

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.

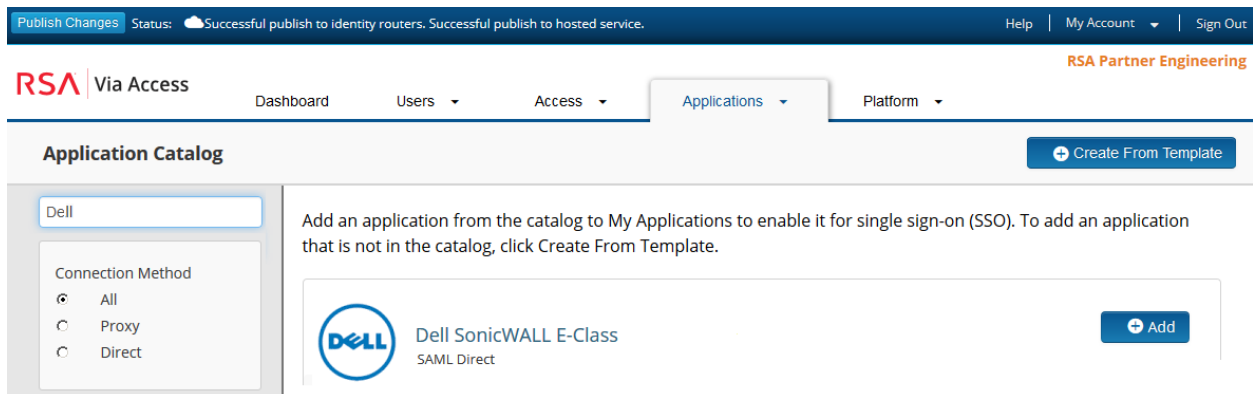
Procedure

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>


Connection URL 


IDP-initiated SP-initiated

Binding Method for SAML Request


Redirect


POST

Signed 

 No certificate loaded


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

Identity Provider URL 


Issuer Entity ID 

Default (idp_id): exseries

Override

SAML Response Signature 

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

Private Key Loaded 

Certificate Loaded

CN=gs.local, Valid Until: 12/10/2019

Include Certificate in Outgoing Assertion

- 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.

Service Provider

Assertion Consumer Service (ACS) URL ?

https://<FQDN>/saml2ssoconsumer

Audience (Service Provider Entity ID) ?

<SP_ENTITY_ID>

- 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**.

User Identity

Name ID

Identifier Type

Email Address

User Store

PE_AD

Property

mail

⌵ Show Advanced Configuration

9. Click **Next Step**.

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

All fields are required (except where noted)

User Access

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy

No Access Allowed

Cancel

Next Step →


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.

Publish Changes

Status:  Changes Pending

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**.

The screenshot displays the Dell Secure Mobile Access Management Console interface. The top left shows the Dell logo and 'Secure Mobile Access | Management Console'. The main area is titled 'vm3116 Dashboard' and includes a 'Show: Daily' dropdown and an 'Auto-refresh: Off' button. The dashboard features several monitoring charts: 'Active users: 0', 'Network bandwidth: 0.01/0.00 Mbps', 'CPU usage: 0%', 'Memory usage: 37%', 'Disk usage: 1%', and 'Swap usage: 0%'. The right sidebar, 'System Information', lists services (Network tunnel, Web proxy, WorkPlace), logs (System, Management), model (Dell Secure Mobile Access 8200v), hypervisor platform (VMware ESX Server), version (11.4.0-468), system time (Thu May 12 2016 11:01:03 EDT), and time since last reboot (1 days 12 hrs 5 mins 35 secs).

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

The screenshot shows the 'SSL Settings' page. The 'SSL certificates' section lists three certificates: 'Default appliance certificate (WorkPlace and other access methods)' with IP 10.100.53.116, 'Management console certificate (AMC)' with IP 192.168.0.10, and 'Virtual hosting certificates for WorkPlace sites and URL resources' with IPs 10.100.53.116 and 192.168.0.10. The 'CA certificates' section shows '135 certificates' and an 'OCSP' section.

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

CA Certificates SSL Settings > CA Certificates

Manage the CA certificates used by the appliance. Click the CA name to configure certificate revocation and determine the connection types it is used to secure. To establish a trust relationship with a client, reference a CA certificate in an authentication server or an EPC device profile.

Filters (reset)

Used for: Issued to: Expiration: Used:

All [v] [] All [v] All [v] Refresh

+ New X Delete => Export

Issued to	Valid through	Used
AAA Certificate Services	31 Dec 2028	

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

Security Administration

- Access Control
- Resources
- Users & Groups

User Access

- Realms
- WorkPlace
- Agent Configuration
- End Point Control

System Configuration

- General Settings
- Network Settings
- SSL Settings
- Authentication Servers
- Services
- Virtual Assist
- Maintenance

Monitoring

- User Sessions
- System Status
- Logging
- Troubleshooting

Import CA Certificate CA Certificates > Import CA Certificate

To import CA certificates, either click **Browse** to import a certificate file (in PKCS#7 or X509 format), or copy the certificate text and paste it in the area provided.

Certificate file:

[] Browse...

Certificate text:

[]

Usage

Specify the connection types the certificate is used to secure.

- Authentication server connections (LDAPS)
- Web server connections (HTTPS)
- Device profiling (End Point Control)
- OCSP response verification

Import Cancel

6. Select **Import**.

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

New Authentication Server [Authentication Servers > New Authentication Server](#)

Choose the protocol used to access your user store, and specify how users will authenticate. Click **Continue** to configure the authentication server.

User store _____

Choose the directory type or authentication method:

Authentication directory

- Dell Defender
- Microsoft Active Directory (Basic) A single domain.
- Microsoft Active Directory (Advanced) Multiple domains in a tree or forest.
- LDAP
- RADIUS
- RSA Authentication Manager The appliance supports one RSA Authentication Manager.
- Public key infrastructure (PKI)
- SAML 2.0 Identity Provider

Single sign-on server

- RSA ClearTrust Sign-on to ClearTrust is supported only from a Web browser.

Local user storage

- Local users

Credential type _____

Specify how users will authenticate:

- Digital certificate
- Token/SecurID
- Username/Password

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.

Configure Authentication Server
[Authentication Servers](#) > Configure Authentication Server

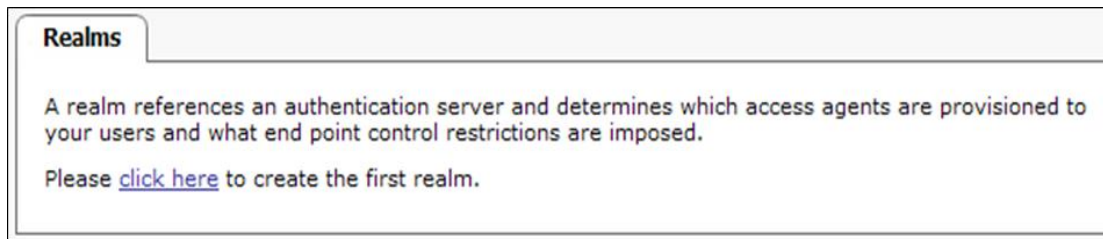
Configure settings for a SAML 2.0 Identity Provider (IdP) authentication server.

Name:*	<input type="text" value="RSA Via Access"/>	The name of the SAML IdP authentication server on the appliance
Appliance ID:*	<input type="text" value="sonicwall"/>	The SAML entity ID of the appliance.
Server ID:*	<input type="text" value="exseries"/>	The SAML entity ID of the IdP, also referred as Issuer URL on IdP.
Authentication service URL:*	<input type="text" value="https://pe108.prod0.pe-lab.com/IdPServlet?idp_id=exseries"/>	The HTTP/S URL where IdP hosts the SAML SSO service.
Logout service URL:	<input type="text" value="https://pe108.prod0.pe-lab.com"/>	The HTTP/S URL where IdP hosts the SAML logout service.
Trust the following certificate:*	<input type="text" value="gs.local"/>	CA certificates are configured here .
<input type="checkbox"/> Sign <i>AuthnRequest</i> message using this certificate:	<input type="text" value="192.168.0.10"/>	The appliance uses this certificate to sign <i>AuthnRequest</i> messages before sending them to the IdP server. SSL signing certificates are configured here .

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.

The screenshot shows the 'General' settings for a realm. The page has a header with 'General' and 'Communities' tabs. The main heading is 'Configure the general settings for the realm.' There are two input fields: 'Name:*' with the value 'singlesignon' and 'Description:' with the value 'RSA Via Access'. To the right of these fields is a note: 'Your users will select or type the realm Name during login. Choose a name that clearly describes the user community.' Below the name field, there is a 'Status:' section with radio buttons for 'Enabled' (selected) and 'Disabled'. There is also a checkbox for 'Display this realm' which is checked. The 'Authentication server:' is a dropdown menu showing 'RSA Via Access' and a 'New' button. There is an unchecked checkbox for 'Enable accounting records'. At the bottom, there is an 'Advanced' section with a downward arrow. At the very bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Finish'.

22. Select **Next**.

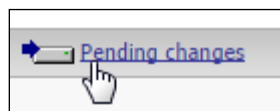
23. Based on your requirements, use the default community or create/configure additional communities and click the **Finish** button. The example below uses the default community.



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.

