Check Point
SOFTWARE TECHNOLOGIES LTD.

ONE STEP AHEAD

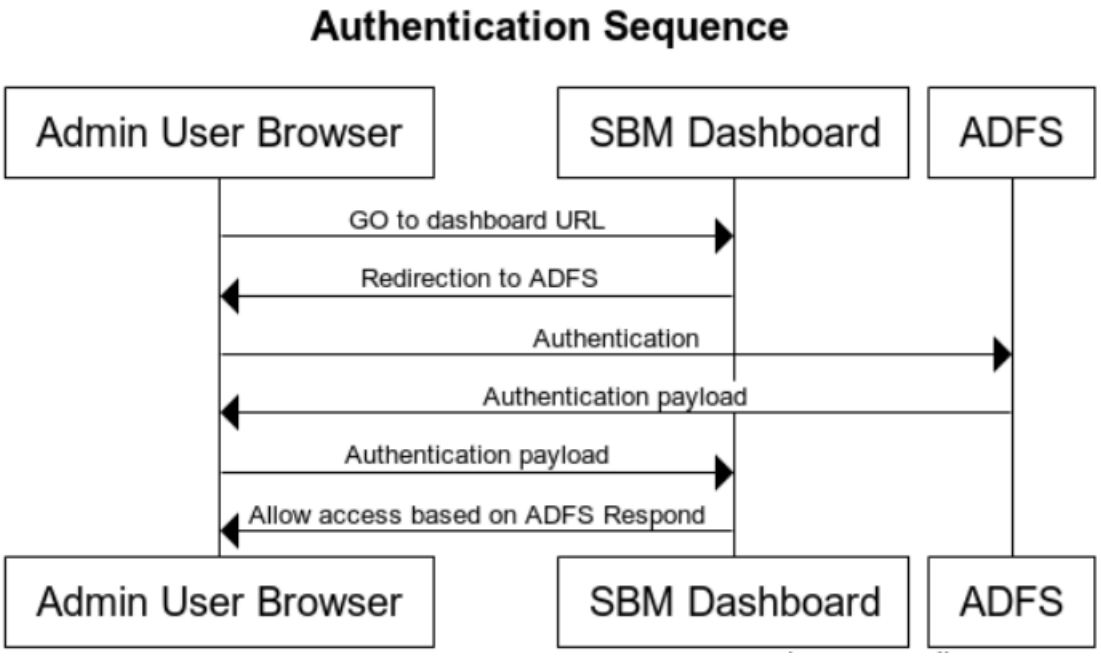
SandBlast Mobile Integration with ADFS Administration Guide

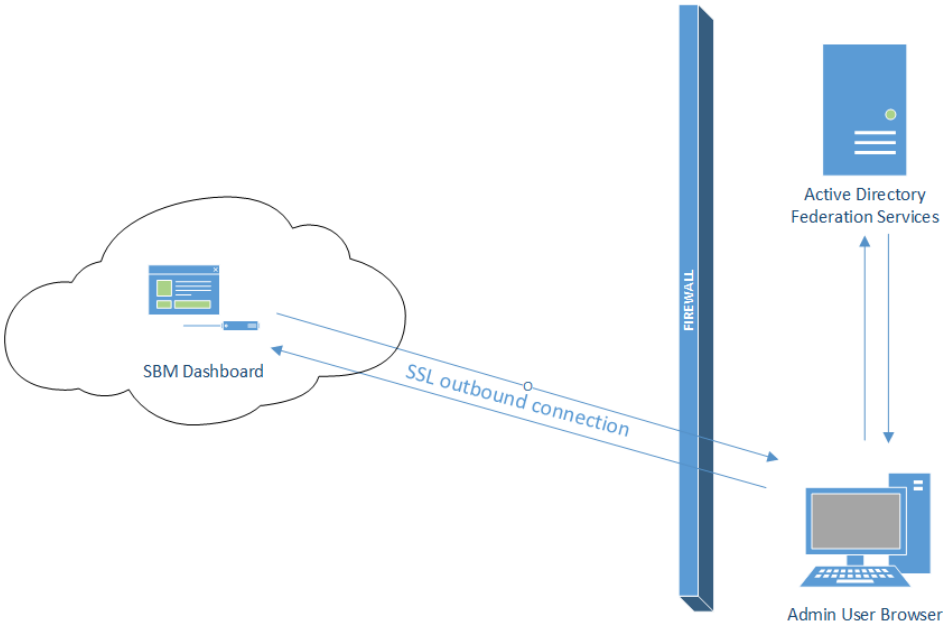
Micha Burd

28 May 2018

©2018 Check Point Software Technologies Ltd. All rights reserved
[Protected]

Solution Architecture





©2018 Check Point Software Technologies Ltd. All rights reserved
[Protected]

Overview

Active Directory Federation Services (ADFS) is a technology that extends Active Directory configuration to services outside of the AD infrastructure. With ADFS, you can give AD users access to SBM dashboard without them having to manage another set of credentials.

SBM Dashboard creates a local dashboard account for users which passes the ADFS authentication and assigns security roles based on the ADFS response.

ADFS Configuration

Before you begin, verify that the following are true:

1. ADFS service is installed.
2. You have a user with Administrative privileges on the AD.
3. You have a superuser on the SBM dashboard.

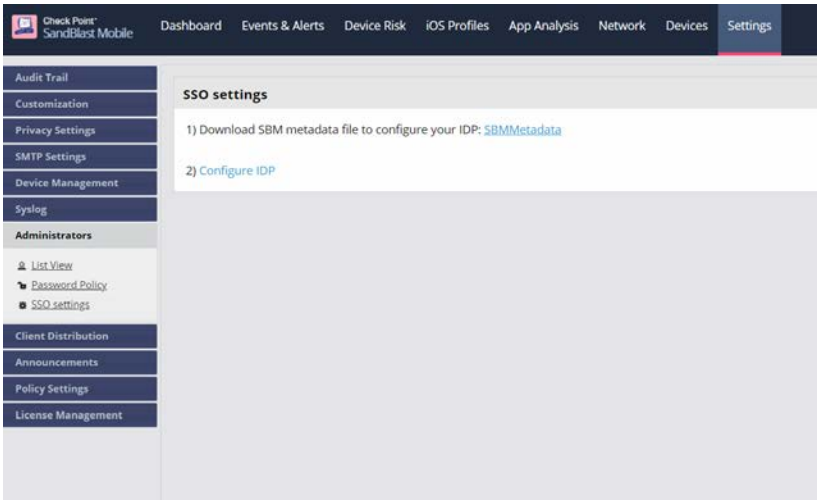
AD security groups (recommended)

1. Create a security group to each dashboard role.
    - Super User
    - Admin Configuration
    - Device Admin
    - Security Manager
    - Security Manager Viewer
2. Create a security group for all SMB users with all the above groups as group members.

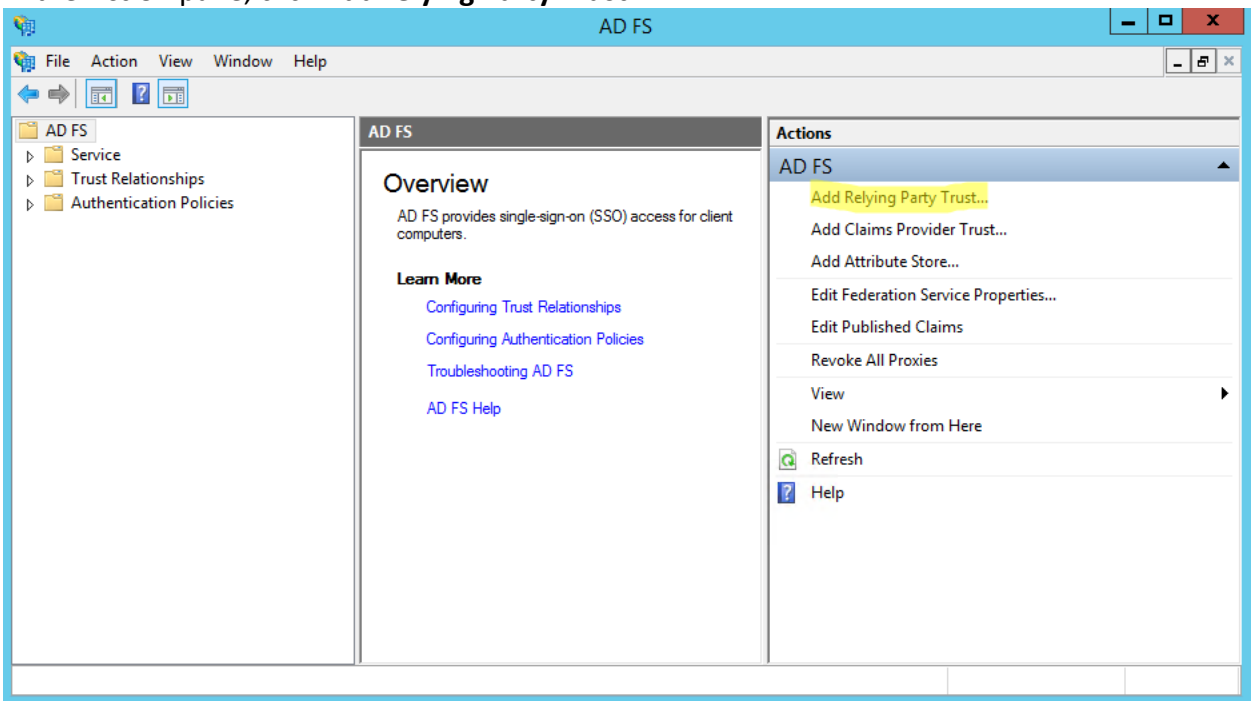
©2018 Check Point Software Technologies Ltd. All rights reserved
[Protected]

Configure the ADFS

1. Sign in to the SBM dashboard.
2. Go to the **Settings > Administrators > SSO** settings.
3. Download the SMB metadata file.
   This file will be used with ADFS management to configure a new **Relying Party Trust**.
   It will be easy to open the dashboard on the same machine you will configure the ADFS and download the XML.



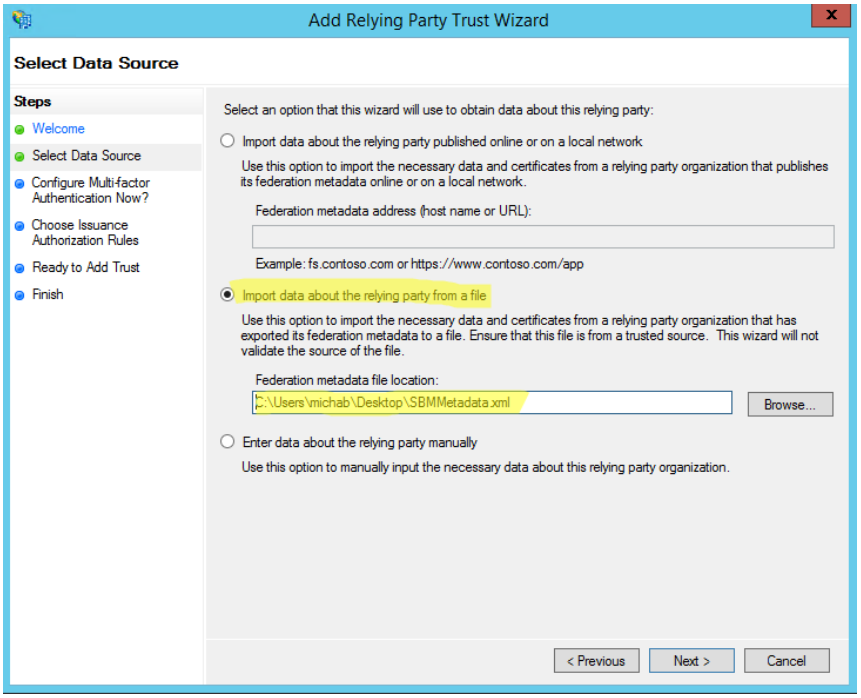
4. Open **AD FS** management.
5. In the **Action** pane, click **Add relying Party Trust…**



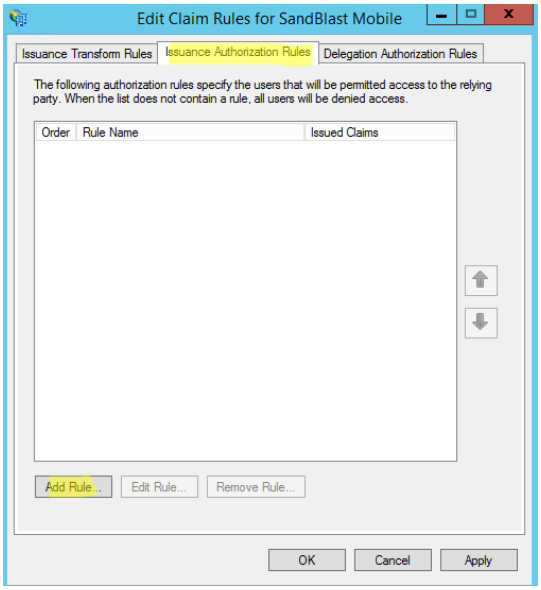
6. Click **Start**.
7. In the **Select Data Source**, select **Import data about the relying party from a file** radio button.

©2018 Check Point Software Technologies Ltd. All rights reserved
[Protected]

8. Click **Browse** and select the SMB metadata file downloaded on the previous step.
9. Click **Next**.

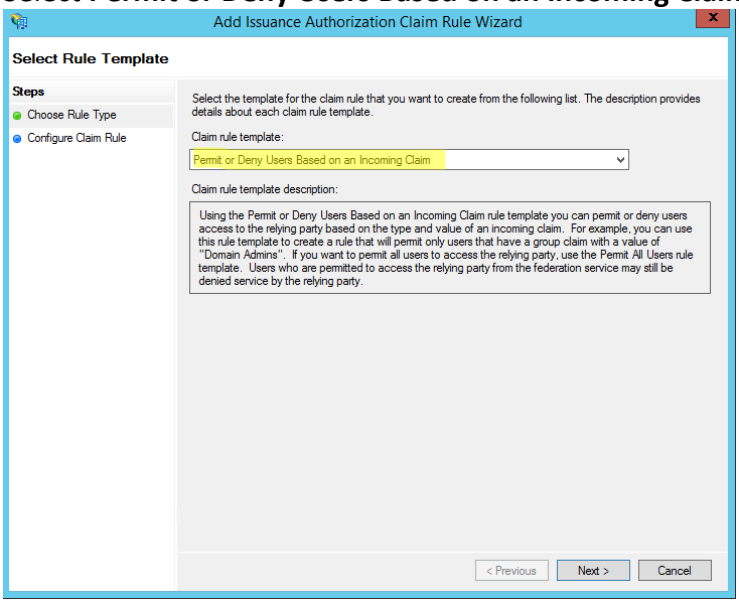


10. In the **Specify Display Name**, enter display name and description for the rely party.
11. Click **Next**.
12. Check **Open the Edit Claim rules** dialog for this relying party trust when the wizard closes.
13. Click **Close**.
14. Click **Issuance Authorization Rules**.
15. Click **Add Rule…**

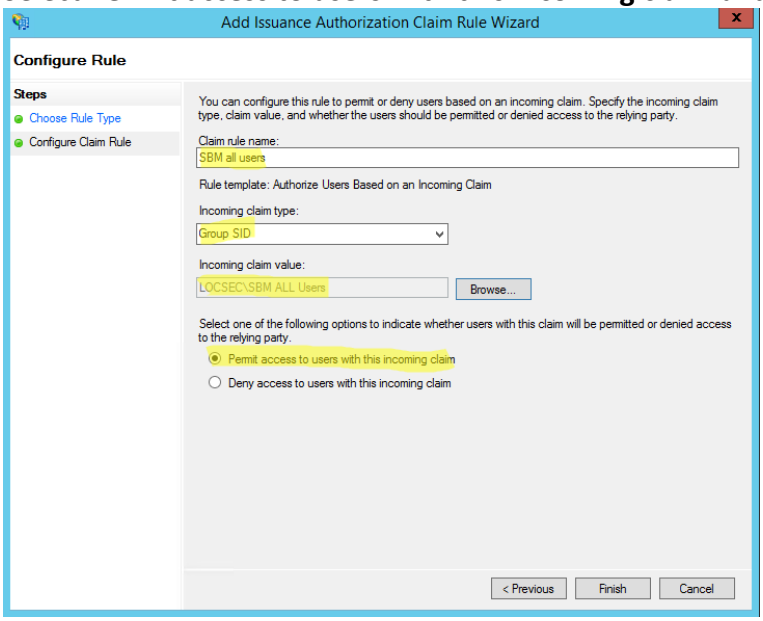


©2018 Check Point Software Technologies Ltd. All rights reserved
[Protected]

16. Select **Permit or Deny Users Based on an Incoming Claim** and click **Next**.

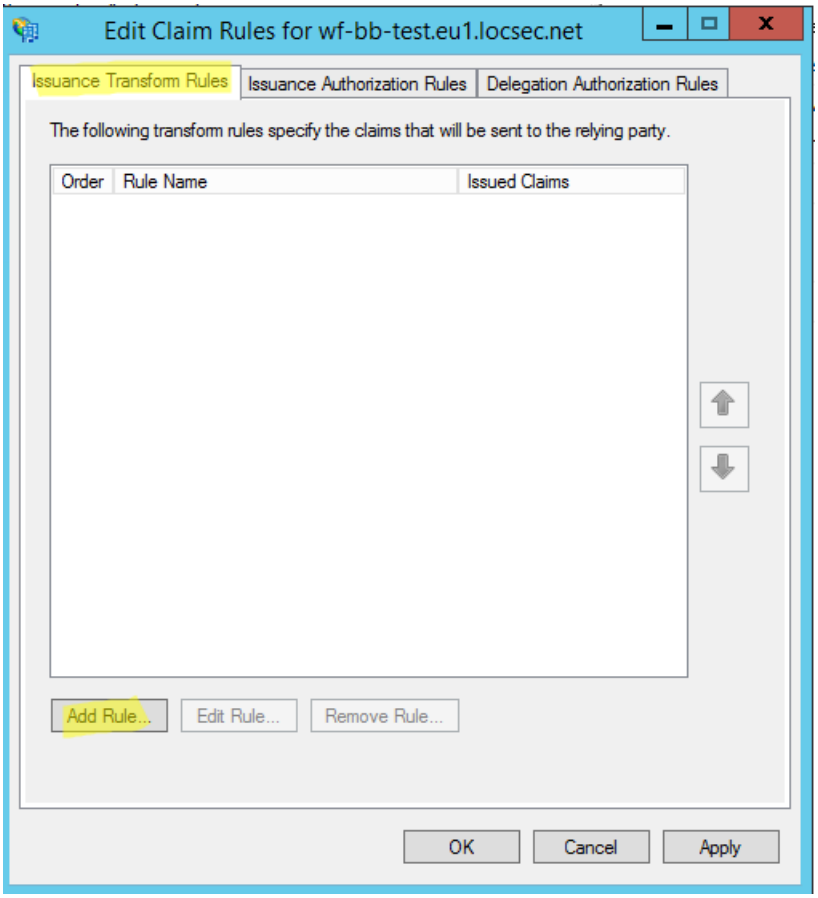


17. Enter **Claim rule name**.
18. For **Incoming claim type**, select **Group SID**.
19. For **Incoming claim value**, select the security group which include all SBM users.
20. Select **Permit access to users with this incoming claim** and click **Finish**.



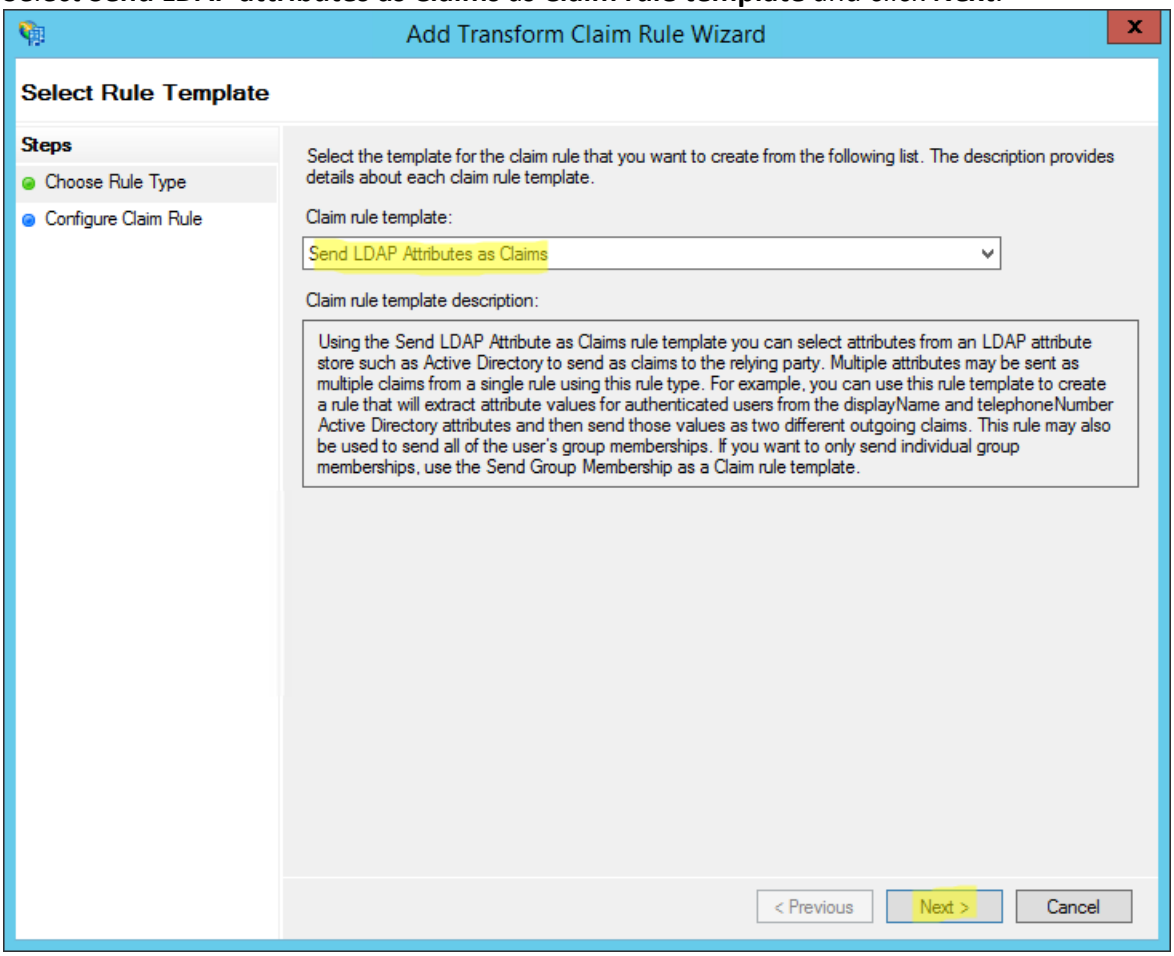
©2018 Check Point Software Technologies Ltd. All rights reserved | P. 6
[Protected]

21. Click on **Issuance Transform Rules** and **Add Rule…**



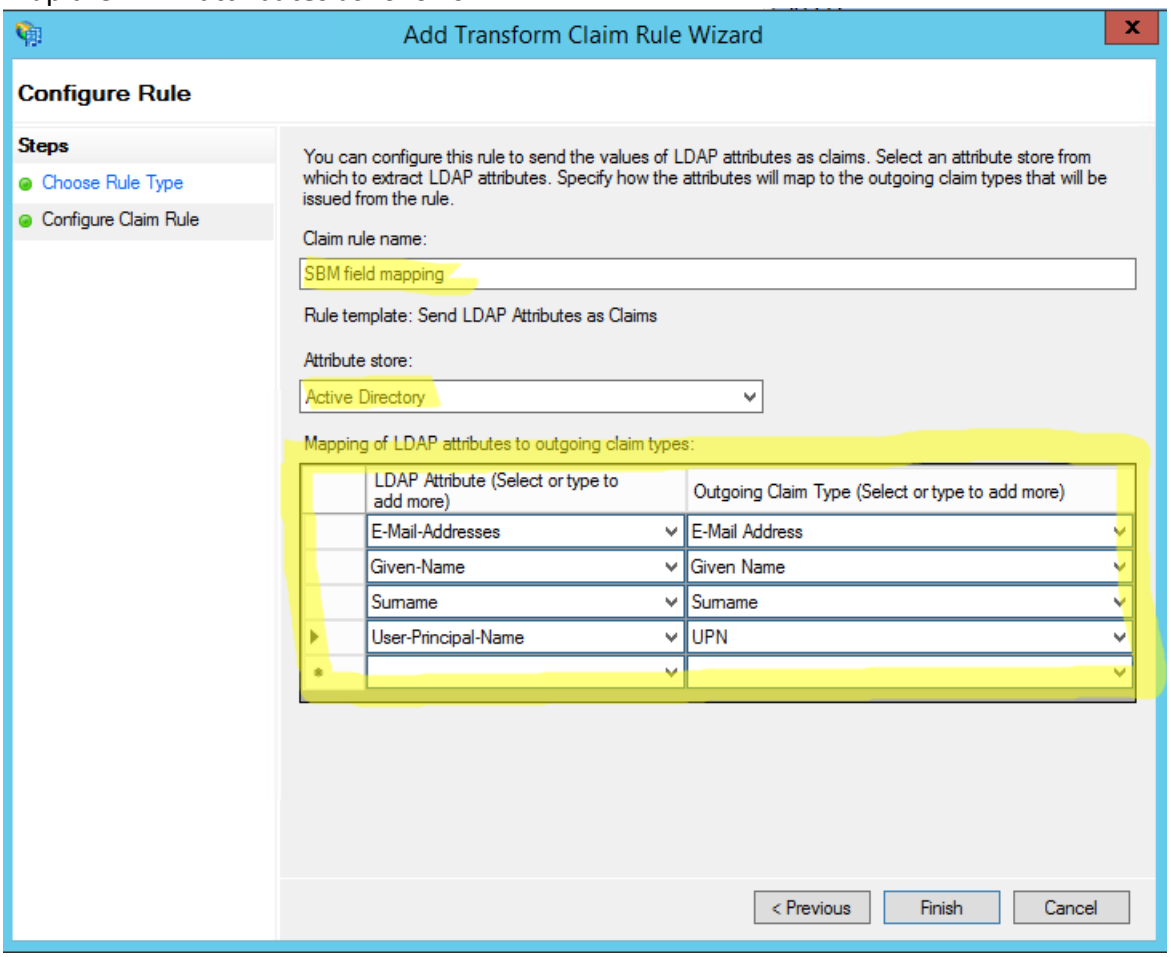
©2018 Check Point Software Technologies Ltd. All rights reserved
[Protected]

22. Select **Send LDAP attributes as Claims** as **Claim rule template** and click **Next**.



©2018 Check Point Software Technologies Ltd. All rights reserved
[Protected]

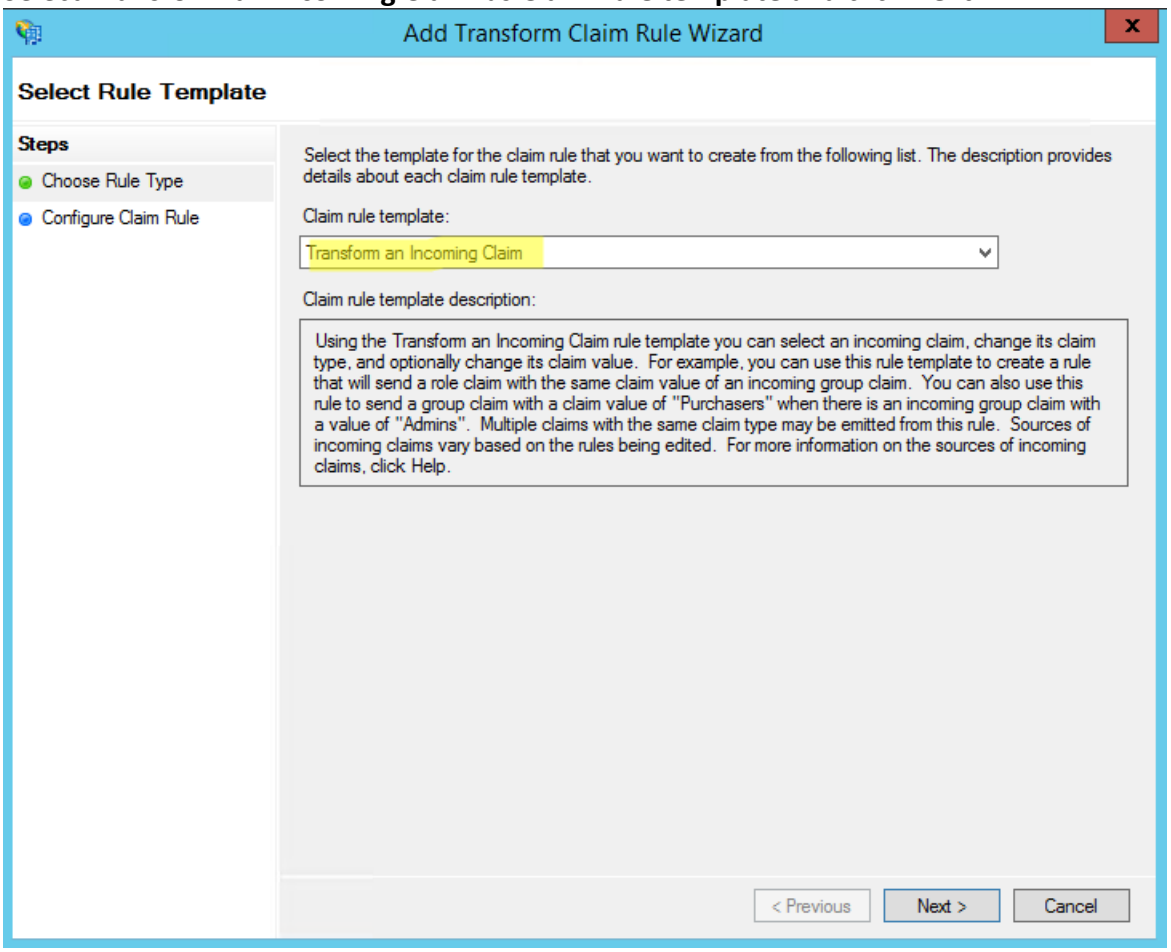
23. Enter the **Claim rule name**, select **Active Directory** as the **Attribute Store**.
24. Map the **LDAP attributes** as follows:



25. **Click Finish**.

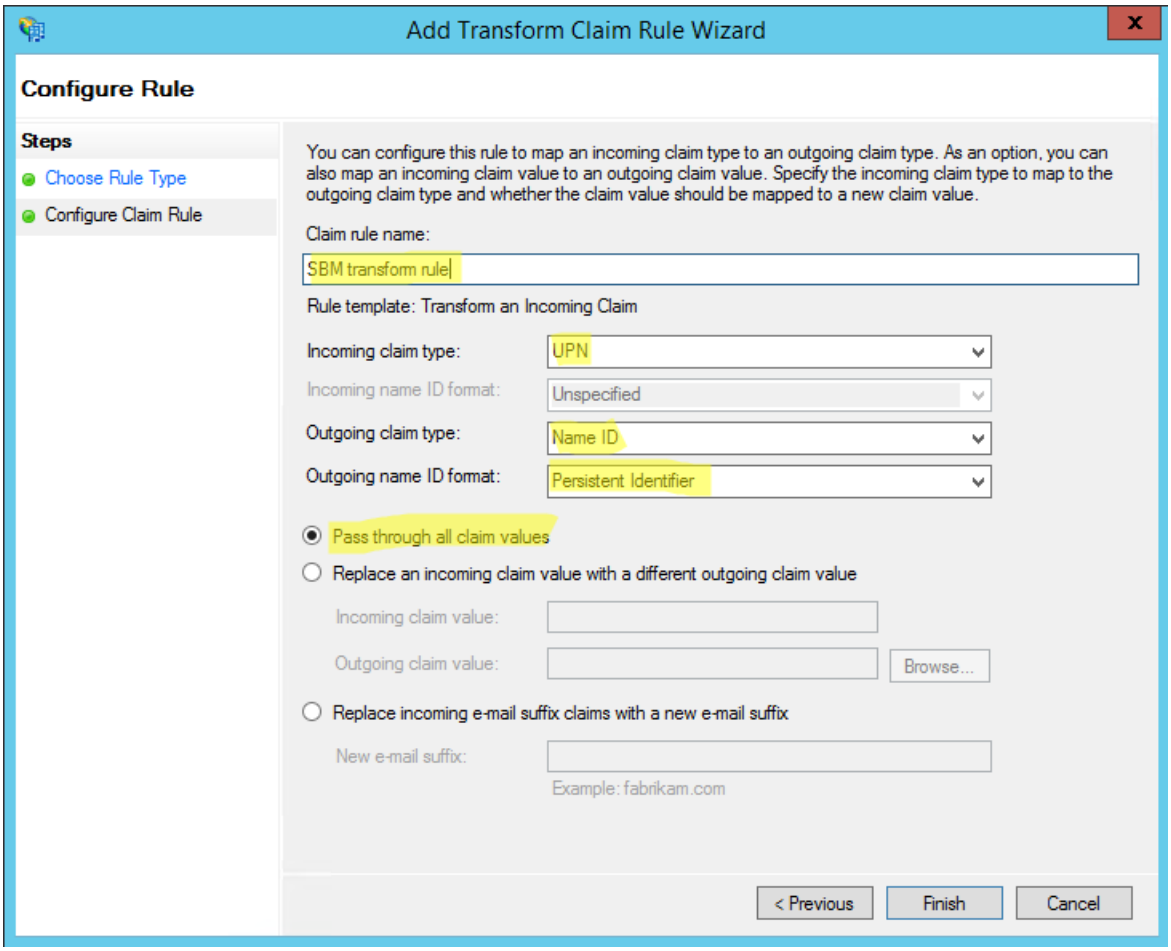
©2018 Check Point Software Technologies Ltd. All rights reserved
[Protected]

26. Click on the **Issuance Transform Rules** and click **Add Rule…**
27. Select **Transform an Incoming Claim** as **Claim rule template** and click **Next**.



©2018 Check Point Software Technologies Ltd. All rights reserved
[Protected]

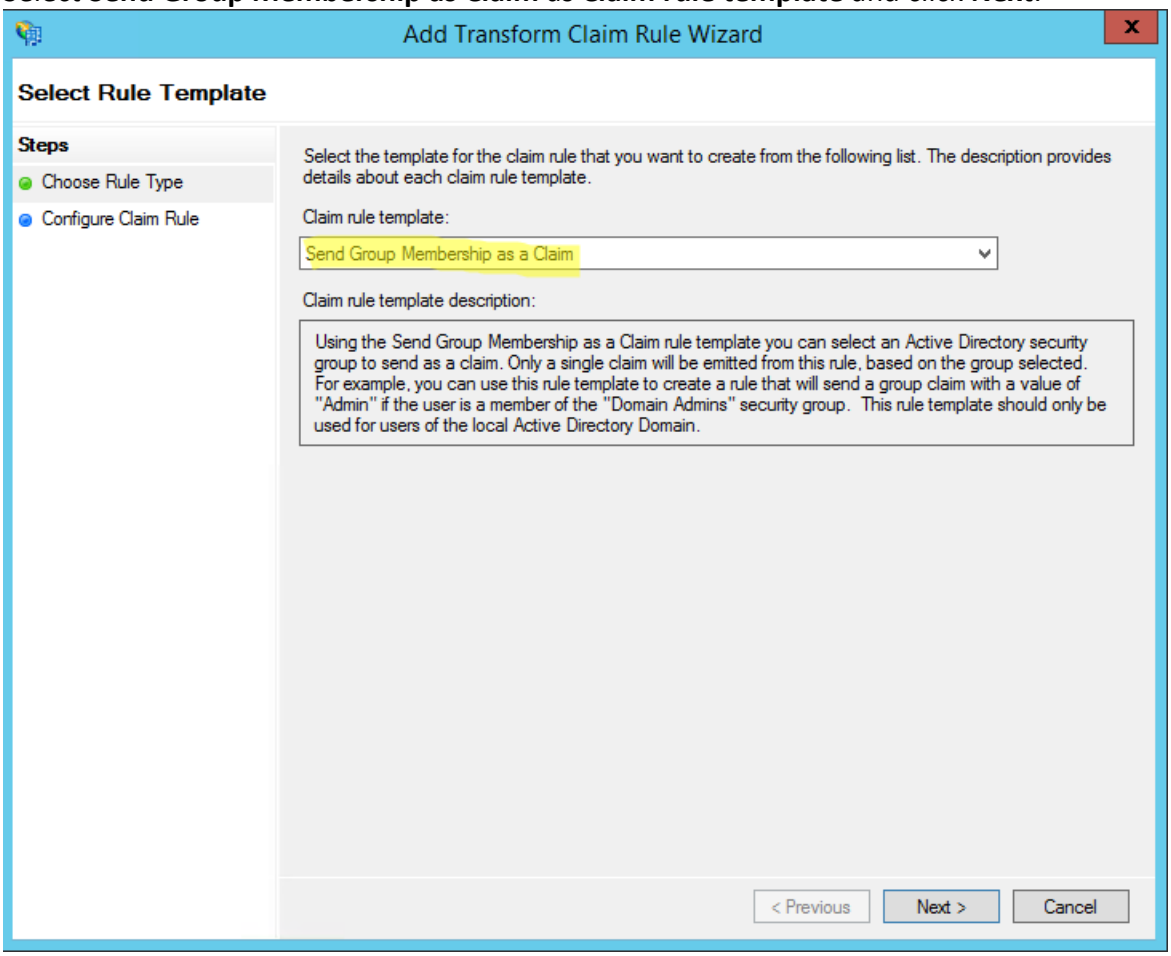
28. Enter the **Claim rule name**, select **UPN** as **Incoming claim type**, select **Name ID** as the **Outgoing name ID format**, and make sure **Pass through all claim values** is selected.
29. Click **Finish**.



30. You will need to repeat steps 18-20 for each dashboard role that will be used. Each time you repeat the step, change the **AD group** and for **Outgoing claim value** for the relevant dashboard role.
    The following values will be used as **Outgoing claim value**:
    - Superuser
    - Security Manager
    - Basic Security Manager
    - Security Manager Viewer
    - Support
    - Basic Support
    - Administrator
    - Device Administrator
31. Click on the **Issuance Transform Rules** and **Add Rule…**

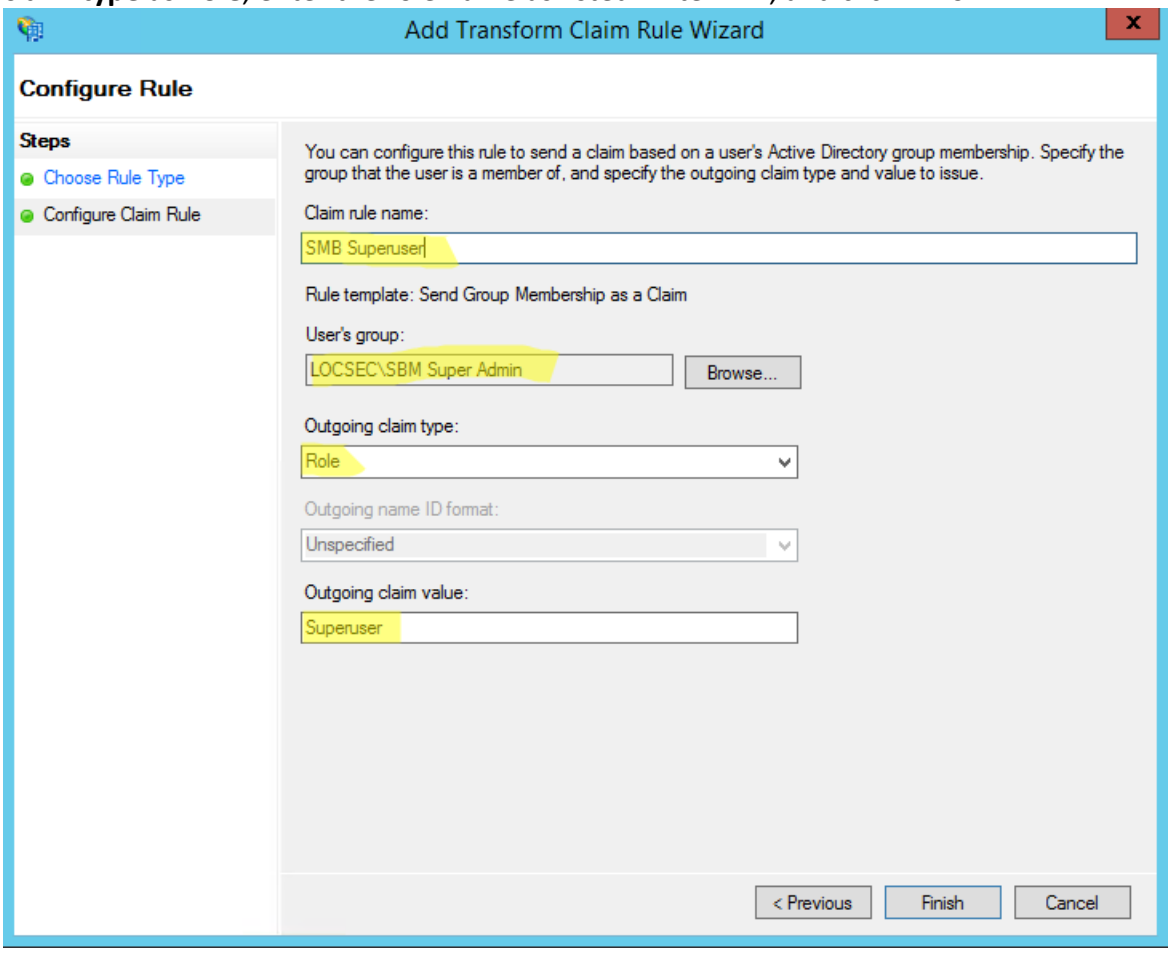
©2018 Check Point Software Technologies Ltd. All rights reserved
[Protected]

32. Select **Send Group Membership as Claim** as **Claim rule template** and click **Next**.



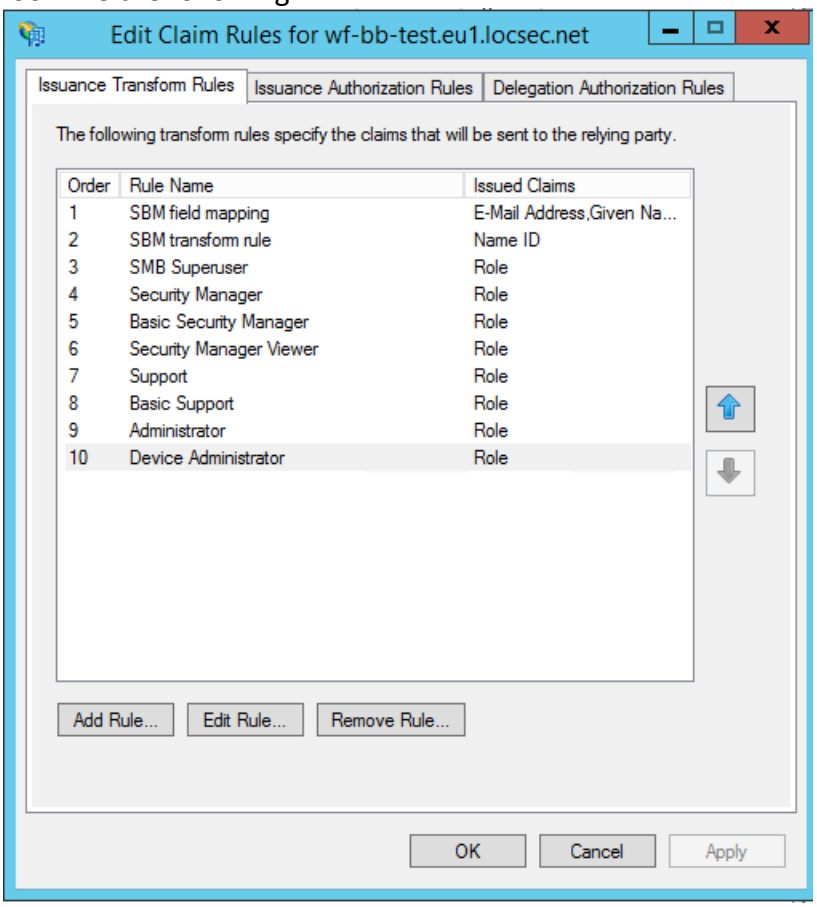
©2018 Check Point Software Technologies Ltd. All rights reserved
[Protected]

33. Enter **Claim rule name**, select the relevant AD group per dashboard role, select **Outgoing claim type** as **Role**, enter the role name as listed in item 17, and click **Finish**.



©2018 Check Point Software Technologies Ltd. All rights reserved
[Protected]

34. After repeating steps 18-20 for each dashboard role, the **Issuance Transform Rules** would look like the following:

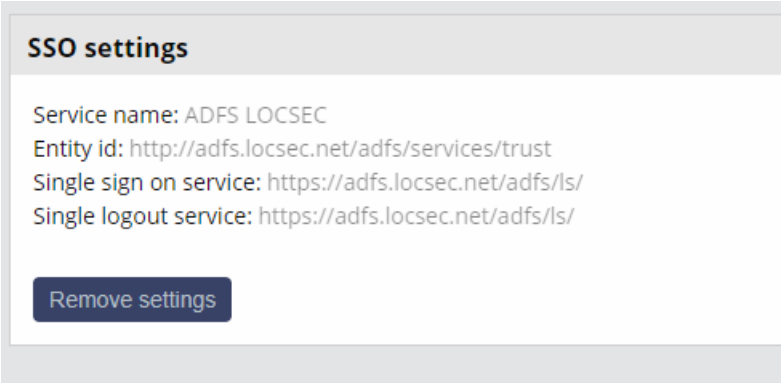


35. Download the `FederationMetadata.XML` file by going to the following link (change the *localhost* to your ADFS host machine):
https://<localhost>/FederationMetadata/2007-06/FederationMetadata.xml
36. Sign in to the SBM dashboard and go to the **Settings > Administrators > SSO** settings.
37. Click **Configure IDP**.
38. Enter **Service name**, click **Browse**, and select the `FederationMetadata.XML` file downloaded in step 22, and click **Save**.



©2018 Check Point Software Technologies Ltd. All rights reserved
[Protected]

39. The **SSO settings** screen will display the SSO settings.



40. Once **SSO setting** are activated on the dashboard, each time users open the dashboard the sign-in page will automatically redirect the users to the ADFS sign-in page.
    The users sign in using AD account details and based on the ADFS claims will be given permission with relevant roles to the dashboard.
    If the user does not have a dashboard account, it will be created automatically.
41. To log in to the dashboard using the local sign in page go to:
    https://<dashboard URL>/login/

©2018 Check Point Software Technologies Ltd. All rights reserved
[Protected]