

WALLIX Bastion

Contents

- [Install Trustelem Connect](#)
- [Trustelem LDAP on Bastion](#)
- [Trustelem Radius on Bastion for AD users](#)
- [Trustelem Radius on Bastion for Bastion users](#)
- [Trustelem Radius on Bastion for Trustelem users](#)

Install Trustelem Connect

Start by installing **Trustelem Connect**.

This will give Trustelem the ability to process LDAP and 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 a Bastion application will be detailed in the next chapters.

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.

Trustelem LDAP on Bastion

On **Trustelem admin page**

- Go on the tab **Apps**, and create a **Bastion** application

- Enable the **LDAP** protocol

Settings for **Bastion 1** [DEBUG]

Name	<input type="text" value="Bastion 1"/>
Icon	
State	<input type="text" value="Enabled"/>
LDAP	<input type="text" value="Enabled"/>
Base DN	<input type="text" value="DC=trustelem-demo,DC=trustelem,DC=com"/>
LDAP service account	<input type="text" value="trustelem"/>
LDAP service password	<input type="password" value="....."/>  
Radius	<input type="text" value="Enabled"/>
Radius secret	<input type="password" value="....."/>  

[Display setup instructions](#) [Close](#)

- Go on the **Service** setup in the **Install Trustelem Connect** chapter
- Click on **Add an application +** and select the **Bastion**
- Enable **LDAP protocol** by clicking on the **LDAP 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 *
 - you can let the default port **2001**

- Click **Save** !

Applications		Add an application +		
Name	Service settings			
Bastion 	LISTEN ADDRESS	PORT	PROTOCOLS	
	  * ▾	<input type="text" value="2001"/>	<input type="checkbox"/> LDAPS	
	  * ▾	<input type="text" value="1812"/>		

On the **Bastion admin page**

- Go on **Configuration > External authentication**
- Create a new **Active Directory authentication**
- In the field **Authentication name** choose a name for your LDAP authentication like **Trustelem AD**
- In The fields **Server** and **Port**, write the IP / FQDN of the machine running **Trustelem Connect** and the port defined on the **Trustelem Service** previously setup (should be 2001)

- In the **Timeout** field let the default value, unless you have latency on your network

Network parameters

Authentication type *

Active Directory

Name *

Trustelem-AD

Server *

10.10.126.201

Port *

2001

Timeout *

3

In seconds

Encryption



None



StartTLS



SSL

CA certificate



Choose file

*.cert file in PEM format

- Let the **Bind method** to **simple**
- Enter **trustelem** in the field **User**.
trustelem is the default value, but can be changed on the Trustelem Bastion app model. Of course if you changed it for a good reason, provide the right service account name
- Provide the **password of trustelem account** in the fields **Password** and **Confirm Password**.
This password can be found in the Trustelem Bastion app model.

Authentication

Bind method

simple (password) ▾

User *

trustelem (⊗)

Password

..... (🗑)

Confirm password

..... (🗑)

Test authentication

- Write the **LDAP Base DN** provides in your Trustelem Bastion app model, in the **Base DN** field.
- Change the **Login attribute** and **User name attribute** to **mail**
 - Usually Trustelem LDAP is used to provision **local Trustelem users** on the Bastion, and they can be authenticated only with the login attribute **mail**.
If for some reason you want to authenticate **synchronized Trustelem AD users** instead, you can use **sAMAccountName** for those attributes.

User attributes

Base DN (dc=...) *

DC=trustelem-demo,DC=trustelem,DC=com (⊗)

Login attribute *

mail (⊗)

User name attribute *

mail (⊗)

- Click on **Test authentication**, you should see a message with **Authentication success**
 - If not, read the [debug chapter of LDAP-Radius Trustelem Connect](#)

- Click on **Apply**
- Go on **Configuration > Authentication domains**
- Create a new **Active Directory authentication domain**
- Choose a **Server domain name** --> no impact on the setup
- Choose an **Authentication domain name** --> used for the Bastion/AM login (sAMAccountName@domain_name, email@domain_name...)
- In the tab **Directory** select the previous **Active Directory authentication**
- Enter a **Default email domain** in the corresponding field --> should not be used for this kind of authentication where the login is usually not the sAMAccountName
- Click on **Apply**
- On the top of the screen, click on **Mappings** --> in some Bastion versions, the mapping is not a different tab and can be set with the previous settings.
- Click on **Add**
- Select a **Bastion user group** and a **profile** --> define the available access
- Provide the **Trustelem group CN**

```
CN=[ Trustelem Group Name], OU=Groups, DC=[ Trustelem Domain], DC=trustelem, DC=com
```

--> if you don't respect the case, the authentication won't work

Edit mapping

User group *

External1

User group profile *

user

A change of the user group profile will impact all mappings associated with the user group

Default group for users without group in this domain

Group *

CN=TMA-Bastion,OU=Groups,DC=trustelem-demo,DC=trustelem,DC=com

DN format

- Click on **Apply and close**

You now have a working LDAP authentication, with access to targets based on Trustelem groups. /!\ Trustelem users will not be found by the Bastion before having an access rule (1 or 2 factors)

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

For this kind of authentication, you need a **LDAP access rule** set to **1 factor** if it will be combined with a **Radius authentication** or **2 factors** if not.

Trustelem Radius on Bastion for AD users

On Trustelem admin page

- Go on the tab **Apps**, and create a **Bastion** application (if not already done in a LDAP setup)
- Enable the **Radius** protocol

Settings for **Bastion 1** [DEBUG]

Name

Icon 

State

LDAP

Base DN

LDAP service account

LDAP service password 👁️ 📄

Radius

Radius secret 👁️ 📄

📄 Display setup instructions
✕ Close

- Go on the **Service** setup in the **Install Trustelem Connect** chapter
- Click on **Add an application +** and select the **Bastion** (if not already done in a LDAP setup)
- 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 *
 - you can let the default port **1812** but if you don't know if it is already used on the machine running the connector, choose **2812** instead

- Click **Save** !

Applications		Add an application +		
Name	Service settings			
Bastion 	LISTEN ADDRESS	PORT	PROTOCOLS	
	 LDAP  * ▾	<input type="text" value="2001"/>	<input type="checkbox"/> LDAPS	
	 Radius  * ▾	<input type="text" value="1812"/>		

On the **Bastion admin page**

- Go on **Configuration > External authentication**
- Create a new **Radius authentication**
- In the field **Name** choose a name for your Radius authentication like **Trustelem Radius**
- In The fields **Server** and **Port**, write the IP / FQDN of the machine running **Trustelem Connect** and the port defined on the **Trustelem Service** previously setup (should be 1812 or 2812)
- In the **Timeout** field let the default value, unless you have latency on your network
- Provide the **Radius secret** in the fields **New secret** and **Confirm secret**.
This secret can be found in the Trustelem Bastion app model.
- Check the option **Use mobile device for 2 factor authentication(2FA)**
 - This option has be designed for MFA with push authentication. But the real effect is to skip the login + password step for the Radius authentication by automatically sending the login and an empty password.
 - Here we want to use Active Directory for the login + password step, so we don't want to ask for the Radius password = we need to activate this option.

- Click on **Apply**

Authentication type *

RADIUS

Name *

Trustelem-Radius with mobile device ⊗

Server *

10.10.126.201 ⊗

Port *

1812 ⊗

Timeout *

5 ⊗

In seconds

New secret

⊗

Confirm secret

⊗

Description

Use mobile device for Two-Factor Authentication (2FA)
Display a message informing the use of the mobile device to authenticate via a push notification

- Go on **Configuration > Authentication domains**
- Click on your existing **Active Directory authentication domain**
- In the field **Secondary authentication** select the previous **Radius external authentication**
- Click on **Apply**

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 skip the 2nd factor step for some users, you can select for them the rule **Always allow** instead

on Trustelem.

If the authentication doesn't work correctly:

- Read the [debug chapter of LDAP-Radius Trustelem Connect](#)
- You can also verify if you checked the option **Use mobile device** on the **Radius external authentication**

Trustelem Radius on Bastion for Bastion users

On [Trustelem admin page](#)

- Go on the tab **Apps**, and create a **Bastion** application (if not already done in a LDAP setup)
- Enable the **Radius** protocol

The screenshot displays the 'Settings for Bastion 1' configuration page in the Trustelem admin interface. The page has a '[DEBUG]' tab selected. The configuration is organized into several sections:

- Name:** Bastion 1
- Icon:** WALLIX BASTION logo
- State:** Enabled
- LDAP:** Enabled
- Base DN:** DC=trustelem-demo,DC=trustelem,DC=com
- LDAP service account:** trustelem
- LDAP service password:** Masked with dots, with visibility and copy icons.
- Radius:** Enabled
- Radius secret:** Masked with dots, with visibility and copy icons.

At the bottom right, there are two buttons: 'Display setup instructions' and 'Close'.

- Go on the **Service** setup in the **Install Trustelem Connect** chapter
- Click on **Add an application +** and select the **Bastion** (if not already done in a LDAP setup)

- 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 *
 - you can let the default port **1812** but if you don't know if it is already used on the machine running the connector, choose **2812** instead
- Click **Save !**

Applications Add an application +

Name	Service settings		
Bastion 	LISTEN ADDRESS	PORT	PROTOCOLS
	  * ▾	<input style="width: 100px;" type="text" value="2001"/>	<input type="checkbox"/> LDAPS
	  * ▾	<input style="width: 100px;" type="text" value="1812"/>	

On the **Bastion admin page**

- Go on **Configuration > External authentication**
- Create a new **Radius authentication**
- In the field **Name** choose a name for your Radius authentication like **Trustelem Radius**
- In The fields **Server** and **Port**, write the IP / FQDN of the machine running **Trustelem Connect** and the port defined on the **Trustelem Service** previously setup (should be 1812 or 2812)
- In the **Timeout** field let the default value, unless you have latency on your network
- Provide the **Radius secret** in the fields **New secret** and **Confirm secret**.
This secret can be found in the Trustelem Bastion app model.
- Don't check the option **Use mobile device for 2 factor authentication(2FA)**
 - This option has be designed for MFA with push authentication. But the real effect is to skip the login + password step for the Radius authentication by automatically sending the login and an empty password.
 - Here we want to verify login + password + 2nd factor with Radius, because a local Bastion user can't have the authentication local password + Radius. So this option must not be activated.

- Click on **Apply**

Authentication type *

RADIUS

Name *

Trustelem-Radius without mobile device 

Server *

10.10.126.201 

Port *

1812 

Timeout *

5 

In seconds

New secret



Confirm secret



 **Description**

Use mobile device for Two-Factor Authentication (2FA)
Display a message informing the use of the mobile device to authenticate via a push notification

- Go on **Accounts**
- Click on an existing user
- Verify if his login (**UserName**) is something known by Trustelem : should be an email if the associated Trustelem user is a local one.
- In the field **Authentication and backup servers** select only the previous **Radius external authentication**
 - As mentioned before, this user can't have a local password + Radius. If you select both, the Bastion will try the first method (local password). If it is a success, the authentication is completed, if not the Bastion will try the Radius authentication.
- Click on **Apply**

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 **2 factors**

If the authentication doesn't work correctly:

- Read the [debug chapter of LDAP-Radius Trustelem Connect](#)
- As mentioned in this page, if the login of the local user is unknown by Trustelem the authentication won't work, but you'll have some logs

Trustelem Radius on Bastion for Trustelem users

On Trustelem admin page

- Go on the tab **Apps**, and create a **Bastion** application (if not already done in a LDAP setup)

- Enable the **Radius** protocol

Settings for **Bastion 1** [DEBUG]

Name

Icon 

State

LDAP

Base DN

LDAP service account

LDAP service password 👁️ 📄

Radius

Radius secret 👁️ 📄

ⓘ Display setup instructions
 ✕ Close

- Go on the **Service** setup in the **Install Trustelem Connect** chapter
- Click on **Add an application +** and select the **Bastion** (if not already done in a LDAP setup)
- 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 *
 - you can let the default port **1812** but if you don't know if it is already used on the machine running the connector, choose **2812** instead

- Click **Save** !

Applications		Add an application +		
Name	Service settings			
Bastion 	LISTEN ADDRESS	PORT	PROTOCOLS	
	 LDAP  * ▾	<input type="text" value="2001"/>	<input type="checkbox"/> LDAPS	
	 Radius  * ▾	<input type="text" value="1812"/>		

On the **Bastion admin page**

- Go on **Configuration > External authentication**
- Create a new **Radius authentication**
- In the field **Name** choose a name for your Radius authentication like **Trustelem Radius**
- In The fields **Server** and **Port**, write the IP / FQDN of the machine running **Trustelem Connect** and the port defined on the **Trustelem Service** previously setup (should be 1812 or 2812)
- In the **Timeout** field let the default value, unless you have latency on your network
- Provide the **Radius secret** in the fields **New secret** and **Confirm secret**.
This secret can be found in the Trustelem Bastion app model.
- Check the option **Use mobile device for 2 factor authentication(2FA)**
 - This option has be designed for MFA with push authentication. But the real effect is to skip the login + password step for the Radius authentication by automatically sending the login and an empty password.
 - Here we want to use Active Directory for the login + password step, so we don't want to ask for the Radius password = we need to activate this option.

- Click on **Apply**

Authentication type *

RADIUS

Name *

Trustelem-Radius with mobile device ⊗

Server *

10.10.126.201 ⊗

Port *

1812 ⊗

Timeout *

5 ⊗

In seconds

New secret

⊗

Confirm secret

⊗

Description

Use mobile device for Two-Factor Authentication (2FA)
Display a message informing the use of the mobile device to authenticate via a push notification

- Go on **Configuration > Authentication domains**
- Click on your existing **Trustelem Active Directory authentication domain**
- In the field **Secondary authentication** select the previous **Radius external authentication**
- Click on **Apply**

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 skip the 2nd factor step for some users, you can select for them the rule **Always allow** instead

on Trustelem.

If the authentication doesn't work correctly:

- Read the [debug chapter of LDAP-Radius Trustelem Connect](#)
- You can also verify if you checked the option **Use mobile device** on the **Radius external authentication**

Revision #18

Created 1 July 2022 08:49:51 by WALLIX Admin

Updated 21 February 2024 09:38:55 by WALLIX Admin