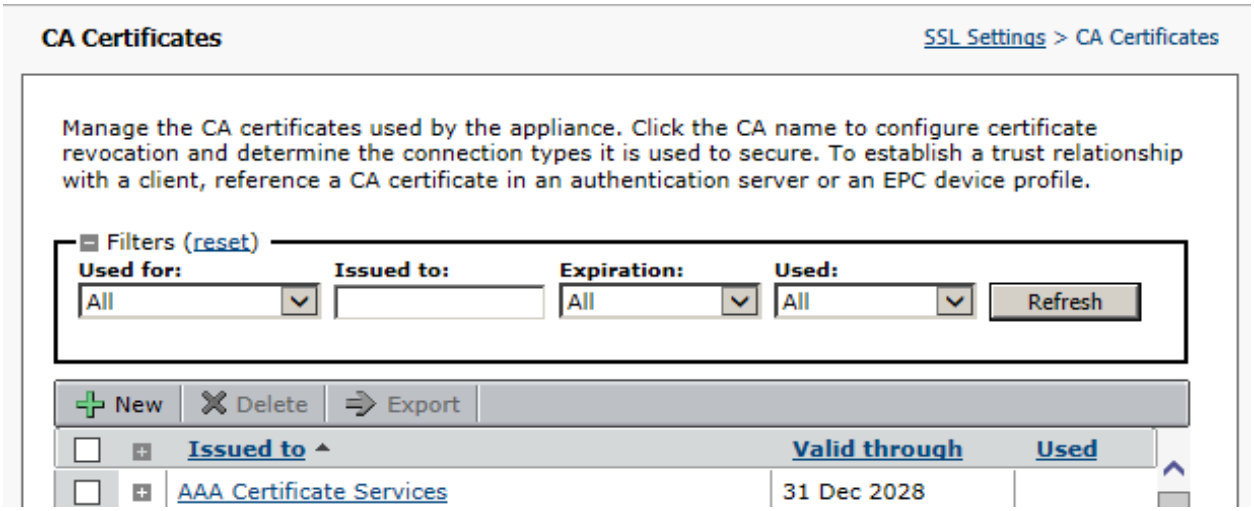
1. Log in to the Aventail Management Console (AMC) as an administrator. The FQDN is the address of the SonicWALL. https://<FQDN>:8443
2. From the left menu, select **System Configuration > SSL Settings**.



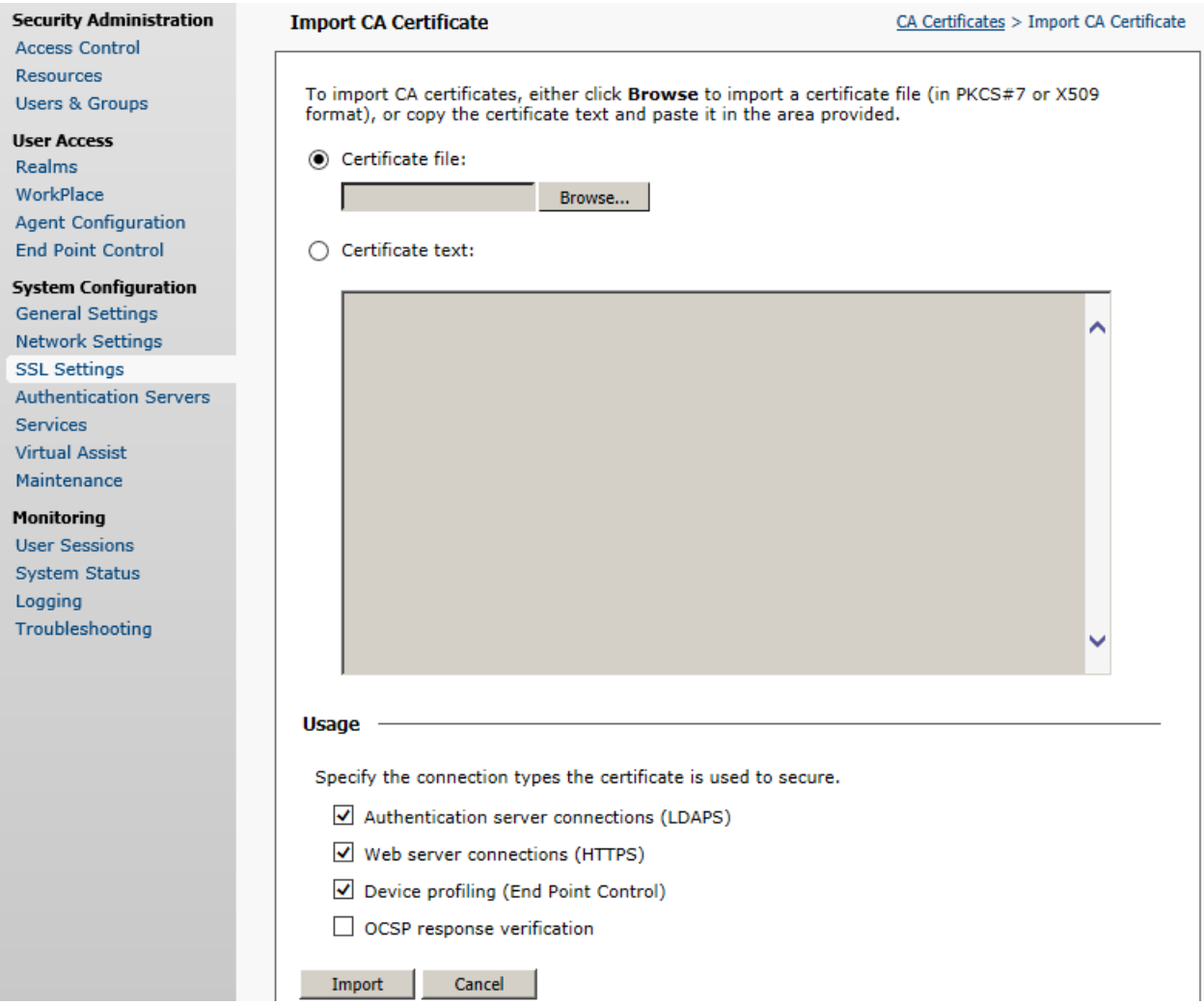

3. Click the first **Edit** under CA certificates.



4. In the CA Certificates window, click **+New**.

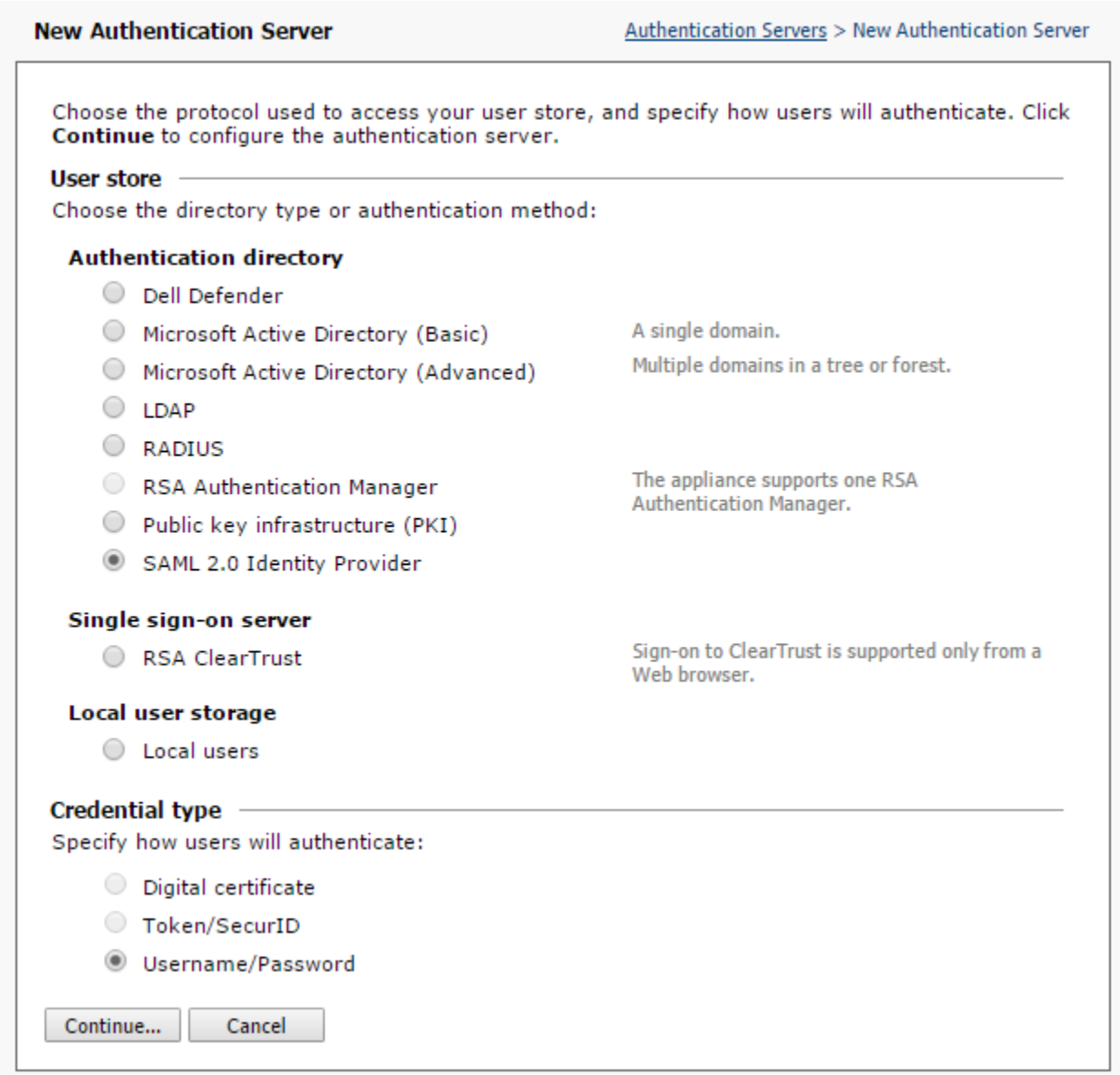



5. Use the **Browse** button and select the RSA SecurID Access certificate .pem file used in step 5c on page 2.



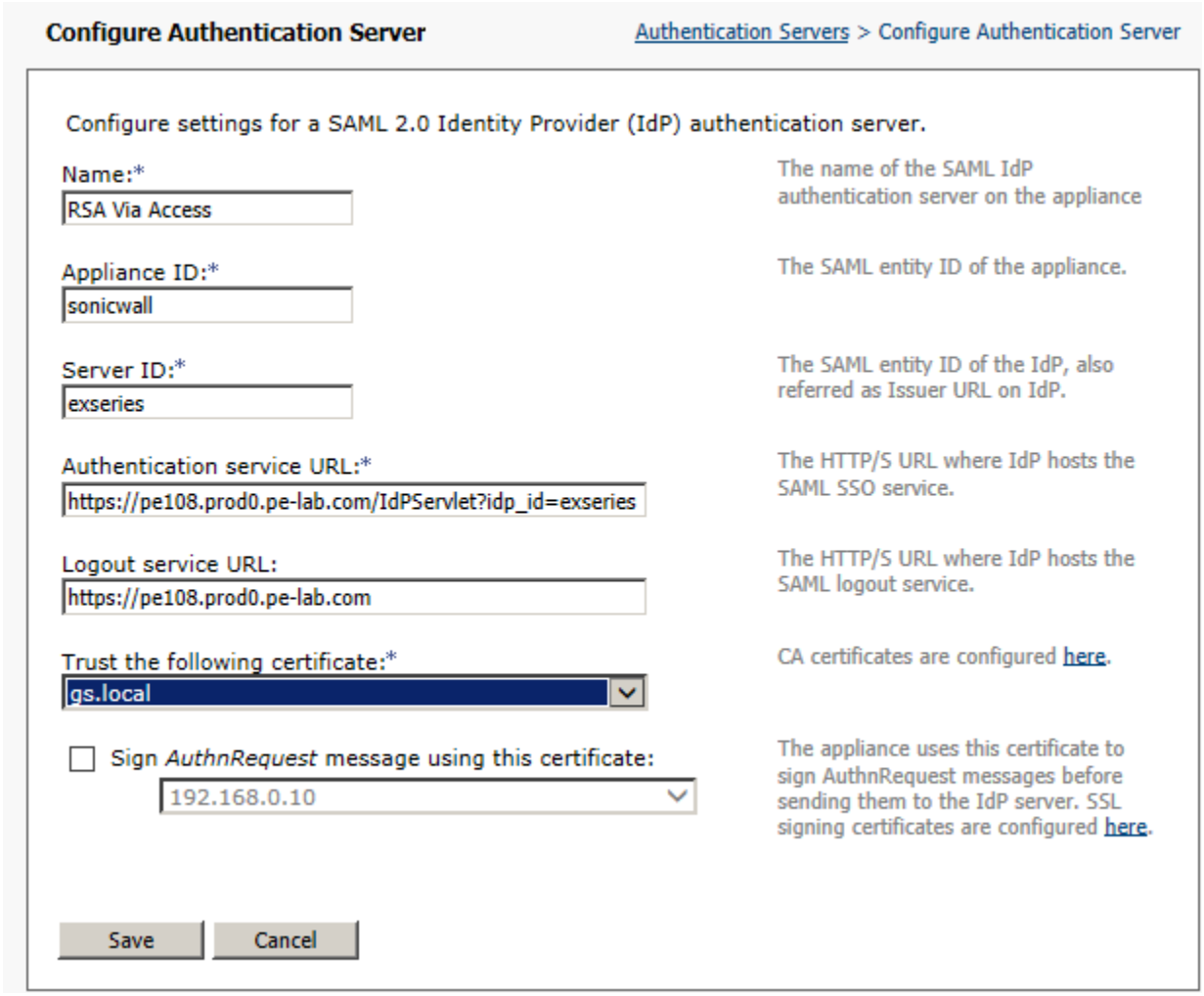

6. Select **Import**.

7. Select **System Configuration > Authentication Servers**.
8. Select **New**.
9. Select **SAML 2.0 Identity Provider**.



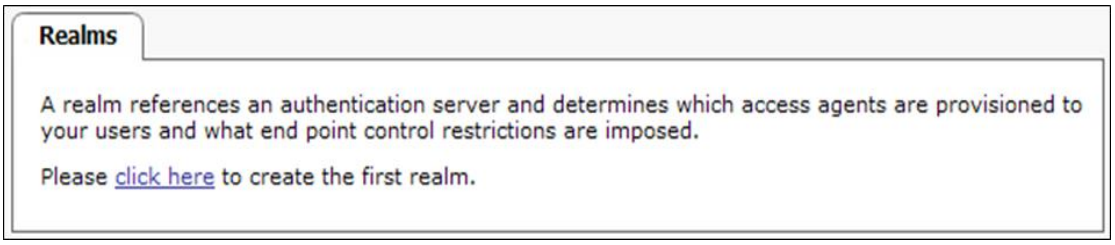

10. Click **Continue**…

11. Enter the name for the SAML IdP.
12. Enter the Service Provider Entity ID in the **Appliance ID** field found on page 3 step 6b.
13. Enter the RSA SecurID Access Entity ID in the **Server ID** field found on page 2 step 5.
14. Enter the RSA SecurID Access Identity URL into the **Authentication service URL** field from page 2 step 5.
15. Enter the **Logout service URL**.
16. Select the RSA SecurID Access certificate you imported on page 6 step 6.

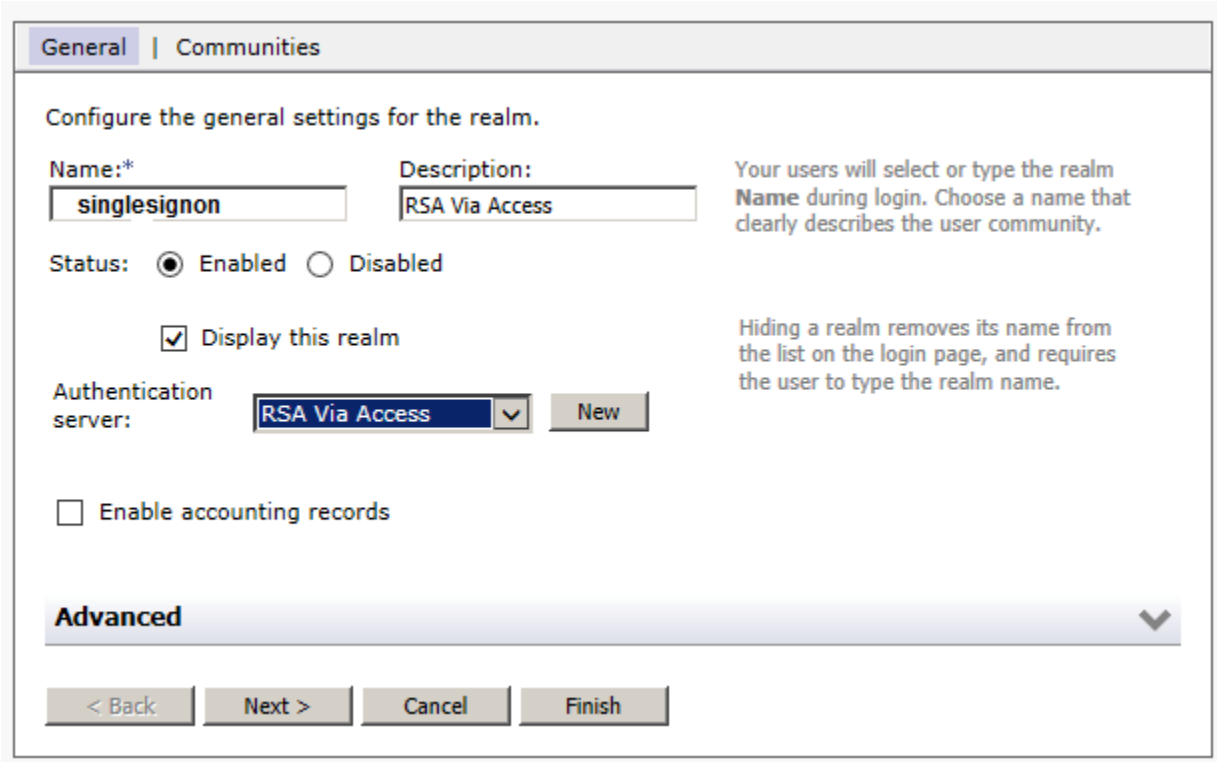



17. Click **Save**.

18. Select the **User Access > Realms**.
19. Click the **click here** link to add your first realm or the **+New realm** button to add an additional realm.

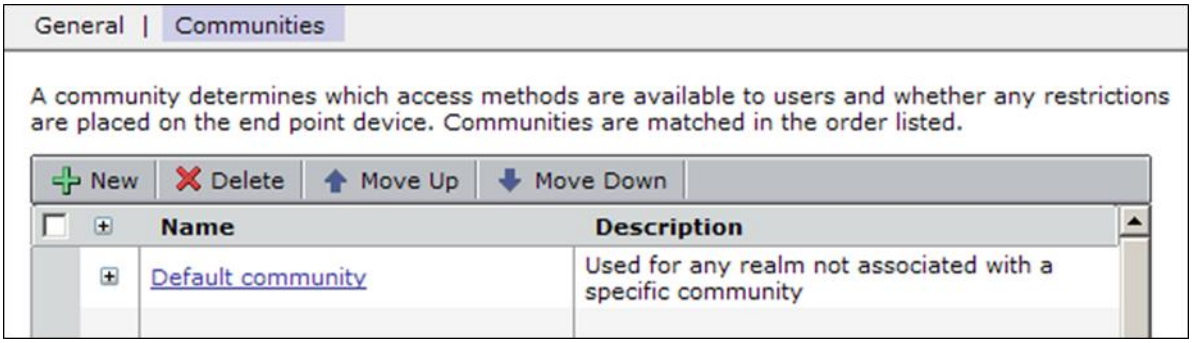



20. Enter a name and (optionally) a description for the new realm.
21. From the Authentication server pull down list, select the SAML authentication server you created on page 7 step 8.

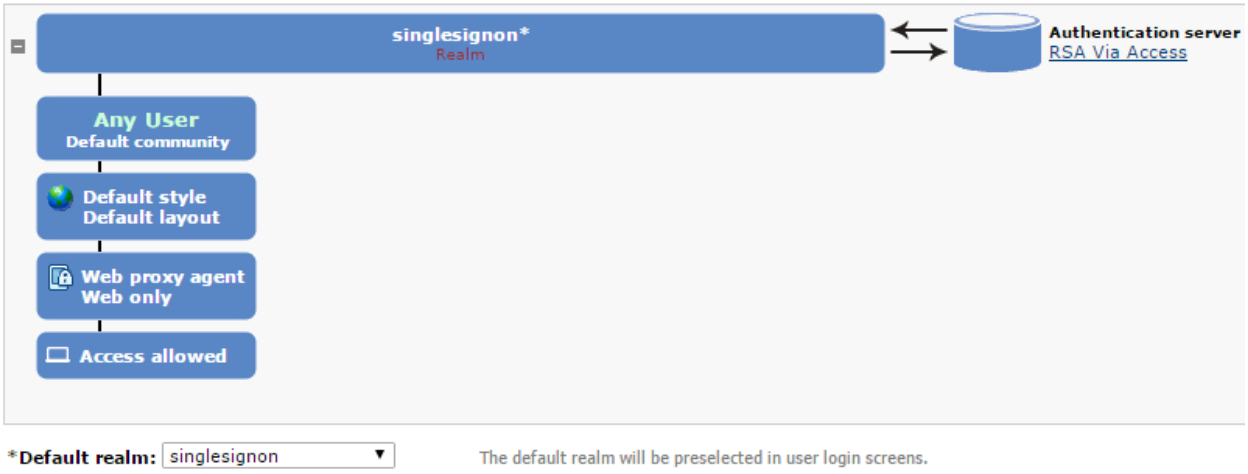



22. Select **Next**.

23. Based on your requirements, use the default community or create/configure additional communities and click the **Finish** button. The example below uses the default community.

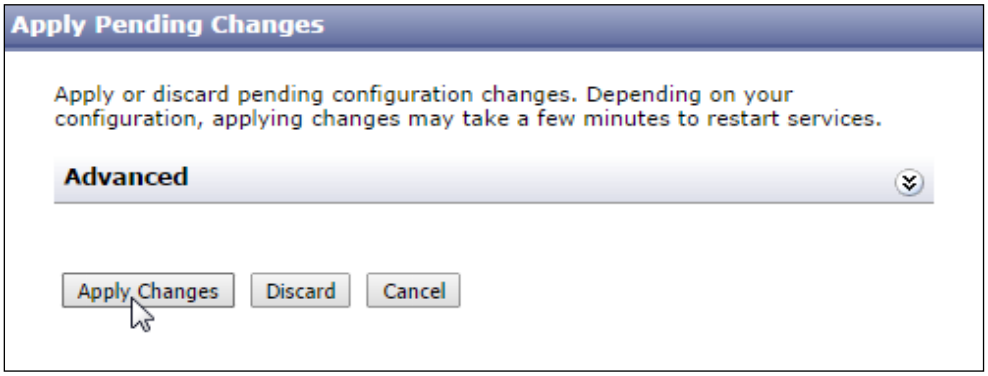



24. Use the **Default realm** pull down to select the realm presented first on the user login screen.




25. Click the **Pending changes** link. In the upper right corner of the AMC .


26. Click the **Apply Changes** button to commit the pending changes to the appliance.




GLS