

WALLIX Access Manager

Contents

- [Trustelem Radius on Access Manager for AD users](#)
- [Trustelem Radius on Access Manager for AM users](#)
- [Trustelem SAML on Access Manager for AD users](#)
- [Trustelem SAML on Access Manager for Trustelem users](#)
- [Debug](#)

Trustelem Radius on Access Manager for AD users

Install **Trustelem Connect**

Start by installing Trustelem Connect.

This will give Trustelem the ability to process Radius authentications.

The documentation is the following:

<https://trustelem-doc.wallix.com/books/trustelem-administration/page/ldap-radius-trustelem-connect>

You don't need to read the chapter **Setup an application to use Trustelem Connect**, the specific instructions for an Access Manager application will be detailed in this chapter.

The common mistakes will be also detailed, but if the authentication is not working you should start by reading the **Debug** chapter in this [LDAP-Radius - Trustelem Connect](#) documentation.






































On **Trustelem admin page**

- Go on the tab **Apps** and create an **Access Manager** application
- Let the **root url** / **organization identifier** / **domain** fields empty
- Enable the **Radius** protocol
- Go on the Service setup in the **Install Trustelem Connect** chapter
- Click on **Add an application +** and select the **Access Manager**
- Enable **Radius protocol** by clicking on the **Radius button**
 - the listen address can be **localhost**, all existing IP address on the machine = *, or a specific IP = ...
 - this will open the defined udp (Radius) or tcp (LDAP) port on the machine running **Trustelem Connect** on the IP 127.0.0.1 (localhost) OR on all local IPs (*) OR on a specific local IP (...)
 - if you have a dedicated VM for the connector, choose *

- If you don't already have a Bastion using it, you can let the default port 1812. Otherwise, you can use 2812, 3812...

- Click **Save**

Service setup

Name	WINAD2019-PCH																
Description	Short description (location, ...)																
Service ID	skgnmeusrsjzeumsuwbjqqg																
Connector list 	<table> <thead> <tr> <th></th> <th>NAME</th> <th>IP</th> <th>ENABLED</th> <th>STATE</th> <th>VERSION</th> </tr> </thead> <tbody> <tr> <td>^</td> <td>WIN-753G9M5AFKF</td> <td>212.85.146.100</td> <td>Yes</td> <td>Connected since 2023-10-30 13:27</td> <td>1.01  </td> </tr> </tbody> </table>						NAME	IP	ENABLED	STATE	VERSION	^	WIN-753G9M5AFKF	212.85.146.100	Yes	Connected since 2023-10-30 13:27	1.01  
	NAME	IP	ENABLED	STATE	VERSION												
^	WIN-753G9M5AFKF	212.85.146.100	Yes	Connected since 2023-10-30 13:27	1.01  												
Applications	Add an application 																
Name	Service settings																
Access Manager 	<table> <thead> <tr> <th></th> <th>LISTEN ADDRESS</th> <th>PORT</th> </tr> </thead> <tbody> <tr> <td> Radius </td> <td>* </td> <td>2812</td> </tr> </tbody> </table>						LISTEN ADDRESS	PORT	 Radius 	* 	2812						
	LISTEN ADDRESS	PORT															
 Radius 	* 	2812															
Bastion 	<table> <thead> <tr> <th></th> <th>LISTEN ADDRESS</th> <th>PORT</th> <th></th> </tr> </thead> <tbody> <tr> <td> LDAP </td> <td>* </td> <td>2001</td> <td><input type="checkbox"/> LDAPS</td> </tr> <tr> <td> Radius </td> <td>* </td> <td>1812</td> <td></td> </tr> </tbody> </table>						LISTEN ADDRESS	PORT		 LDAP 	* 	2001	<input type="checkbox"/> LDAPS	 Radius 	* 	1812	
	LISTEN ADDRESS	PORT															
 LDAP 	* 	2001	<input type="checkbox"/> LDAPS														
 Radius 	* 	1812															

On Access Manager admin page

- Add a Radius Server on Access Manager: **Configuration/RADIUS Servers**
 - **Organization:** select the organization where your AD users are
 - **Name:** choose what you want
 - **Host:** the IP/fqdn of the machine running **Trustelem Connect**
 - **Protocol:** PAP
 - **Authentication Port:** the port is defined on the **Trustelem Service** previously setup (should be 1812 or 2812)
 - **Connection Timeout:** let de default value, unless you have latency on your network
 - **Login type:** simple login
 - **Shared Secret:** this secret can be found in the Trustelem Access Manager app model.

- **NAS Identifier:** empty

Add a RADIUS Authentication Server

Organization

Trustelem

Name *

Trustelem Radius

Host *

10.10.126.201

Protocol

PAP

Authentication Port

2812

Connection Timeout (s)

3

Login type ⓘ

Simple login

Shared Secret *

.....

NAS Identifier

NAS-ID

 Test Connection

Cancel

 Save

- Click on **Test Connection** then **Save**
- Edit the Access Manager domain used for the authentication of your AD users --> **Configuration > Domains** > should be the **Active Directory** domain
- In the field **Associated Authenticators: Active Directory Authenticator** Factor 1 - **Radius Authenticator** Factor 2

You can't test the authentication yet, first you need to define the **access rules** on Trustelem.

The documentation is provided in the page: <https://trustelem-doc.wallix.com/books/trustelem-administration/page/access-rules>

For this kind of authentication, you need a **Radius access rule** set to **2nd factor only**.

Note: for the user authentication, first provide the **AD login and password** then provide the **Trustelem TOTP code**, even if the name of the input is **Password** again.

Trustelem Radius on Access Manager for AM users

Install Trustelem Connect

Start by installing Trustelem Connect.

This will give Trustelem the ability to process Radius authentications.

The documentation is the following:

<https://trustelem-doc.wallix.com/books/trustelem-administration/page/ldap-radius-trustelem-connect>

You don't need to read the chapter **Setup an application to use Trustelem Connect**, the specific instructions for an Access Manager application will be detailed in this chapter.























The common mistakes will be also detailed, but if the authentication is not working you should start by reading the **Debug** chapter in this [LDAP-Radius - Trustelem Connect](#) documentation.

On Trustelem admin page

- Go on the tab **Apps** and create an **Access Manager** application
- Let the **root url / organization identifier / domain** fields empty
- Enable the **Radius** protocol
- Go on the Service setup in the **Install Trustelem Connect** chapter
- Click on **Add an application +** and select the **Access Manager**
- Enable **Radius protocol** by clicking on the **Radius button**
 - the listen address can be **localhost**, all existing IP address on the machine = *, or a specific IP = ...
 - this will open the defined udp (Radius) or tcp (LDAP) port on the machine running **Trustelem Connect** on the IP 127.0.0.1 (localhost) OR on all local IPs (*) OR on a specific local IP (...)
 - if you have a dedicated VM for the connector, choose *
 - If you don't already have a Bastion using it, you can let the default port 1812. Otherwise, you can use 2812, 3812...

- Click **Save**

Service setup

Name	WINAD2019-PCH																
Description	Short description (location, ...)																
Service ID	skgnmeursrsizeumsuwbjqgg																
Connector list 	<table> <thead> <tr> <th></th> <th>NAME</th> <th>IP</th> <th>ENABLED</th> <th>STATE</th> <th>VERSION</th> </tr> </thead> <tbody> <tr> <td>^</td> <td>WIN-753G9M5AFKF</td> <td>212.85.146.100</td> <td>Yes</td> <td>Connected since 2023-10-30 13:27</td> <td>1.01</td> </tr> </tbody> </table>						NAME	IP	ENABLED	STATE	VERSION	^	WIN-753G9M5AFKF	212.85.146.100	Yes	Connected since 2023-10-30 13:27	1.01
	NAME	IP	ENABLED	STATE	VERSION												
^	WIN-753G9M5AFKF	212.85.146.100	Yes	Connected since 2023-10-30 13:27	1.01												
Applications	Add an application 																
Name	Service settings																
Access Manager 	<table> <thead> <tr> <th></th> <th>LISTEN ADDRESS</th> <th>PORT</th> </tr> </thead> <tbody> <tr> <td> Radius </td> <td>* ▾</td> <td>2812</td> </tr> </tbody> </table>						LISTEN ADDRESS	PORT	 Radius 	* ▾	2812						
	LISTEN ADDRESS	PORT															
 Radius 	* ▾	2812															
Bastion 	<table> <thead> <tr> <th></th> <th>LISTEN ADDRESS</th> <th>PORT</th> </tr> </thead> <tbody> <tr> <td> LDAP </td> <td>* ▾</td> <td>2001</td> </tr> <tr> <td> Radius </td> <td>* ▾</td> <td>1812</td> </tr> </tbody> </table>						LISTEN ADDRESS	PORT	 LDAP 	* ▾	2001	 Radius 	* ▾	1812			
	LISTEN ADDRESS	PORT															
 LDAP 	* ▾	2001															
 Radius 	* ▾	1812															

On **Access Manager** admin page

- Add a Radius Server on Access Manager: **Configuration/RADIUS Servers**
 - **Organization:** select the organization where your AM users are
 - **Name:** whatever you want
 - **Host:** the IP/fqdn of the machine running **Trustelem Connect**
 - **Protocol:** PAP
 - **Authentication Port:** the port is defined on the **Trustelem Service** previously setup (should be 1812 or 2812)
 - **Connection Timeout:** let de default value, unless you have latency on your network
 - **Login type:** simple login
 - **Shared Secret:** this secret can be found in the Trustelem Access Manager app model.

- **NAS Identifier:** empty

Add a RADIUS Authentication Server

Organization

Trustelem

Name *

Trustelem Radius

Host *

10.10.126.201

Protocol

PAP

Authentication Port

2812

Connection Timeout (s)

3

Login type ⓘ

Simple login

Shared Secret *

.....

NAS Identifier

NAS-ID

 Test Connection

Cancel

 Save

- Click on **Test Connection** then **Save**
- Edit the Access Manager domain used for the authentication of your AM users --> **Configuration > Domains** > should be the **local** domain
- In the field **Associated Authenticators**:
 - if you want to keep AM user password: **Local database** Factor 1 - **Radius Authenticator** Factor 2
 - if you want to use Trustelem password: **Local database** Factor Unused - **Radius Authenticator** Factor 1

You can't test the authentication yet, first you need to define the **access rules** on Trustelem. The documentation is provided in the page: <https://trustelem-doc.wallix.com/books/trustelem-administration/page/access-rules>

For this kind of authentication, you need a:

- **Radius access rule** set to **2nd factor only** if you want to keep AM user password
--> first provide the **local login and password** then provide the **Trustelem TOTP code**, even if the name of the input is **Password** again
- **Radius access rule** set to **2 factors** if you want to use Trustelem password

Trustelem SAML on Access Manager for AD users

On Trustelem admin page

- Go on the tab **Apps** and create an **Access Manager** application
- Enter the **root URL of your Access Manager** (ex: `https://wam.com/wabam`)
- Enter your **organization identifier** (you can find it in: Access Manager → Configuration → Organizations)
 - The organization must have a Bastion configured
 - The organization must not already have the needed domain used (see next point)--> a domain is unique in an organization.
- Enter the correct **domain** value. This domain has to match the **Authentication domain name** of your **Active Directory Authentication domain**

The screenshot shows the 'General' tab of the Trustelem admin interface. The 'Authentication domain type' is set to 'Active Directory'. The 'Server domain name' is 'Windows'. The 'Authentication domain name' is 'trustelem.demo', which is highlighted with a red rectangle. There is a 'Default domain' checkbox which is unchecked.

General	Mappings
General	
Authentication domain type Active Directory	
Server domain name * Windows	
Authentication domain name * trustelem.demo	
<input type="checkbox"/> Default domain	

The screenshot shows the 'Settings for WALLIX Access Manager 3' window. The 'Name' is 'WALLIX Access Manager 3'. The 'Icon' is the WALLIX Access Manager logo. The 'State' is 'Enabled'. The 'WALLIX Access Manager root URL' is 'https://10.10.126.203/wabam'. The 'WALLIX Access Manager organization Identifier' is 'tlmm'. The 'WALLIX Access Manager domain' is 'trustelem.demo'.

Settings for WALLIX Access Manager 3 [DEBUG]	
Name	WALLIX Access Manager 3
Icon	
State	Enabled
WALLIX Access Manager root URL	https://10.10.126.203/wabam
WALLIX Access Manager organization Identifier	tlmm
WALLIX Access Manager domain	trustelem.demo
LDAP	

- If on Access Manager you need different profiles for Users, click on the + at the end of the line **Custom scripting**
- The point is to send the **name of an Access Manager profile** in a **SAML attribute named profile** :

```
//Define a default profile attribute which matches the name of the Access Manager profile
msg.setAttr("profile","User")
//Change the default profile depending on the email address
if(user.email=="rose.keler@trustelem.demo"){msg.setAttr("profile","Auditor")}
//Change the default profile depending on Trustelem groups
for (let group in groups) {
  if(group=="Trustelem admin group name"){msg.setAttr("profile","Administrator")}
}
```

WALLIX Access Manager root URL

https://10.10.126.203/wabam

WALLIX Access Manager organization Identifier

tlm

WALLIX Access Manager domain

trustelem.demo

Custom scripting

Script that allows to customize the SAML response message

Script

API

```
function customSAMLresponse(msg: SAMLresponse, user: User, groups: Groups, deny: Deny): SAMLresponse {
  //Using email for the uid
  msg.setAttr("uid",user.email);
  //Define a standard profil attribute
  msg.setAttr("profile","User")
  //Change it depending on the email address
  if(user.email=="rose.keler@trustelem.demo"){msg.setAttr("profile","Auditor")}
  //Change it depending on the groups
  for (let group in groups) {
    if(group=="Trustelem group name"){msg.setAttr("profile","Auditor")}
  }
}
```

- **Save** the modifications
- Download the **metadata file**

On Access Manager admin page

- Click on: **Configuration** → **SAML Identity Providers** → **+Add**
- Select your organization (the one with the identifier used on Trustelem setup)
- Choose a name, for the identity provider setup
- In the tab **Service Provider**:

- In the field **WALLIX-AM Entity ID**, enter the value **WALLIX-AM**
- Turn OFF **Sign Messages, Encrypt Messages**
- Turn ON **Signed Response, Signed Assertion**
- In the tab **Identity Provider**:
 - Import the Trustelem metadata file
 - Copy the **Redirect Binding Uri** and paste it in **Redirect Logout Uri**, replacing « sso » by « on_logout »
- In the tab **Domain**:
 - In the field **Domain Name**, enter the domain for federated users : still the same value used on the Bastion and on Trustelem setup
 - Choose a **Default Profile** for new users.
 - Usually it is **User**
 - You can let **No Default Profile** if Trustelem is in charge of the profile.
 - Click on the pen on the line **Attributes**, and enter the following attributes:
 - Login** → uid
 - Display Name Attribute** → displayname
 - Email Attribute** → email
 - Language Attribute** → lang **Profile Attribute** → let this field empty, or enter **profile** depending on if Trustelem provides this attribute or not

You can't test the authentication yet, first you need to define the **access rules** on Trustelem.

The documentation is provided in the page: <https://trustelem-doc.wallix.com/books/trustelem-administration/page/access-rules>

For this kind of authentication, you need **internal and external** set to **2 factors**

Trustelem SAML on Access Manager for Trustelem users


On Trustelem admin page

- Go on the tab **Apps** and create an **Access Manager** application
- Enter the **root URL of your Access Manager** (ex: `https://wam.com/wabam`)
- Enter your **organization identifier** (you can find it in: Access Manager → Configuration → Organizations)
 - The organization must have a Bastion configured
 - The organization must not already have the needed domain used (see next point)--> a domain is unique in an organization.
- Enter the correct **domain** value. This domain has to match the **Authentication domain name** of your **Trustelem Active Directory Authentication domain**

The screenshot shows the 'General' tab of the 'Access Manager' application configuration. The 'Authentication domain type' is 'Active Directory'. The 'Server domain name' is 'Windows'. The 'Authentication domain name' is 'trustelem.demo', which is highlighted with a red box. There is a red asterisk next to the 'Authentication domain name' label, indicating it is a required field.

Settings for **WALLIX Access Manager 3**
[DEBUG]
×

Name
WALLIX Access Manager 3

Icon


State
Enabled


WALLIX Access Manager root URL
https://10.10.126.203/wabam

WALLIX Access Manager organization Identifier
tlmm

WALLIX Access Manager domain
trustelem.demo

LDAP
Disabled

Radius
Disabled

Certificate
Cert. 2 (2048 bits, expires on 2026-04-18)



Download metadata file


Display setup instructions
Close

- If on Access Manager you need different profiles for Users, click on the + at the end of the line **Custom scripting**
- The point is to send the **name of an Access Manager profile** in a **SAML attribute named profile** :

```
//Define a default profile attribute which matches the name of the Access Manager profile
msg.setAttr("profile","User")
//Change the default profile depending on the email address
if(user.email=="rose.keler@trustelem.demo"){msg.setAttr("profile","Auditor")}
//Change the default profile depending on Trustelem groups
for (let group in groups) {
  if(group=="Trustelem admin group name"){msg.setAttr("profile","Administrator")}
}
```

WALLIX Access Manager root URL	https://10.10.126.203/wabam
WALLIX Access Manager organization Identifier	tlm
WALLIX Access Manager domain	trustelem.demo

Custom scripting Script that allows to customize the SAML response message 

Script API 

```
function CUSTOMSAMLResponse(msg: SAMLResponse, user: User, groups: Groups, deny: Deny): SAMLResponse {
    //Using email for the uid
    msg.setAttr("uid",user.email);
    //Define a standard profil attribute
    msg.setAttr("profile","User")
    //Change it depending on the email address
    if(user.email=="rose.keler@trustelem.demo"){msg.setAttr("profile","Auditor")}
    //Change it depending on the groups
    for (let group in groups) {
        if(group=="Trustelem group name"){msg.setAttr("profile","Auditor")}
    }
}
```

- **Save** the modifications
- Download the **metadata file**

On Access Manager admin page

- Click on: **Configuration → SAML Identity Providers → +Add**
- Select your organization (the one with the identifier used on Trustelem setup)
- Choose a name, for the identity provider setup
- In the tab **Service Provider**:
 - In the field **WALLIX-AM Entity ID**, enter the value **WALLIX-AM**
 - Turn OFF **Sign Messages, Encrypt Messages**
 - Turn ON **Signed Response, Signed Assertion**
- In the tab **Identity Provider**:
 - Import the Trustelem metadata file
 - Copy the **Redirect Binding Uri** and paste it in **Redirect Logout Uri**, replacing « sso » by « on_logout »
- In the tab **Domain**:
 - In the field **Domain Name**, enter the domain for federated users : still the same value used on the Bastion and on Trustelem setup
 - Choose a **Default Profile** for new users.
 - Usually it is **User**
 - You can let **No Default Profile** if Trustelem is in charge of the profile.
 - Click on the pen on the line **Attributes**, and enter the following attributes:
 - Login** → email
 - Display Name Attribute** → displayname
 - Email Attribute** → email

Language Attribute → lang **Profile Attribute** → let this field empty, or enter **profile** depending on if Trustelem provides this attribute or not

You can't test the authentication yet, first you need to define the **access rules** on Trustelem. The documentation is provided in the page: <https://trustelem-doc.wallix.com/books/trustelem-administration/page/access-rules>

For this kind of authentication, you need **internal and external** set to **2 factors**

Debug

If the Radius authentication is not working:

- Read the [debug chapter of LDAP-Radius Trustelem Connect](#)
- Verify if the protocol is set to **PAP**
- Reminder: if the password is not handle by Trustelem, the authentication is login + password (AD, local...) then Trustelem TOTP even if the input name is **Password** again.

If the SAML authentication is not working:

- Verify if the setup is correct: there is a lot of information to copy and paste, and an error can quickly happen.
- Verify the time on Access Manager: SAML assertion are valid for a short period.
- Verify if the user doesn't already exist. For instance if the SAML domain was used before for LDAP authentication, the users may already exist. In these case the authentication will not work and it has to be deleted first.
- Verify the attributes mapped in Access Manager
--> reminder: a local Trustelem user must have an uid set to email
- Verify if the domain used in the SAML setup is the same used on the Bastion for the Authentication domain name

If after that you still you don't have a working SAML authentication, you can try 2 things:

- Download the browser plugin **SAML tracer**. This plugin will show you the certificate and the attributes send by Trustelem to the Access Manager.

The screenshot shows the SAML-tracer browser extension interface. At the top, there are controls: a search icon, a close button, and a list of actions: Clear, Pause, Autoscroll, Filter resources, Colorize, Export, and Import. Below this is a list of HTTP requests. The selected request is a POST to `https://10.10.126.200/wabam/tlm/auth?domain=trustelem.tma`. The bottom section shows the details of the SAML response, with tabs for HTTP, Parameters, SAML, and Summary. The SAML tab is active, showing the ID `_137170cd0c78879a1a365064bb1c13f5d0a3762362` and the Version `2.0`.

HTTP	Parameters	SAML	Summary
ID		<code>_137170cd0c78879a1a365064bb1c13f5d0a3762362</code>	
Version		<code>2.0</code>	

- Activate Access Manager logs: **Settings > Application Settings > Configuration > SAML** enabled at DEBUG level
Try to authenticate again, then download the logs on the Access Manager logs setting page.
The files can help you to understand the issue, but they are not easy to read.
-

Revision #22

Created 1 July 2022 08:37:52 by WALLIX Admin

Updated 24 November 2023 14:49:27 by WALLIX Admin