

Sentry SSO with SonicWall

Contents

- [1 Setup AuthControl Sentry Keys](#)
- [2 Setup SSO on SonicWall](#)
- [3 Configure Check Password with Repository on the Swivel Core](#)
- [4 Setup AuthControl Sentry Application definition](#)
- [5 Setup AuthControl Sentry Authentication definition](#)
- [6 Testing authentication to SonicWall via Swivel AuthControl Sentry](#)
- [7 Troubleshooting](#)

Setup AuthControl Sentry Keys

Before you are able to create a Single Sign On configuration on SonicWall, you will need to setup some Keys. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel AuthControl Sentry.

Setup SSO on SonicWall

To configure SSO setting on your SonicWall account you have to create a new authentication server on your Admin console. You should see an screen similar to the one below:

- 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

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
- 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

Continue...

Cancel

You will need to select SAML 2.0 and Username/Password as Credential Type. Then click Continue.

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

Configure Authentication Server [Authentication Se](#)

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

Name:*

Appliance ID:*

Server ID:*

Authentication service URL:*

Logout service URL:

Trust the following certificate:*

Sign *AuthnRequest* message using this certificate:

Name - Type an arbitrary name

Appliance ID - `https://YOURDOMAIN`" That value will need to match with the Entity ID attribute specified on the SonicWall application configured on Sentry
 Set the Login, Logout and Change password URLs below, where `<FQDN_OF_SENTRY_SERVER>` is the public DNS entry of your Swivel AuthControl Sentry server, e.g. `swivel.mycompany.com` or if you do not have a redirect from port 443 to 8443 in place, you may need to include a port number e.g. `swivel.mycompany.com:8443`
 Authentication service URL - `https://<FQDN_OF_SENTRY_SERVER>/sentry/saml20endpoint`

Logout service URL - `https://<FQDN_OF_SENTRY_SERVER>/sentry/singlelogout`

Trust the following certificate - You will need to import the RSA PEM file created earlier on Sentry

After you have entered all the details as below click Save

Configure Check Password with Repository on the Swivel Core

In order to check the user's Active Directory password, ensure that the local Agent is configured as explained [here](#)

Setup AuthControl Sentry Application definition

Please note: you must have setup a SonicWall SSO prior to defining this Application entry within AuthControl Sentry. This is so that you are able to populate the Endpoint URL field. Login to the AuthControl Sentry Administration Console. Click Applications in the left hand menu. To add a new Application definition for SonicWall, click the Add Provider button.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application



Note: The Endpoint URL is used only if the ACS SAML (Security Assertion Markup Language) re

Name

SonicWall

Image

SonicWall.png

Points

0

Portal URL

https://sonicwall.yourdoma

Endpoint URL

https://sonicwall.yourdoma

Entity ID

https://sonicwall.yourdoma

Federated Id

email

- **Name:** SonicWall
- **Image:** SonicWall.png (selected by default)
- **Points:** 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)
- **Endpoint URL:** https://sonicwall.yourdomain/saml2ssoconsumer
- **Portal URL:** (this Portal URL is your companies google docs URL which you can usually access on: https://sonicwall.yourdomain)
- **Entity ID:** https://sonicwall.yourdomain (it needs to match with the value defined on SonicWall Appliance ID attribute)
- **Federated id:** email

Setup AuthControl Sentry Authentication definition

As an example here we will be using Turing authentication as the Primary method required for Google authentication.

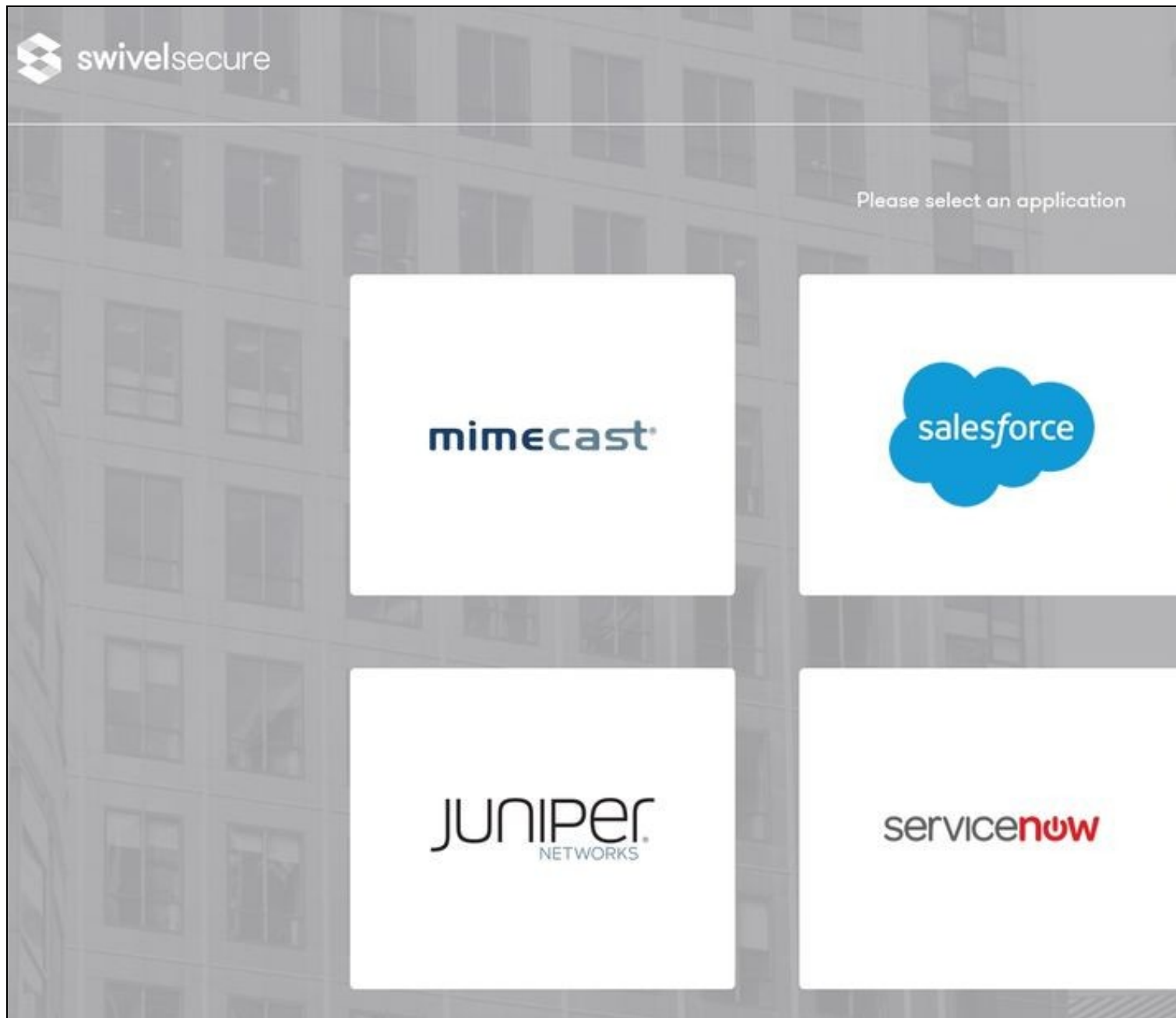
Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the SonicWall Application, this Authentication Method will be offered during login. (Please read about AuthControl Sentry Rules and familiarize your self with AuthControl Sentry [here](#))

Testing authentication to SonicWall via Swivel AuthControl Sentry

This should be the final step after all previous elements have been configured.

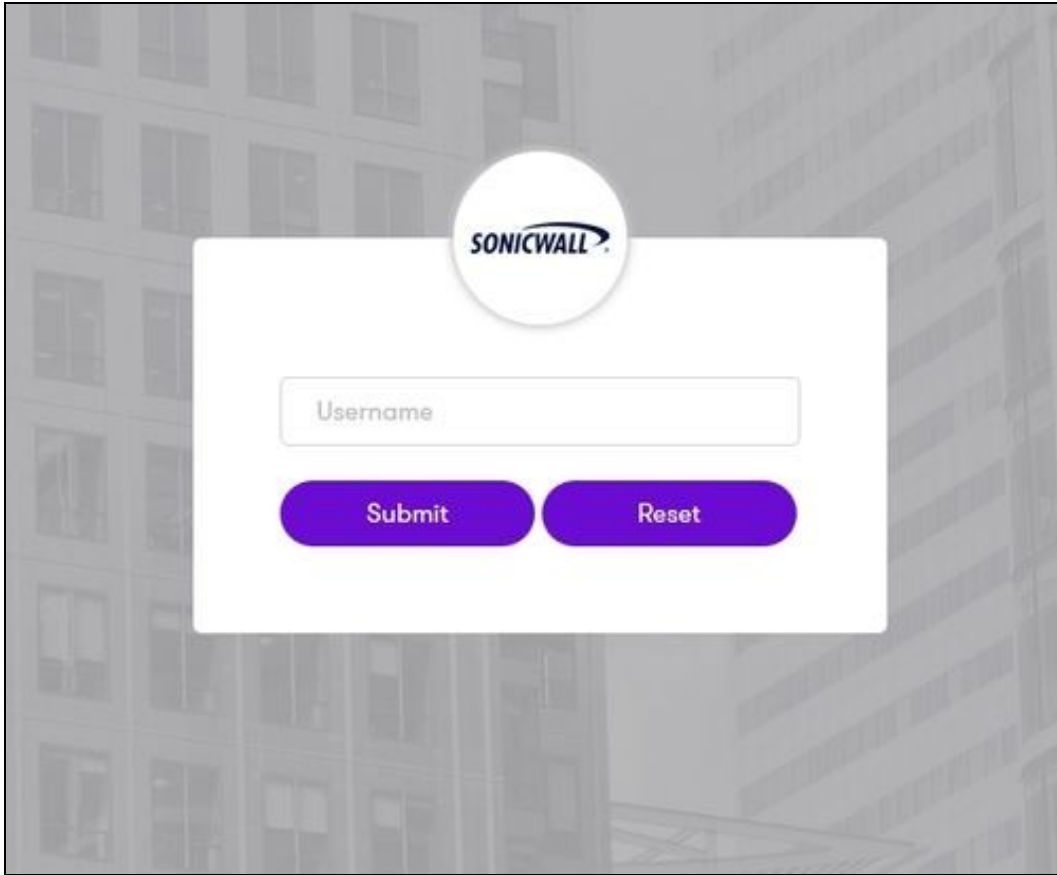
You can visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g.

https://mycompanysentrydomain/sentry/startPage On a Start Page you will be able to see a new SonicWall Icon on which you can click and proceed with authentication (as you would by going straight to the google page)

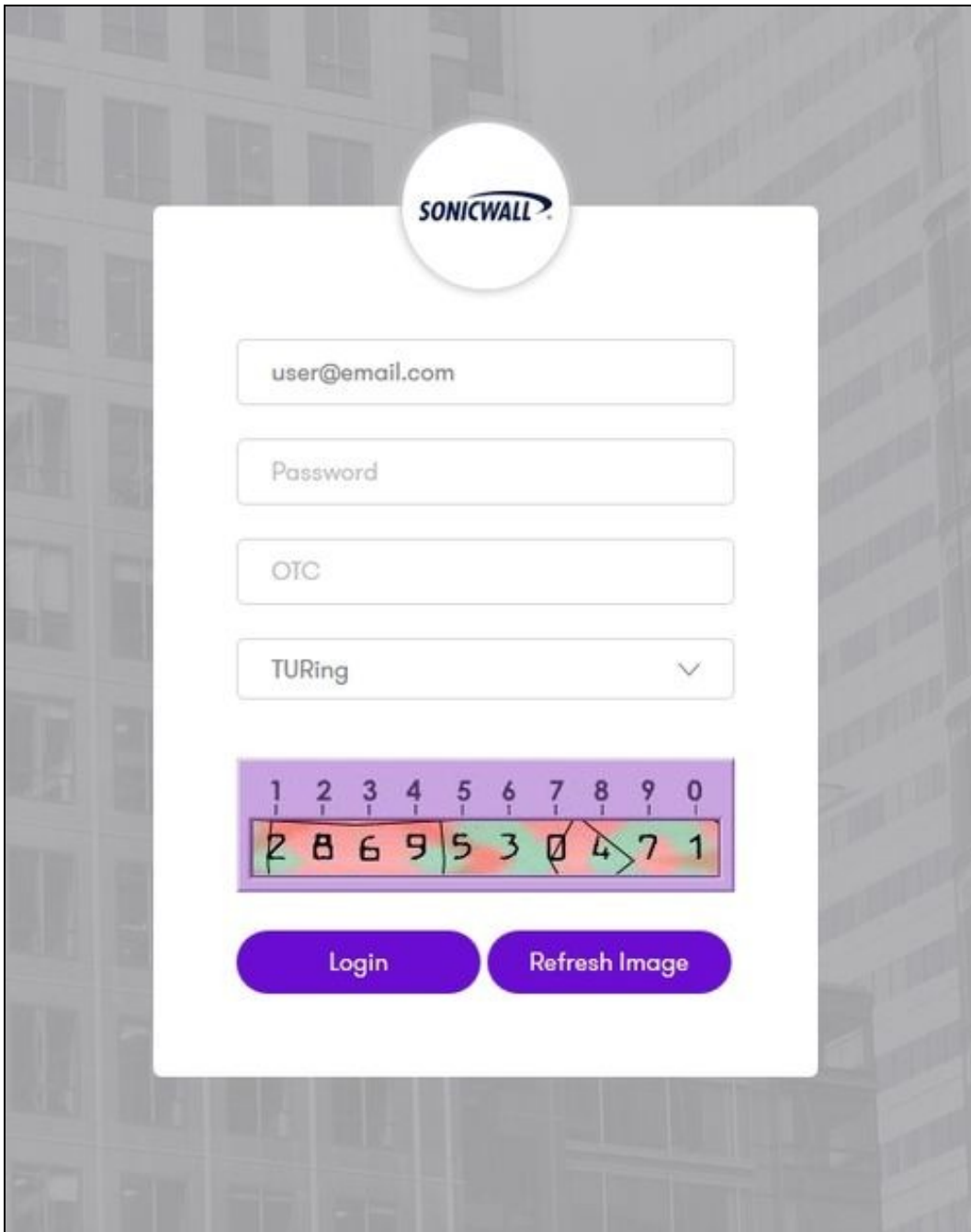


When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup, once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the SonicWall Application definition.

In this login example we are using the email as a username

A screenshot of a SonicWall login interface. At the top center is the SonicWall logo, which consists of the word "SONICWALL" in a bold, sans-serif font next to a stylized blue and white wave icon, all enclosed in a white circle. Below the logo is a white rectangular form with rounded corners. Inside the form, there is a text input field with the placeholder text "Username". Below the input field are two purple buttons with white text: "Submit" on the left and "Reset" on the right. The background of the entire image is a faded, grayscale photograph of a multi-story building with many windows.

After we enter the username we are prompted with another authentication method (in this example we use turing)



After we enter our authentication credentials we successfully will see the SonicWall that we tried to access.

Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

- The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been started for the image request;
- The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from SonicWall and can be useful for comparison with the SonicWall SAML Assertion Validator output;

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the AuthControl Sentry logging shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

- Certificate or decryption issues;
 - ◆ Can AuthControl Sentry find the Certificate locally, is it the correct one?
 - ◆ Has the correct Certificate been uploaded to SonicWall?
 - ◆ Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core since modifying this?