

Sentry SSO with Juniper

Contents

- 1 Introduction
- 2 Overview
- 3 Configure Juniper Login
- 4 Configuring Logout
- 5 Configure Juniper
- 6 Configuring Sentry Login
- 7 Configuring Sentry RADIUS
- 8 SSO
- 9 Authentication with AD/LDAP and Radius
- 10 Testing

Introduction

This article explains how to integrate a Juniper SSL VPN with Sentry.

It focusses on the setting up of Sentry and the modification of the login pages to support the Sentry integration.

It assumes knowledge of how to configure the Juniper to use Sentry as a RADIUS authentication server. Details of these elements can be found in the existing integration guides [Category:Juniper](#)

For this integration it is recommended that the Swivel Radius server is the only authentication required for this realm.

Overview

The integration works by

1. configuring the Juniper login page to redirect the user to Sentry to authenticate
2. user authenticates at Sentry
3. user is redirected back to the Juniper login page with a claim
4. Juniper login page is submitted with username and claim
5. Username and claim are validated via RADIUS
6. User gains access

Therefore the following steps are required

1. Configure Juniper Login
2. Configure Sentry to work with Juniper login page
3. Configure Sentry to accept RADIUS requests from Juniper

Configure Juniper Login

To modify the login pages download the sample.zip file from your Juniper and make the required changes to LoginPage.html. If you also wish to support mobile devices you will need to make the same changes to the other login pages, eg LoginPage-mobile-webtoolkit.html

sample.zip can be found on Upload Custom Sign-In Pages, which can be found on Signing-in -> Sign-in Pages -> Upload Custom Pages... There you will be able to see Sample Templates Files on the right side corner as shown below:

- System
 - Status
 - Configuration
 - Network
 - Clustering
 - IF-MAP Federation
 - Log/Monitoring
- Authentication
 - Signing In
 - Endpoint Security
 - Auth. Servers
- Administrators
 - Admin Realms
 - Admin Roles
- Users
 - User Realms
 - User Roles
 - Resource Profiles
 - Resource Policies
 - Junos Pulse
- Maintenance
 - System
 - Import/Export
 - Push Config
 - Archiving
 - Troubleshooting

[Signing In >](#)

Upload Custom Sign-In Pages

Custom sign-in pages allow you to provide customized templates for various pages that may appear during the sign-in process. Refer to the documentation for information about creating valid templates.

Sign-In Pages

Name:
 Label to reference the custom sign-in pages.

Page Type: Access Meeting

Templates File: No file chosen
 Zip file containing the custom templates and assets.

Upload

Skip validation checks during upload

In order to make the Juniper page work in the desired way once the page has loaded the page must detect if the user has been redirected to this page from the Sentry Auth Manager or if the user have come directly.

If the user has come directly they need to be redirected to Sentry Auth Manager. If they have been directed from Sentry Auth Manager the login form needs to be populated and submitted.

This is the required snippet that needs adding to the head (eg between the <head> and </head> tags) section of the login pages.

The only modification required is to change SENTRYURL for the actual public url of your sentry install.

Note the **applicationNameNoSAML=JuniperVPN**. This is important as this application name must match the settings on Sentry

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js" ></script>
<script>
function redirect() {
    window.location.replace("https://SENTRYURL/noSamlEndPoint?returnurlNoSAML="
    + window.location.href + "&applicationNameNoSAML=JuniperVPN" );
}
var QueryString = function () {
    // This function is anonymous, is executed immediately and
    // the return value is assigned to QueryString!
    var query_string = {};
    var query = window.location.search.substring(1);
    var vars = query.split("&");
    for (var i=0;i<vars.length;i++) {
        var pair = vars[i].split("=");
        // If first entry with this name
        if (typeof query_string[pair[0]] === "undefined") {
            query_string[pair[0]] = pair[1];
            // If second entry with this name
        } else if (typeof query_string[pair[0]] === "string") {
            var arr = [ query_string[pair[0]], pair[1] ];
            query_string[pair[0]] = arr;
            // If third or later entry with this name
        } else {
            query_string[pair[0]].push(pair[1]);
        }
    }
    return query_string;
} ();

$(document).ready(function() {
    usernamePassedIn = QueryString["username"];
    passwordPassedIn = QueryString["password"];
    claimPassedIn = QueryString["claim"];
});
```

```
if(typeof claimPassedIn == 'undefined') {
  redirect();
} else {
  $('[name=password]').val(claimPassedIn);
  $('[name=username]').val(usernamePassedIn);
  // $('[name=user#2]').val(usernamePassedIn);
  // $('[name=password#2]').val(claimPassedIn);
  document.getElementsByName("frmLogin")[0].submit();
}
});
</script>
</head>
```

Configuring Logout

So that when a user logs out of the Juniper they are also logged out of their Sentry session, the Juniper logout pages need to redirect the user to the Sentry single Logout page. This is a simpler version of the modifications made to the login page. The following code needs adding to the page in the logout.html file (and mobile device equivalents)

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js" ></script>
<script>
function redirect(){
  window.location.replace("https://SENTRYURL/singlelogout");
}
$(document).ready(function(){
  redirect();
});
```

Configure Juniper

After you have set up the login and logout pages you should upload them to Juniper (as a zip file) like on the screen here [Sentry SSO with Juniper#Configure Juniper Login](#)

After you have uploaded the pages, you should configure the Authentication Realms for the new pages that you have created, to do so you have to click on the Signing In from the left menu. You will be shown the page as below:

- System
- Status
- Configuration
- Network
- Clustering
- IF-MAP Federation
- Log/Monitoring
- Authentication
- Signing In
- Endpoint Security
- Auth. Servers
- Administrators
- Admin Realms
- Admin Roles
- Users
- User Realms
- User Roles
- Resource Profiles
- Resource Policies
- Junos Pulse
- Maintenance
- System
- Import/Export
- Push Config
- Archiving
- Troubleshooting

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 rules on this page are disabled.

Enable multiple user sessions

Select this check box and enter the maximum number of sessions per user per realm in Users > User Realms > [Realm Name] > Authentication Policy > Limits page. By default, this is 1, or

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 sign-in. The user has to follow the instructions on the warning notification page to proceed.

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

[*/admin/](#)

[Default Sign-In Page](#)

User URLs

Sign-In Page

[*/dctest/](#)

[DCTest2SA](#)

[*/clientdemo/](#)

[Swivel Sign In Page](#)

[*/pulse/](#)

[Pulse](#)

[*/raytest/](#)

[Swivel Sign In Page](#)

[*/](#)

[Swivel Juniper 7R13](#)

[*/robintest/](#)

[Robin's Custom Page](#)

[*/pinsafe/](#)

[PINsafe Demo v62R1](#)

[*/WBY/](#)

[PINSAFE-WBY](#)

[*/ADdemo/](#)

[PINsafe Demo v62R1 2 stage login](#)

[*/grahamtest/](#)

[Swivel Juniper 7R13](#)

[*/sms/](#)

[SMS](#)

[*/remoteaccess/](#)

[Swivel Juniper 7R13](#)

[*/pinpad/](#)

[pinpad](#)

[*/onetouch/](#)

[onetouch](#)

[*/onetouch2stages/](#)

[onetouch2stages](#)

[*/inditex2stageDan/](#)

[inditex2stageDan](#)

You have to click on the User URL and select the realm from the available realms box by clicking on it and clicking Add-> button. Refer to the screenshot below.

- System
 - Status
 - Configuration
 - Network
 - Clustering
 - IF-MAP Federation
 - Log/Monitoring
- Authentication
 - Signing In
 - Endpoint Security
 - Auth. Servers
- Administrators
 - Admin Realms
 - Admin Roles
- Users
 - User Realms
 - User Roles
 - Resource Profiles
 - Resource Policies
 - Junos Pulse
- Maintenance
 - System
 - Import/Export
 - Push Config
 - Archiving
 - Troubleshooting

Signing In >

*/IljaSentry/

Save Changes

User type:

Users Administrators Authorization Only Access

Sign-in URL:

*/IljaSentry/

Format: <host>/<path>/; Use

Description:

Sign-in page:

IljaSentry

To create or manage pages, see [Sign-In pages](#).

Meeting URL:

*/meeting/

Authentication realm

Specify how to select an authentication realm when signing in.

User types the realm name

The user must type the name of one of the available authentication realms.

User picks from a list of authentication realms

The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is automatic.

Available realms:

Add ->

Remove

Selected realms:

Move Up

Move Down

Configure Sign-in Notifications

Pre-Auth Sign-in Notification

Post-Auth Sign-in Notification

Save changes?

Save Changes

You have to click on your Authentication Realm which you should have set for your user URL.

- System
 - Status
 - Configuration
 - Network
 - Clustering
 - IP-MAP Federation
 - Log/Monitoring
- Authentication
 - Signing In
 - Endpoint Security
 - Auth. Servers
- Administrators
 - Admin Realms
 - Admin Roles
- Users
 - User Realms
 - User Roles
 - Resource Profiles
 - Resource Policies
 - Junos Pulse
- Maintenance
 - System
 - Import/Export
 - Push Config
 - Archiving
 - Troubleshooting

[User Authentication Realms >](#)
pinsafeIlja

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 ↑ ↓

When users meet these conditions

1. username is "*"

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.

After clicking on the Authentication Realm you should click on Role Mapping and add a new rule by clicking New Rule In the rule you have to set a rule like on the screenshot below. This rule will assign the users their role for your Juniper network.

System
Status
Configuration
Network
Clustering
(F-MAP Federation)
Log/Monitoring
Authentication
Signing In
Endpoint Security
Auth. Servers
Administrators
Admin Realms
Admin Roles
Users
User Realms
User Roles
Resource Profiles
Resource Policies
Junos Pulse
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting

User Authentication Realms > pinsafellia >

Role Mapping Rule

* Name:

† Rule: (if username...

If more than one username should match, enter one username per line. You can use * wildcards.

...then assign these roles

Available Roles:

- AccountsRemoteAccessRole
- AnonyRole
- bsmith-test
- clientdemo_role
- Custom Dan Role

Add ->

Remove

Selected Roles:

- Users

Stop processing rules when this rule matches

To manage roles, see the [Roles](#) configuration page.

Save changes?

Save Changes

Save as Copy

* indicates required field

After setting up Juniper you should be able to proceed by setting up the Sentry Auth Manager.

Configuring Sentry Login

The Juniper VPN needs to be added to Sentry as an Application.

The following entries are required.

- Name This must match the name in the redirect url, eg JuniperVPN
- Service Provider SwivelVPN. Indicates this is a VPN integration
- Points Number of points required to access the VPN, refer to Sentry User guide

- Endpoint URL This is the URL of the Juniper login page configured to work with Sentry
- Entity ID Should match Name.

Configuring Sentry RADIUS

To complete the integration the Juniper VPN must be added as a NAS on the Sentry server.

The key settings are

- Identifier Must match the Name on Sentry login, eg JuniperVPN
- Hostname Must match IP of Juniper VPN

Two stage auth, Check Password with repository should be set to NO

SSO

For RADIUS VPN applications the login page will be displayed although Sentry has been configured with SSO enabled. That attribute just applies for SAML applications.

Authentication with AD/LDAP and Radius

To be able to authenticate with both AD/LDAP and Radius when logging in you have to add few minor changes. You have to modify the script which you have added at this step [Sentry SSO with Juniper#Configure Juniper Login](#)

You have to uncomment two lines:

```
//$ (' [name=user#2] ') .val (usernamePassedIn);  
//$ (' [name=password#2] ') .val (claimPassedIn);
```

by removing double forward slashes in front of the \$ sign, so it would look like below:

```
$ (' [name=user#2] ') .val (usernamePassedIn);  
$ (' [name=password#2] ') .val (claimPassedIn);
```

And you have to change the password line above the uncommented code from.

```
$ (' [name=password] ') .val (claimPassedIn);
```

To the line below, in the password field we will pass now the password and the claim in the password#2 which we have uncommented above.

```
$ (' [name=password] ') .val (passwordPassedIn);
```

When you have updated the page, you have to re-upload it by following the same steps like previously on [Sentry SSO with Juniper#Configure Juniper Login](#)

After uploading the the index page you have to change settings on your authentication realm to do so, you have to select your authentication realm and first to add the authentication server to be your AD/LDAP. After selecting the authentication server you should select "Additional authentication server" check box and select a previously created Radius server authentication method. The Authentication Realm settings should look similar to the once on the screenshot below:

- System
 - Status
 - Configuration
 - Network
 - Clustering
 - IF-MAP Federation
 - Log/Monitoring
- Authentication
 - Signing In
 - Endpoint Security
 - Auth. Servers
- Administrators
 - Admin Realms
 - Admin Roles
- Users
 - User Realms
 - User Roles
 - Resource Profiles
 - Resource Policies
 - Junos Pulse
- Maintenance
 - System
 - Import/Export
 - Push Config
 - Archiving
 - Troubleshooting

User Authentication Realms >
pinsafelja

General Authentication Policy Role Mapping

* Name: pinsafelja
 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: SWIVEL-WBY-AD
 Directory/Attribute: Same as above
 Accounting: None

Additional authentication server

You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specified by the user on the sign-in page (the labels for these inputs

Authentication #2: pinsafelja
 Username is: specified by user on sign-in page
 predefined as: <USER>
 Password is: specified by user on sign-in page
 predefined as: <PASSWORD>

End session if authentication against this server fails

Dynamic policy evaluation

Session Migration

Other Settings

Authentication Policy: Password restrictions
 Role Mapping: 1 Rule

Save changes?

Save Changes

* Indicates required field

Testing

- Goto to Juniper login url
- User redirected to Sentry, user should be prompted for credentials
- Supply credentials

Should see Sentry logs including

```
Login successful for user: username
SSO_CLAIM_CREATED_FOR_USER, username
```

- User should be redirected to Juniper VPN
- User should gain access

Logs should include

```
JuniperVPN:Processing user username as channel CLAIM
JuniperVPN>Login successful for user: username
```