Integrations installation guide

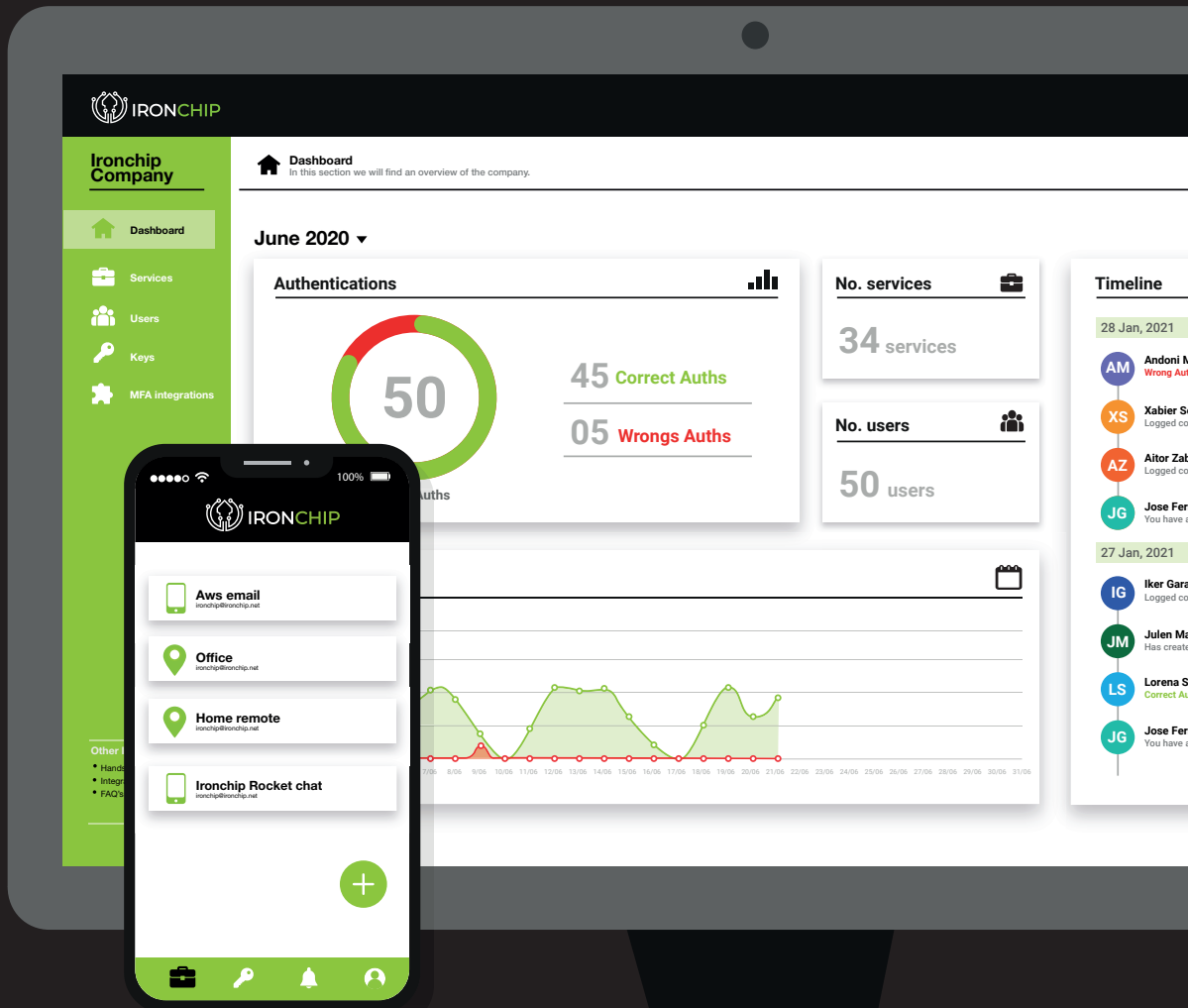
1 MFA Plugin for NPS

- Add service in dashboard
- Install the plugin
- Test the plugin
  Uninstall the plugin

2 MFA Plugin for ADFS

- Configure Claims Xray
- Add MFA integration in Dashboard
  Install the plugin
- Test the plugin
  Uninstall the plugin
  Add Claims XRay service in Dashboard
- ADFS 3.0 Configure Ironchip Mfa for a relying party trust
- ADFS 4.0 Configure Ironchip Mfa for a relying party trust

3 Error FAQ's



Introduction

Microsoft integrations

Ironchip can be easily and quickly integrated into Microsoft environments. For this purpose, we provide two different plugins that allow you to use Ironchip as a multifactor authentication in the active directory federation services (ADFS) and in the microsoft radius server (NPS).

This way we can protect your applications and remote connections in a simple way, just using an installer and configuring within the Microsoft tools.

Ironchip MFA Plugin for NPS

This plugin allows any company to use the Ironchip Location-Based Authentication (LBAuth) service to provide multi-factor authentication to Microsoft Network Policies Server. This allows companies with an Active Directory to provide RADIUS protection based on device and user location to the VPN and other services integrated with RADIUS technology.

The plugin provides:

- Multi-Factor Authentication for NPS.
- License loading from file.
- Plugin installer and uninstaller.
- Out-of-the-box solution. Get license, install and you can use it in your configured services.

Ironchip MFA Plugin for ADFS:

This plugin allows any company to use Ironchip Location Based Authentication service to provide Multi Factor Authentication to Microsoft Active directory Federation Services. This allow companies with an Active Directory to provide account protection based on user device and location to any application.

The plugin provides:

- Multi-Factor Authentication for ADFS.
- License loading from file.
- Plugin installer and uninstaller.
- Out-of-the-box solution. Get license, install and you can use it in your configured services.

The following chapters detail how to configure each of these plugins to use the Ironchip Location-Based Authentication (LBAuth) to provide multi-factor authentication.

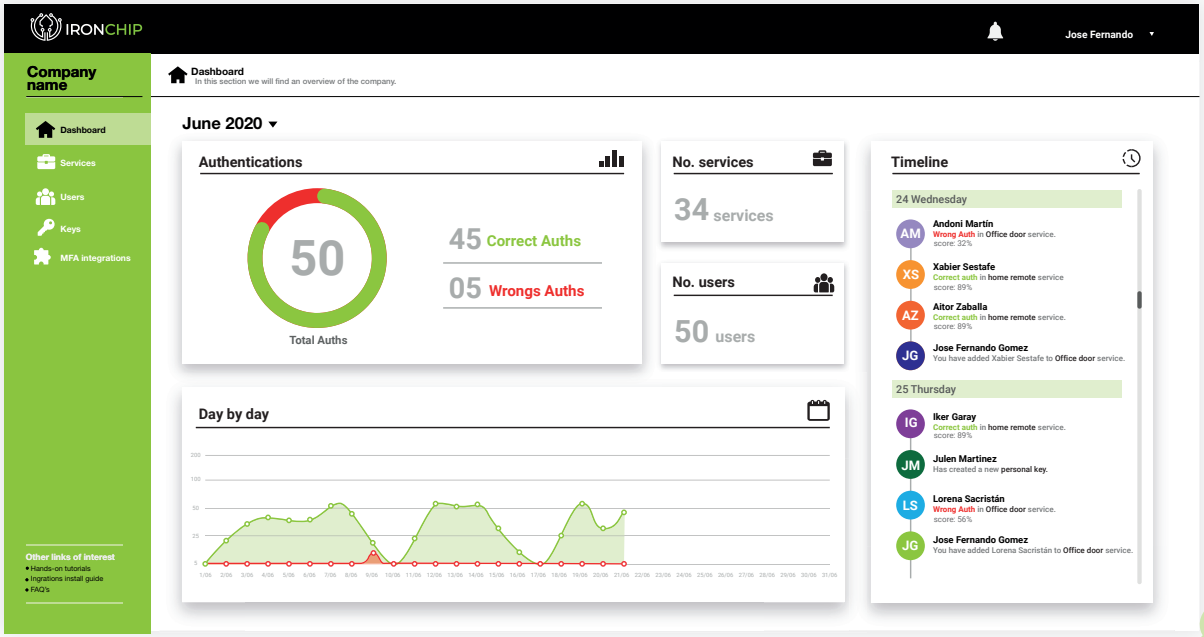
MFA Plugin for NPS

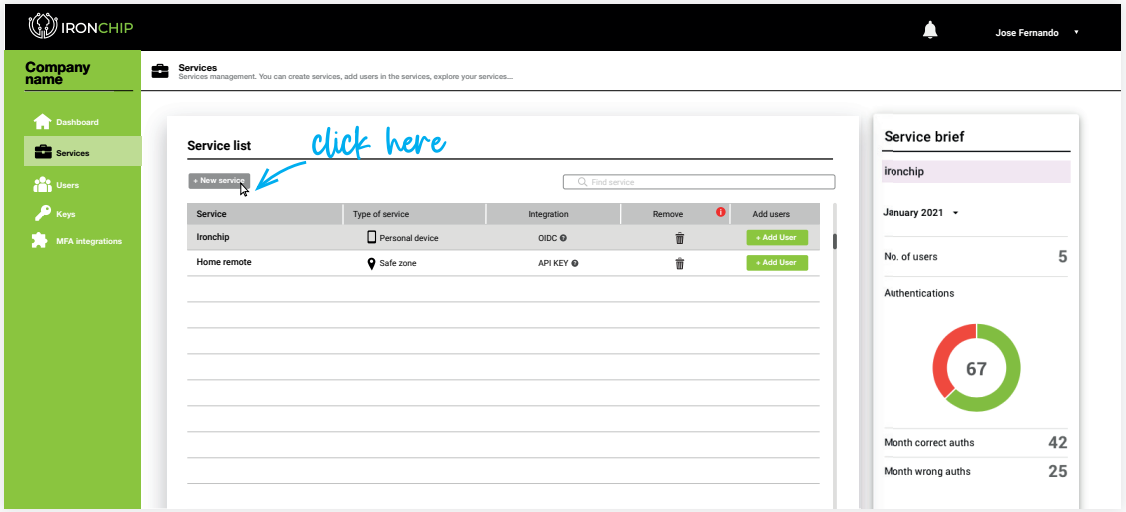
Add NPS integration

Create service in Ironchip dashboard

Once you are part of Ironchip, enter in your **Ironchip dashboard.**

In the following pages you will find the steps to add our technology in the required service with the MFA plugin for NPS.





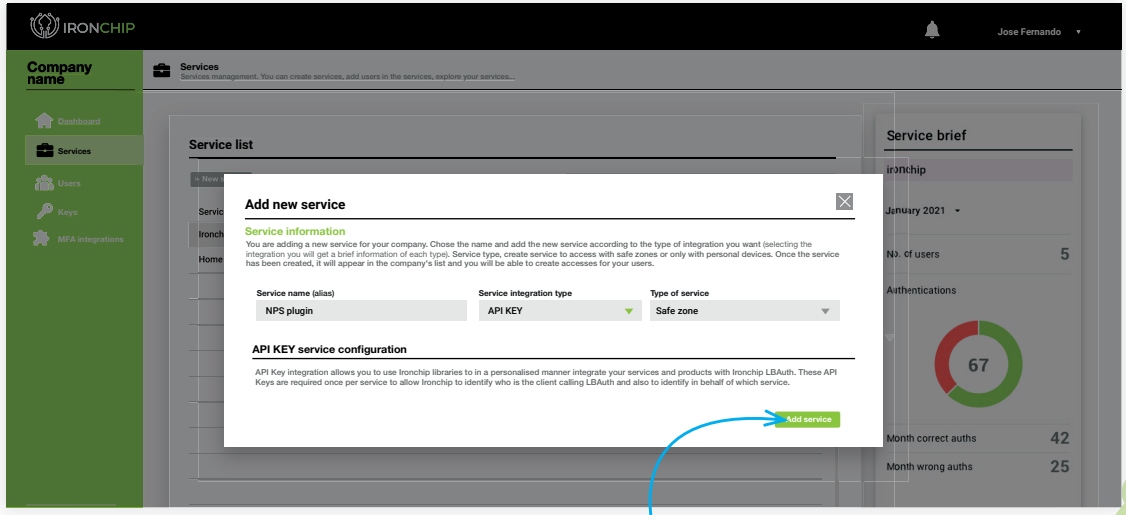
Go to the services section of your dashboard and click on New service to start.

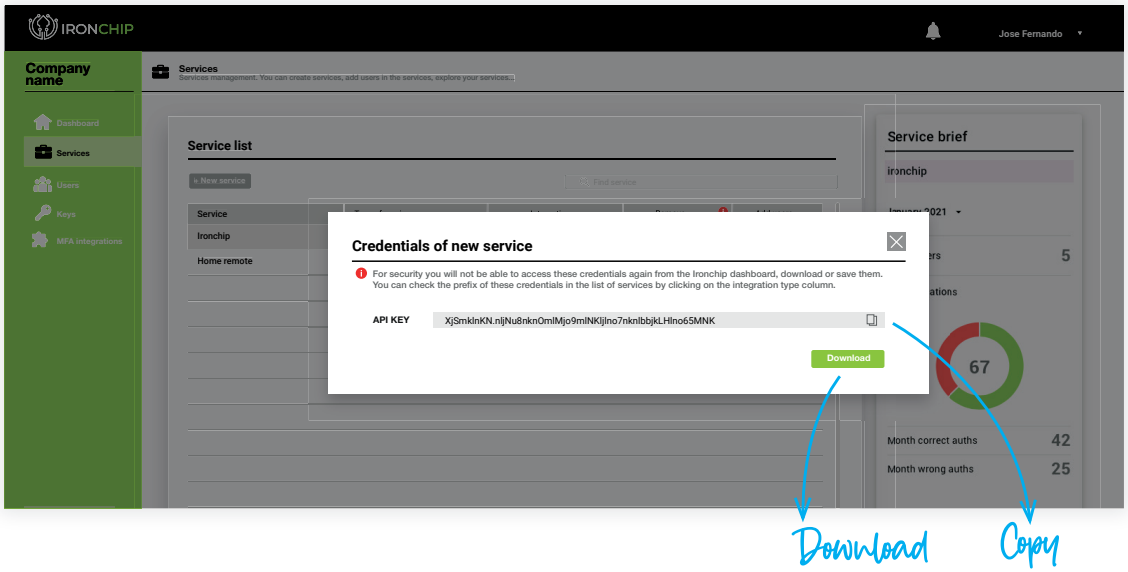
We have next fields:

Service name (alias): Should be declarative for service we are adding.

Integration Type: API KEY is required filed.

Type of service: Select based on our requirements, **personal device** if it will be a service that only needs to be accessed from device, and safe zone if it will be a service that needs to be in a **safe zone** to be accessed.





When you press add you will get the following screen.

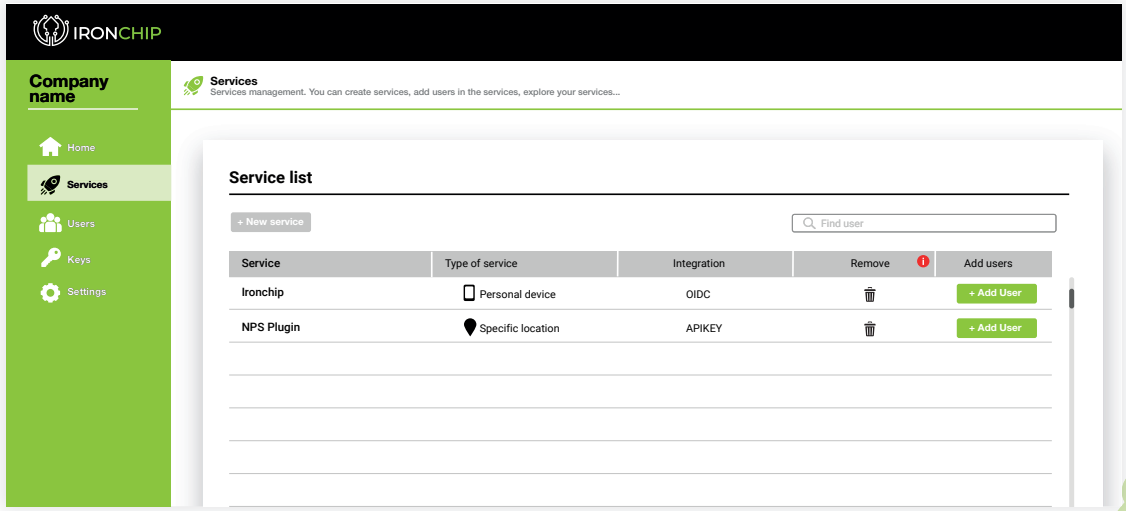
IMPORTANT! Be careful, you will receive an API KEY.

Download/save this data, you will not have access to it again.

You will be able to consult the Hint in the services table in the **Integration type column** in the future when you need it.

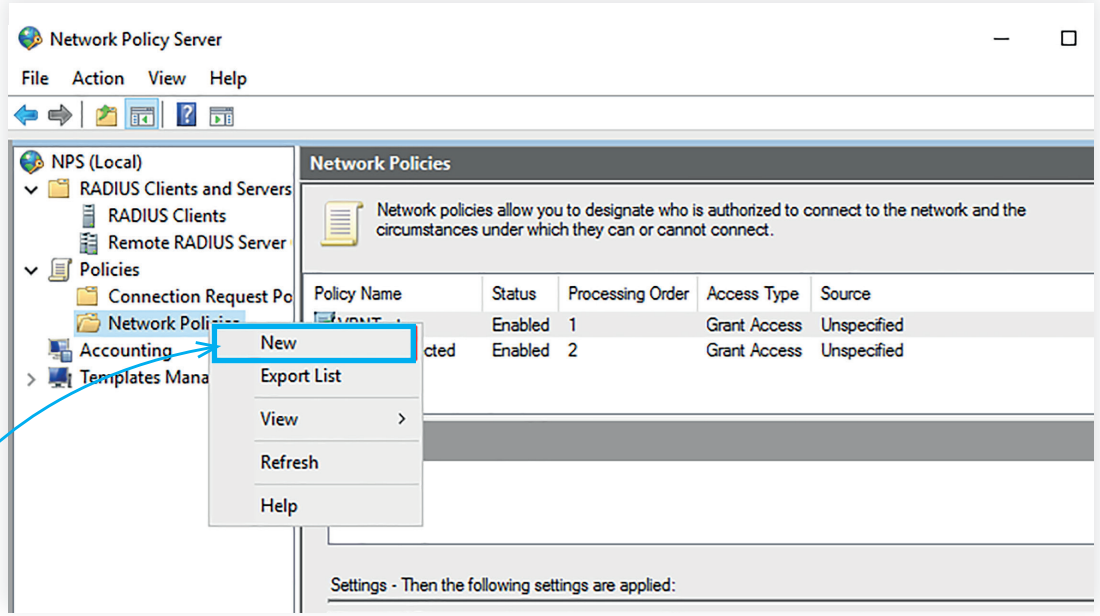
Once the service is added, it will appear in your list of services.

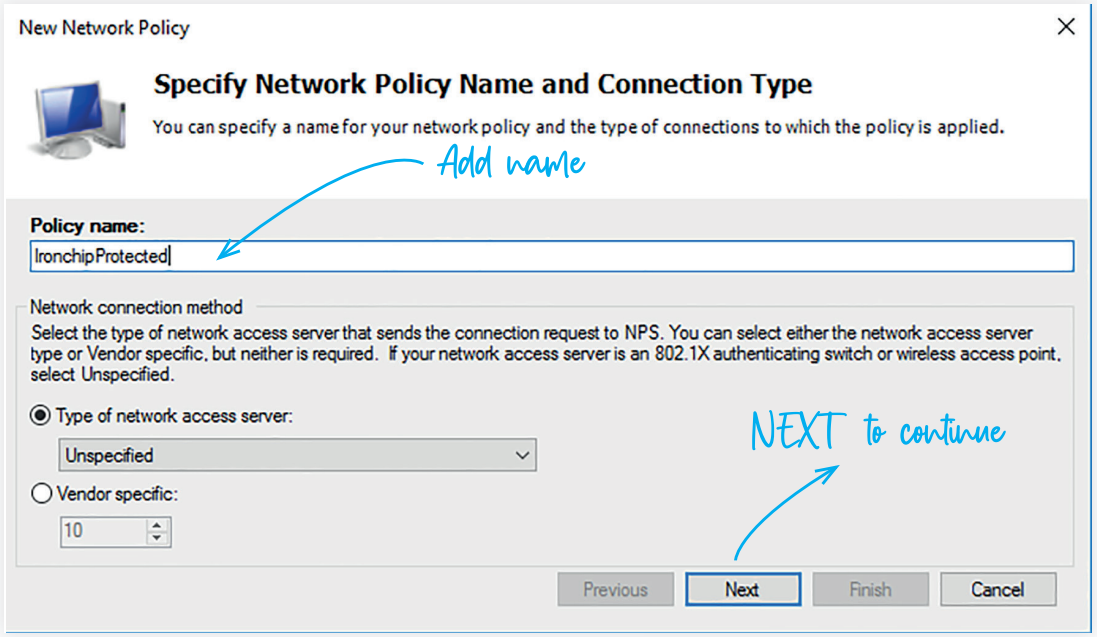
You will be able to have metrics of user interaction with this service by accessing to the service by clicking on the name in that list. To add users to this service refer to the applications manual linked in dashboard> other links of interest> Hands on tutorials.



Add a new network policy to Network Policy Server

Ironchip Multifactor Authentication use network policies to determine which user or group will be protected with Ironchip. To achieve that we must **create a new Network Policy in Network Policy Server**.

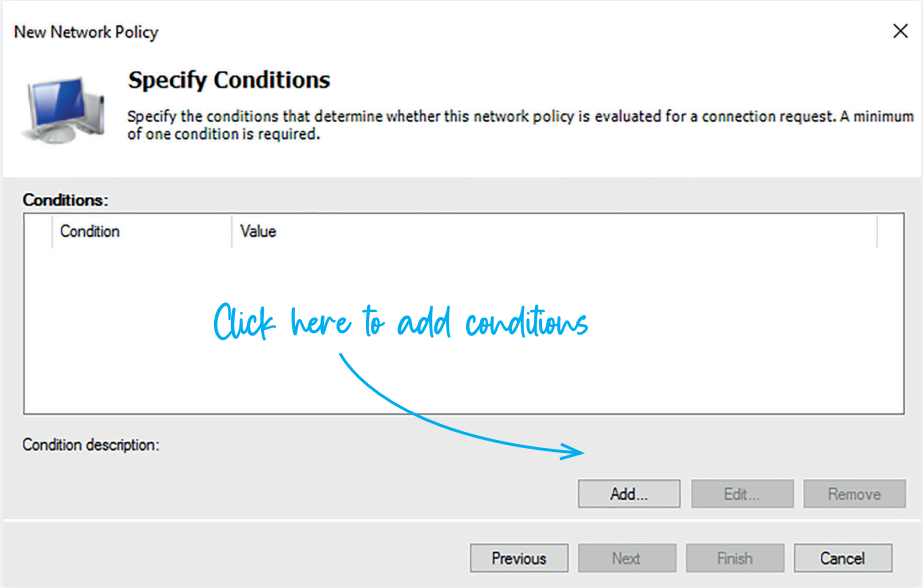


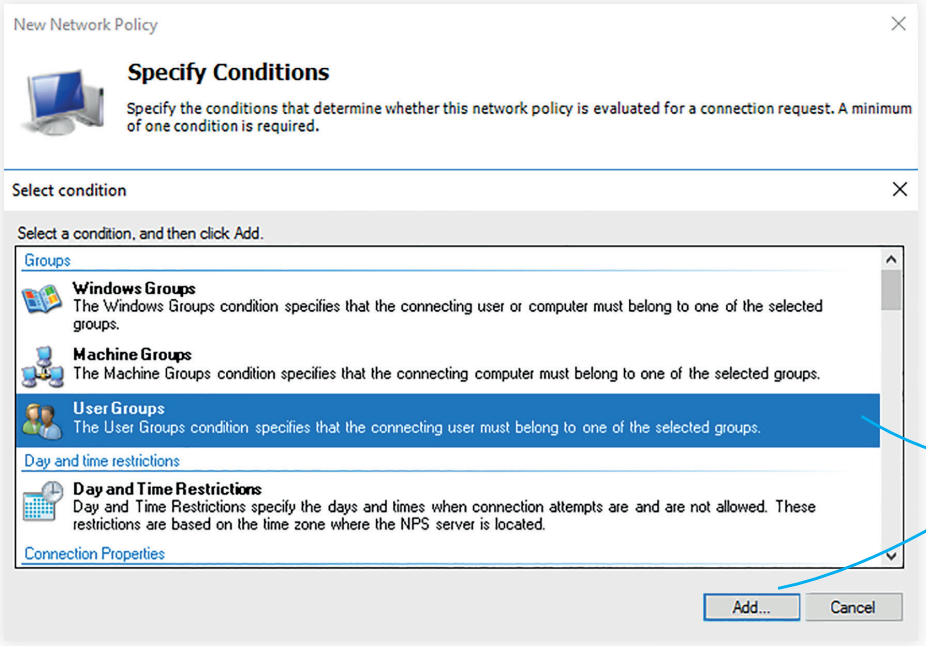


Provide a name to the policy.

This name will be used when you install the NPS MFA Plugin, to determine which policy protect.

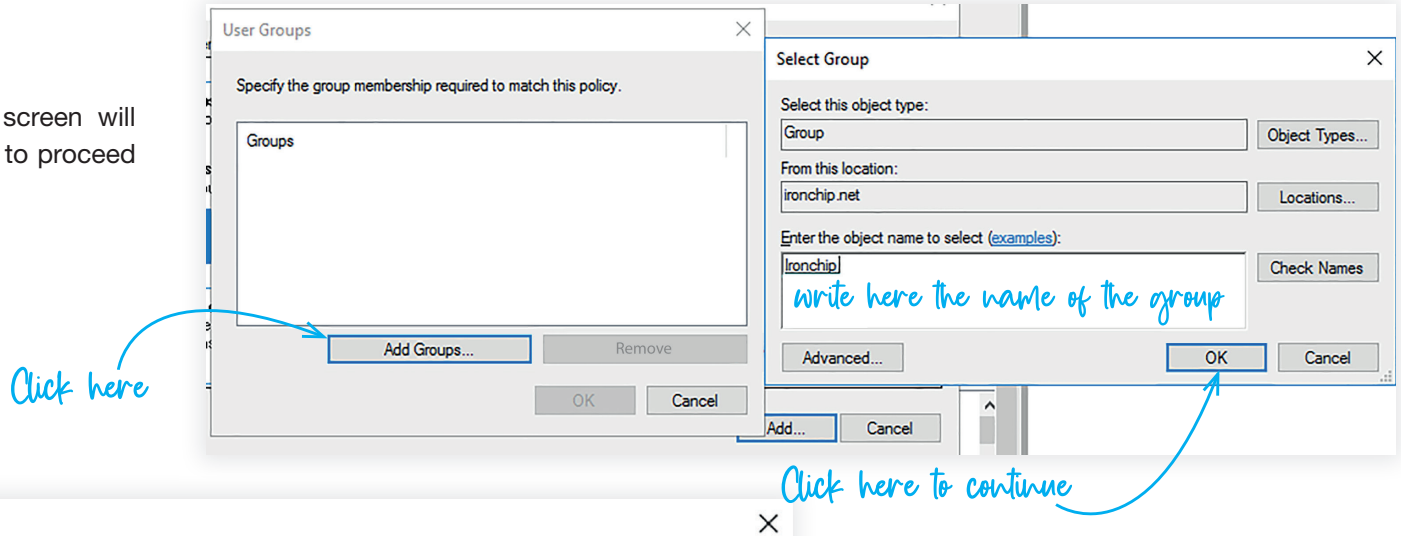
Here you can add all the conditions you want to determine for who and when will be applied this policy.

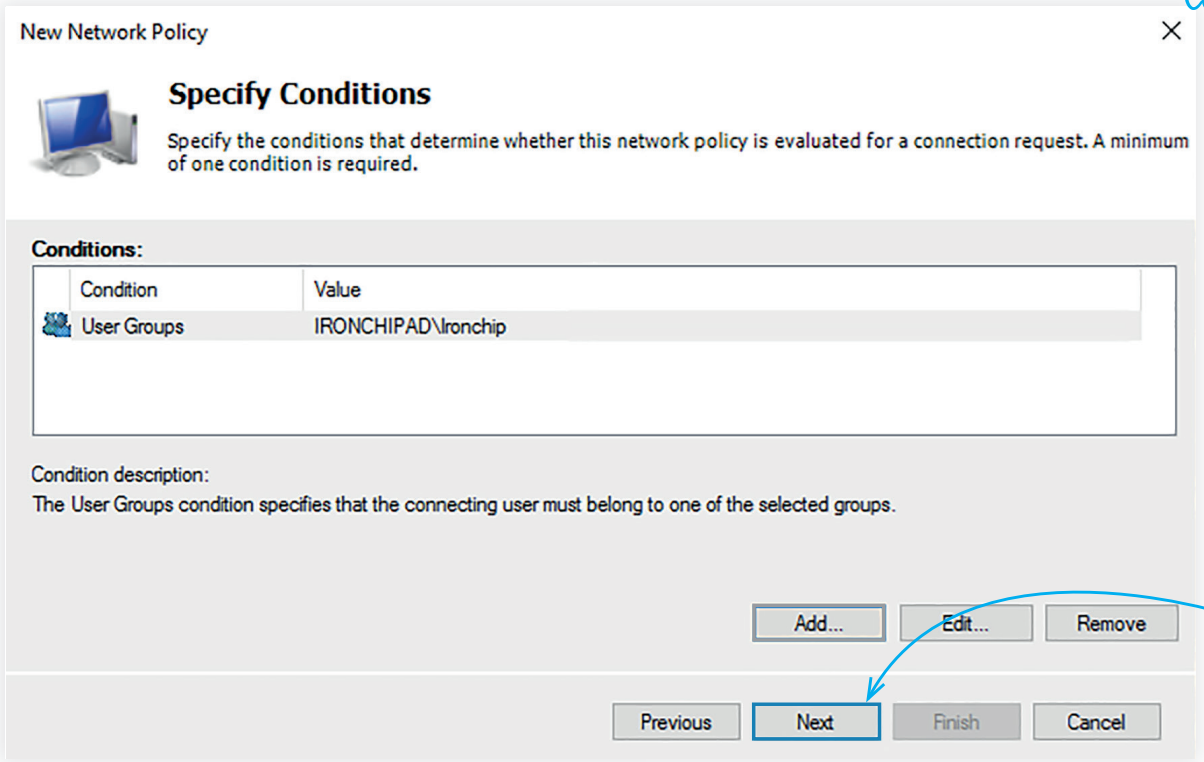




For this example, we will determine that this policy must be applied when a user is member of group Ironchip.

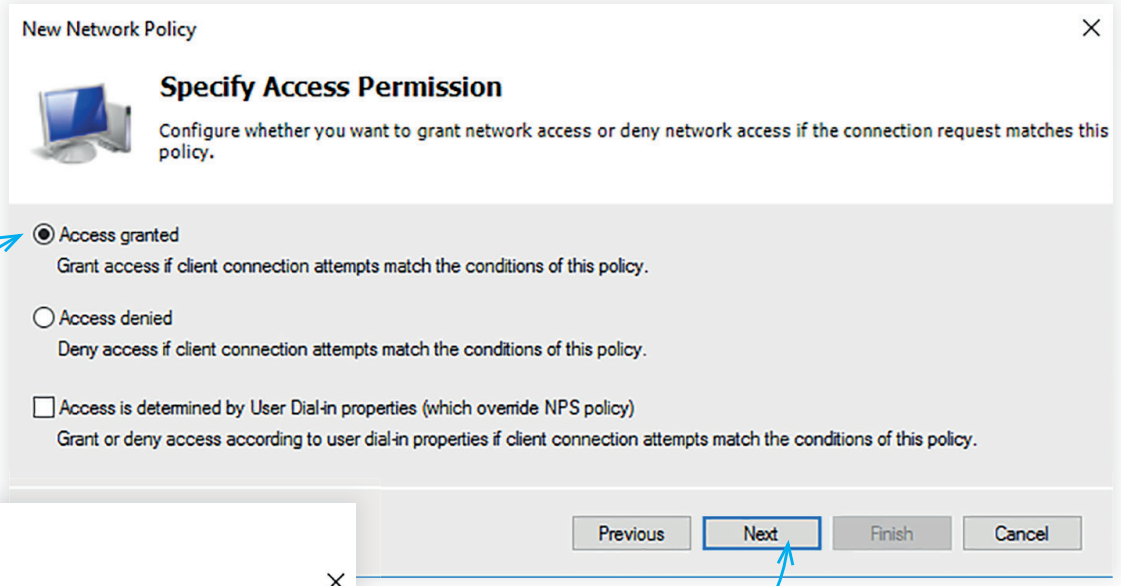
When you press add a new screen will appear, follow the steps below to proceed with the configuration.



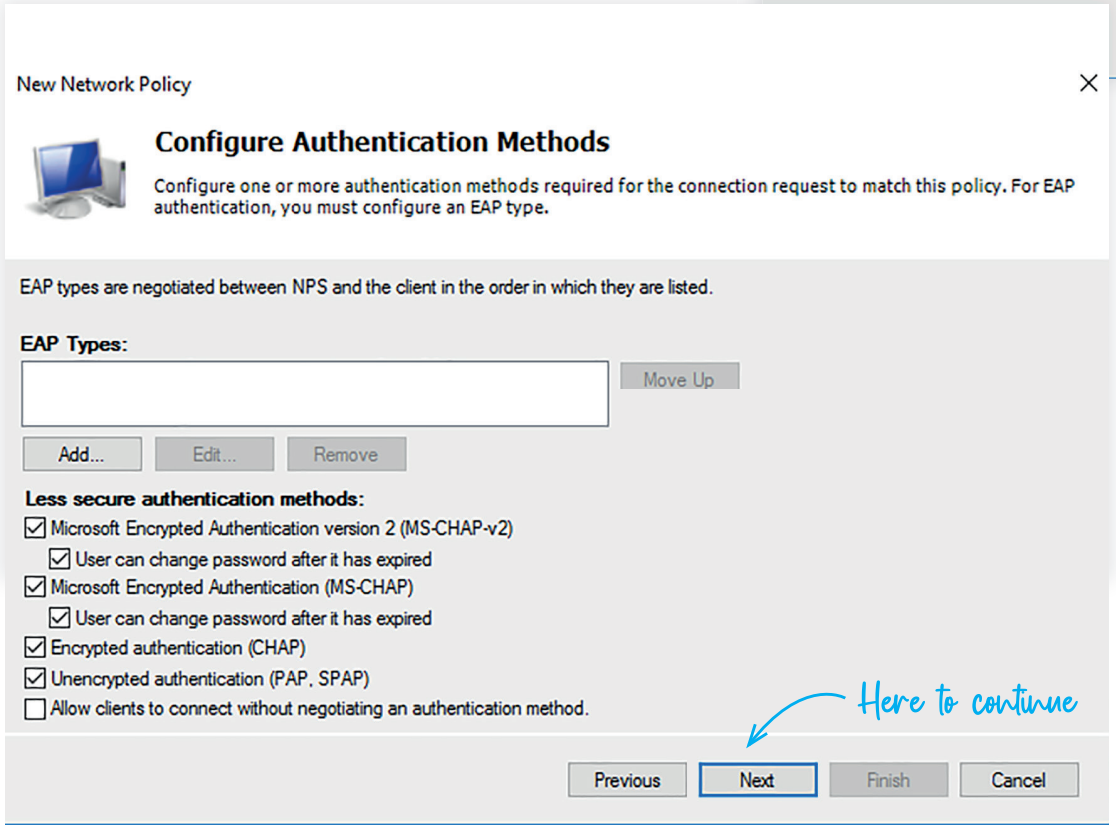


Once added and configured you will see next result. Click next to continue.

Next step, select access granted to grant access to users match this policy conditions, and click next to continue



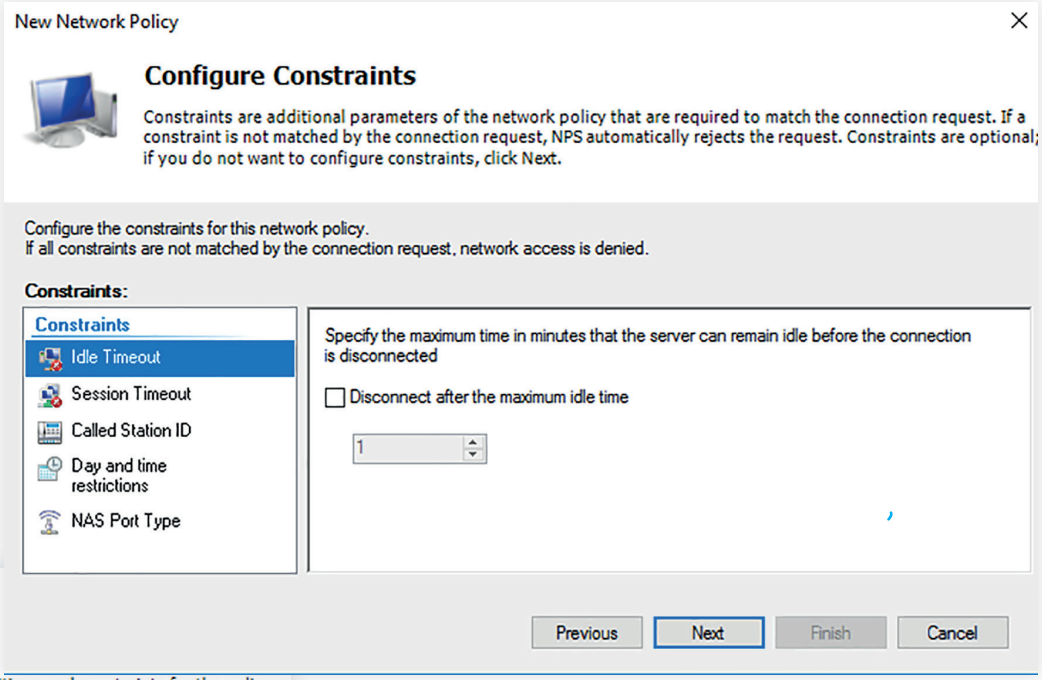
Here to continue

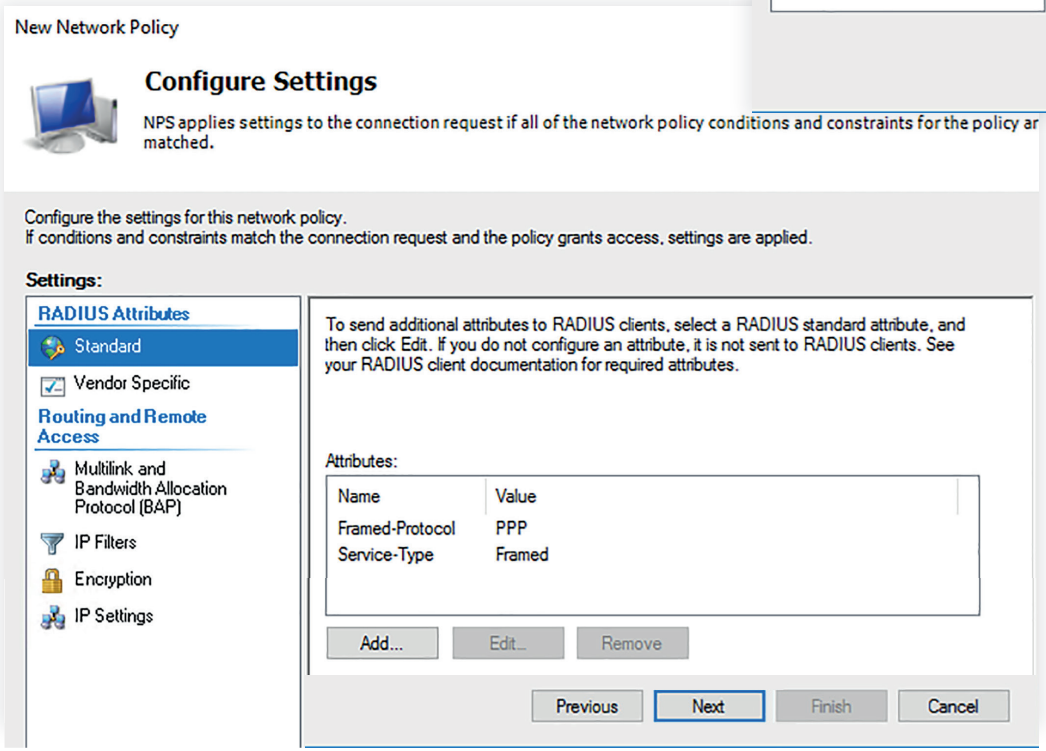


Here to continue

In this screen configure the authentication methods you will use.

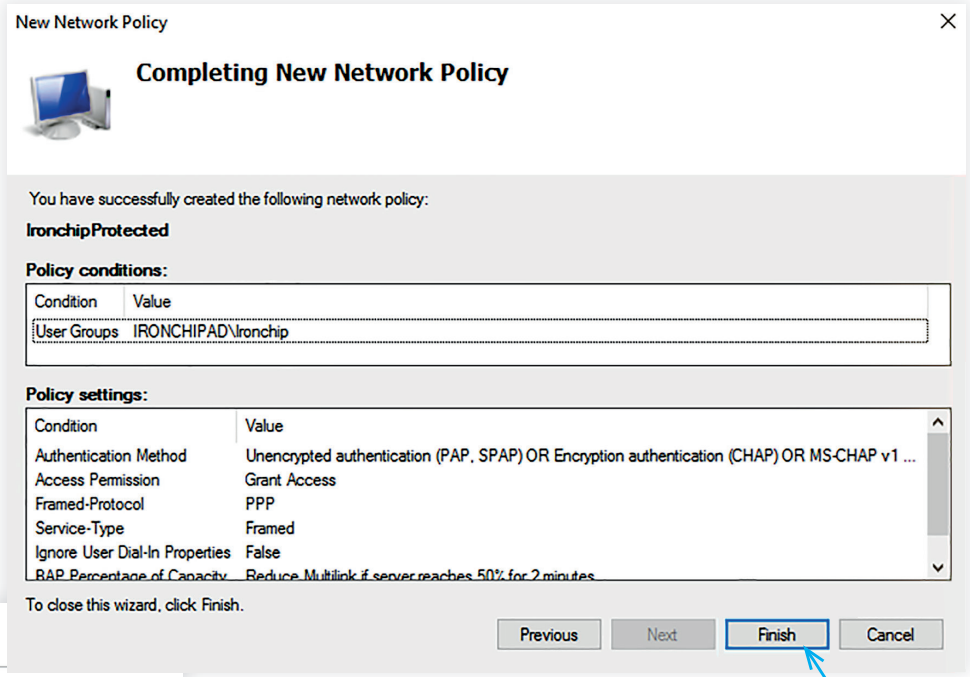
Next screen is for configure constraint to reject access automatically if one of this constraints are not acomplished. Fill this with the options you want.

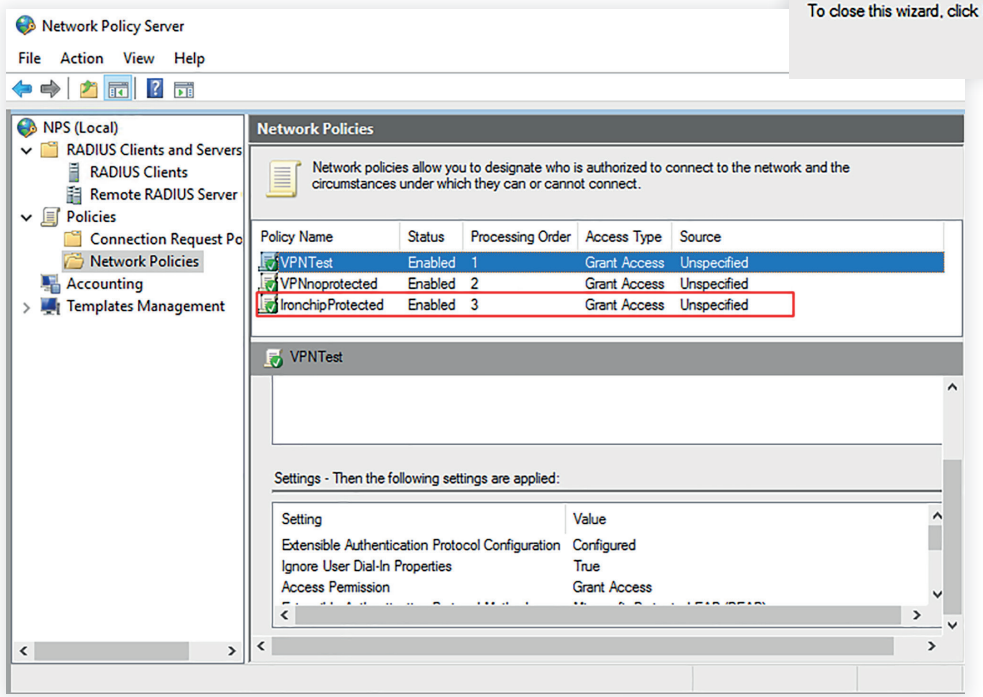




Click next. In this screen you can add settings to apply when policy constraints are matched.

A summary of the configuration will appear. Check that everything is OK and click "**Finish**".





Click here tu finish. You are ready to install the plugin

You have added your network policie and everything is ready for install the plugin.

Install the plugin

To install the plugin, you need the zip file Ironchip_MFA_ADFS_Plugin, which you can download from:

https://www.Ironchip.net/pluginsIronchip-mfa-nps-installer.zip

Unzip the folder in your desired path. We recommend to use:
C:\\Program Files\Ironchip MFA NPS Plugin

Go to that folder. In the folder you can see this files:

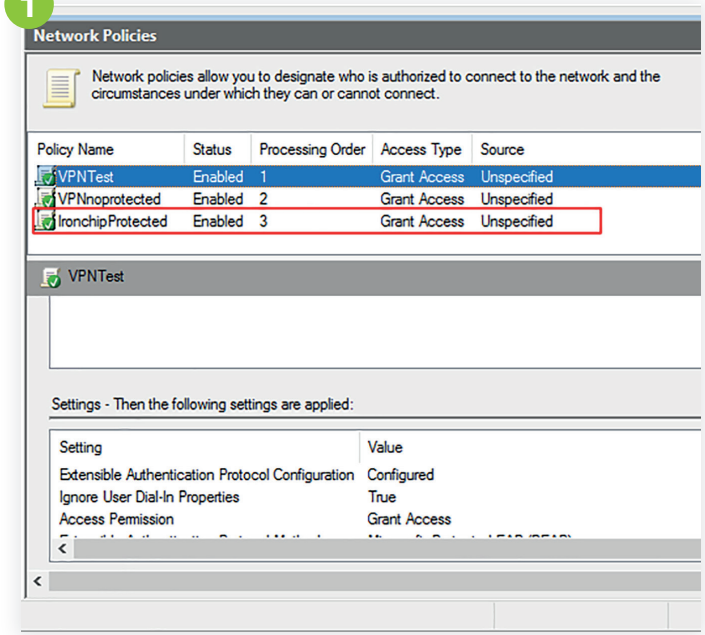
- Ironchip.Nps.BasePlugin.dll
- Ironchip.Nps.NativePlugin.dll
- Ironchip.Nps.MfaPlugin.dll
- IronchipNPSPluginInstaller.ps1
- IronchipNPSPluginUnnstaller.ps1
- IronchipRadiusCFG.json

Use any text editor to change the content of IronchipRadiusCFG.json file, filling:

- Your **Ironchip host**. In case you use our cloud solution, host will be api.Ironchip.com. Else, provide your custom host.
- Your **company API key** (credentials saved /downloaded from the dashboard) in the apiKey value.
- The network policy that you want to protect with Ironchip MFA. In the example we will use created IronchipProtected policy:

You can see the format in this example 2.

1



2

```
{
  "host": "dev.api.Ironchip.com",
  "apiKey": "vlBNO3.WM2A-bQoqM2BSbED1T1UpaZAO50tqCrbSQBMqb2qRhrVLWzzQg",
  "protectedpolicyname":"IronchipProtected"
}
```

After that, you can execute the IronchipNPSPluginInstaller.ps1 as Administrator. Just right-click the file and click over Run with PowerShell:

The installation script will execute the setup process, that will:

1. Check permissions. If you are not executing the script as Administrator user, script will fail and ask you to execute as Administrator.
2. Check if NPS service is installed and configured.
3. Ensure that you have your IronchipRadiusCFG.json configured.
4. Stop the NPS service.
5. Install all the plugin dlls.
6. Grant plugin permissions to user.
7. Configure the logs, and publish them to Event Viewer
8. Add plugin to windows registry.
9. Start the NPS service to detect new plugin.

3 The script will prompt the results in a PowerShell console, that allows you to check the steps:

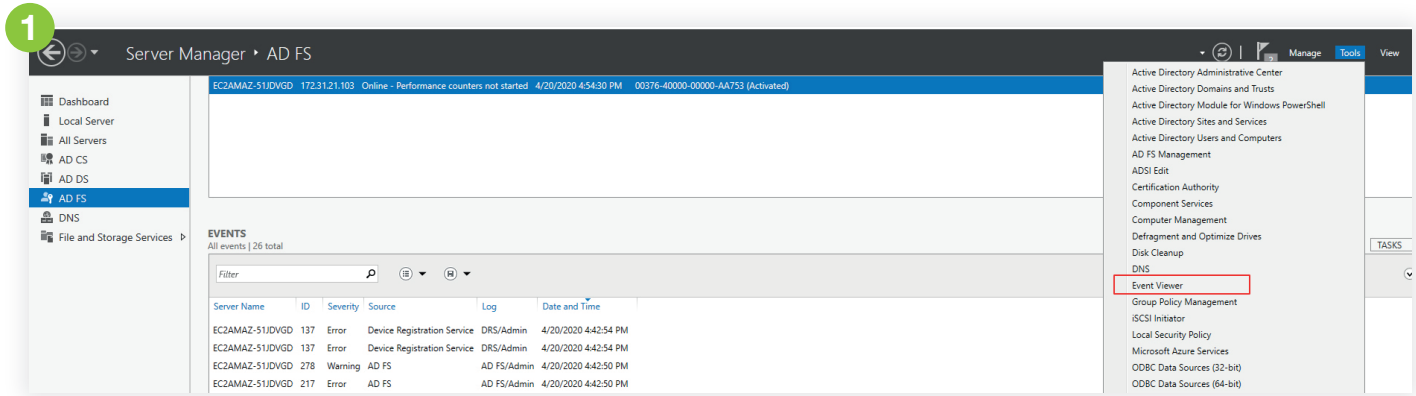
3

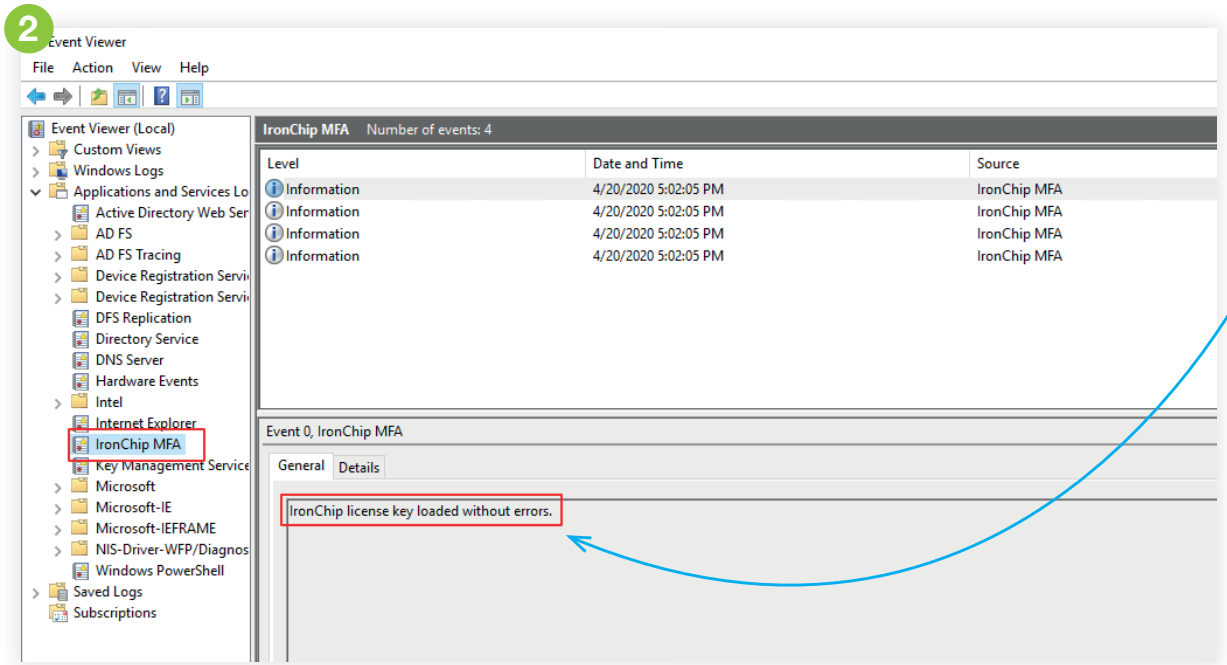
```
Stoping NPS service.
WARNING: Waiting for service 'Network Policy Server (IAS)' to stop...
WARNING: Waiting for service 'Network Policy Server (IAS)' to stop...
Stoped.
Installing Native Base library ...
Installed
Installing Plugin Base library ...
Installed
Installing Plugin library ...
Installed
Configuring Ironchip Plugin library with IronchipRadiusCFG.json properties ...
Configured
Granting permisions for Ironchip Plugin
Permisions granted
Activating event logs for plugin
Creating eventlog 'INPSPlugin'
Activated event logs. You can see logs in EventViewer>INPSPlugin
Adding plugin to NPS windows registry.
Added.
Restarting NPS service.
Restarted.
Ironchip MFA Plugin installed
```

Your plugin is already installed. Now test the plugin!

Test the plugin

1 Access Event Viewer to see Ironchip MFA Plugin logs.





2 If everything is OK, you must see **"INPSPlugin"** in Application and Services Logs list. Click on it, and if plugin is installed you must see **"Ironchip license key loaded without errors."** in logs as you can see here:

3 If you see the message **"Unable to load Ironchip license key. Check that it is the correct license and try again. If problem persist contact Ironchip support for help."**, go to FAQ's chapter at the end of this guide.

Uninstall the plugin

Execute the **Uninstall-Script.ps1** as Administrator. Just right-click the file and click over Run with PowerShell:

You will be prompted to trust the script. Type A and press enter.

The installation script will execute the setup process, that will:

1. Check permissions. If you are not executing the script as Administrator user, script will fail and ask you to execute as Administrator.
2. Check if NPS service is installed and configured.
3. Ensure that you have your License.json configured.
4. Remove logs and config on Event Viewer
5. Remove the plugin in GAC.
6. Restart the NPS service to detect GAC removed libraries.
7. Unegister plugin installed in NPS.
8. Delete Auth Methods and policies to select IronChip MFA.
9. Restart the NPS service to unregister plugin.

1 The script will prompt the results in a PowerShell console, that allows you to check the steps:

1

```
Stoping NPS service.
WARNING: Waiting for service 'Network Policy
Server (IAS)' to stop...
WARNING: Waiting for service 'Network Policy
Server (IAS)' to stop...
Stoped.
Removing plugin of NPS windows registry.
Removed.
Removing Plugin library ...
Removed
Removing Native Base library ...
Removed
Removing Plugin Base library ...
Removed
Removing eventlog 'INPSPlugin'
Removed
Restarting NPS service.
Restarted.
IronChip NPS Plugin removed
```

MFA Plugin for ADFS

Add ADFS integration

Below are the steps to follow to install the ADFS plugin with the authentication of our technology in the required service.

To do so, you will first need to have:

- ADFS configured
- and access to the LBAuth control panel.

Configure Claims Xray as test ADFS application

Navigate to **https://adfshelp.microsoft.com/ClaimsXray/TokenRequest** and follow instructions

1 Execute PowerShell as Administrator and run:

This adds Claims Xray as RelyingPartyTrust

If you want to add OIDC integration execute 2 :

Now we should see Claims Xray as Relying Party Trusts 3

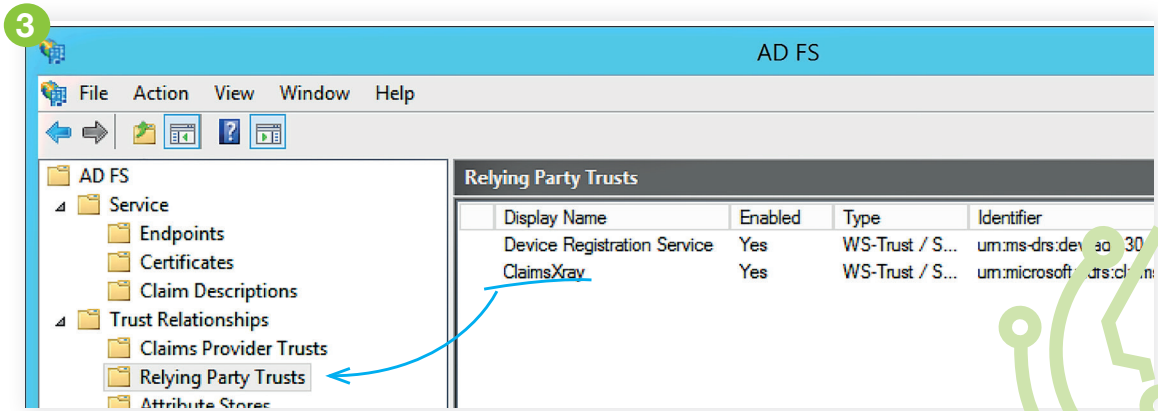
1

```
$authzRules = "=>issue(Type = `"http://schemas.microsoft.com/authorization/claims/permit`", Value = `"true`"); "

$issuanceRules = "@RuleName = `"Issue all claims`"`nx:[]=>issue(claim = x); "

$redirectUrl = "https://adfshelp.microsoft.com/ClaimsXray/TokenResponse"

$samlEndpoint = New-AdfsSamlEndpoint - Binding POST -Protocol SAMLAssertionConsumer - Uri $redirectUrl


Add-ADFSRelyingPartyTrust -Name "ClaimsXray" -Identifier "urn:microsoft:adfs:claimsxray" -IssuanceAuthorizationRules $authzRules -IssuanceTransformRules $issuanceRules -WSFedEndpoint $redirectUrl -SamlEndpoint $samlEndpoint
```

2

```
Add-AdfsClient -Name "ClaimsXrayClient" -ClientId "claimsxrayclient" -RedirectUri https://adfshelp.microsoft.com/ClaimsXray/TokenResponse


if ([System.Environment]::OSVersion.Version.major -gt 6) { Grant-AdfsApplicationPermission -ServerRoleIdentifier urn:microsoft:adfs:claimsxray -AllowAllRegisteredClients -ScopeNames "openid","profile" }
```

3

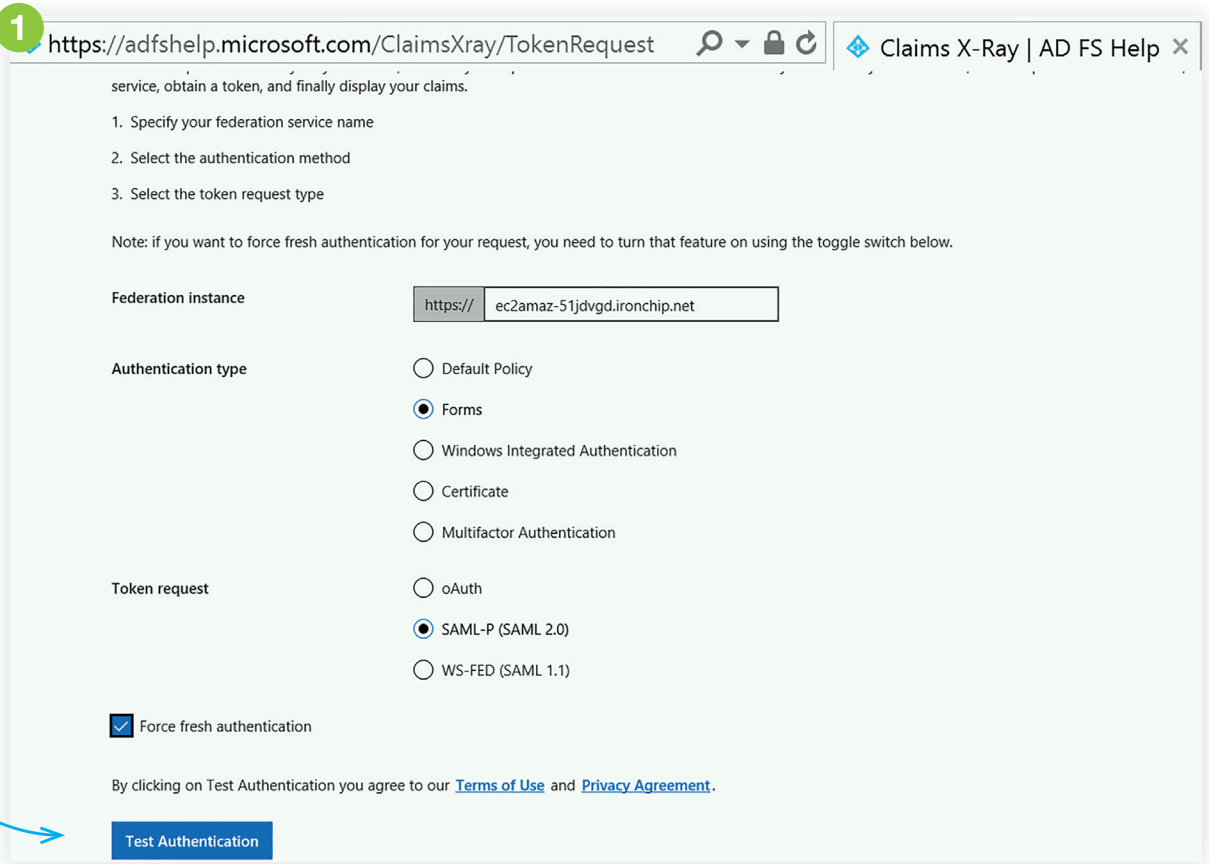


Test X-Ray

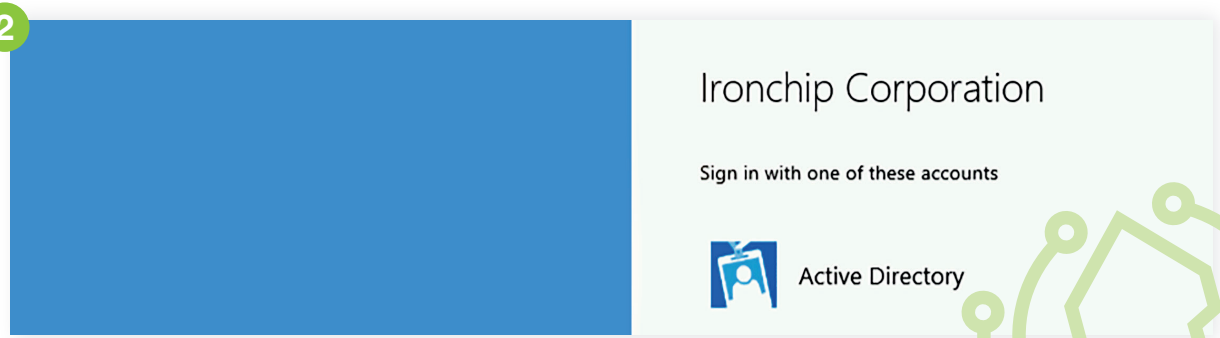
You can use the tool to test adfs. After that, configure it as you can see in next image 1 :

When you click on **Test Authentication,** you will be redirected to your ADFS 2 .

1

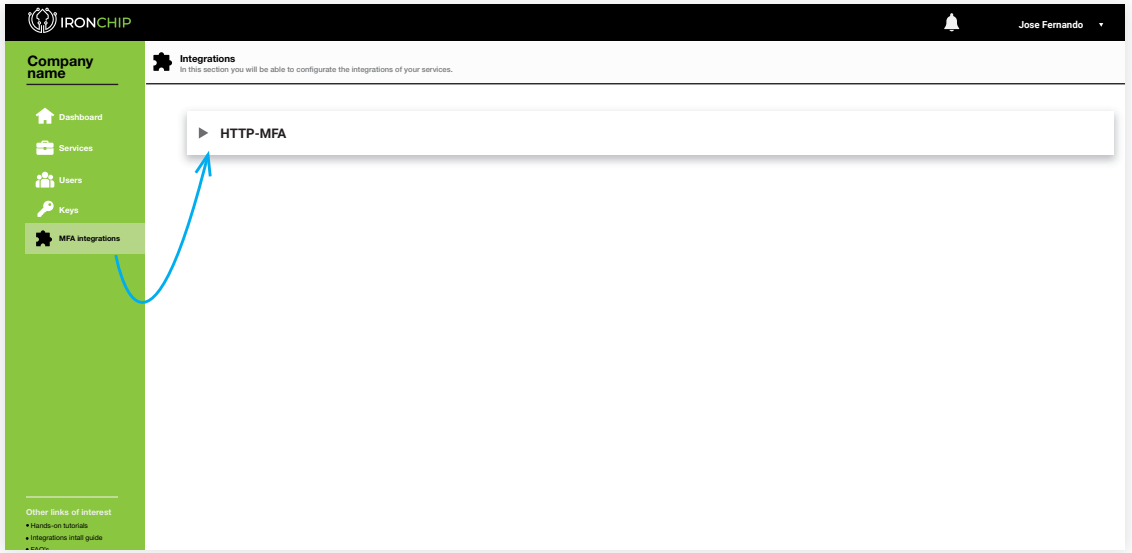


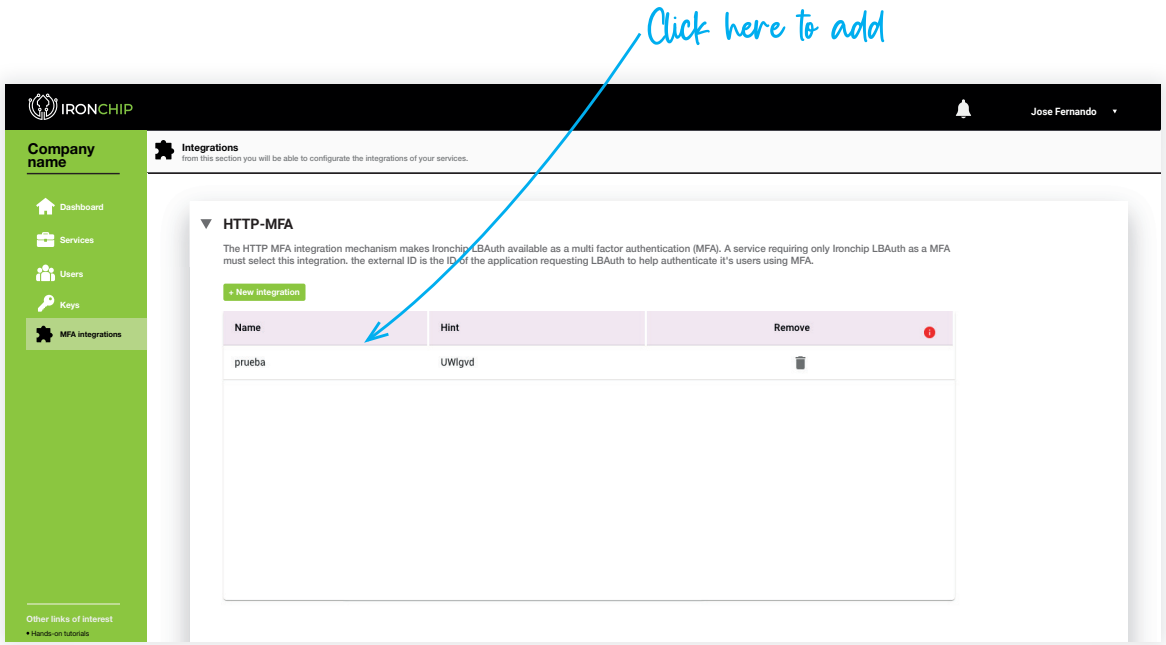
2



Add ADFS as Multifactor Authentication in Ironchip Dashboard

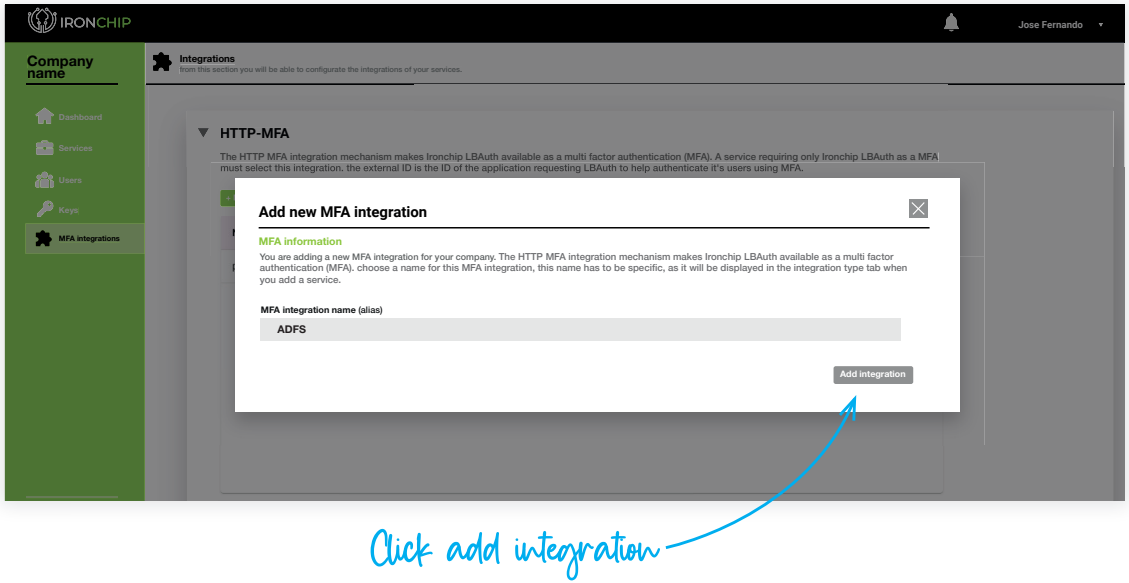
Once we access into **Ironchip Dashboard** we have to navigate into **Integrations section**, to http-mfa.

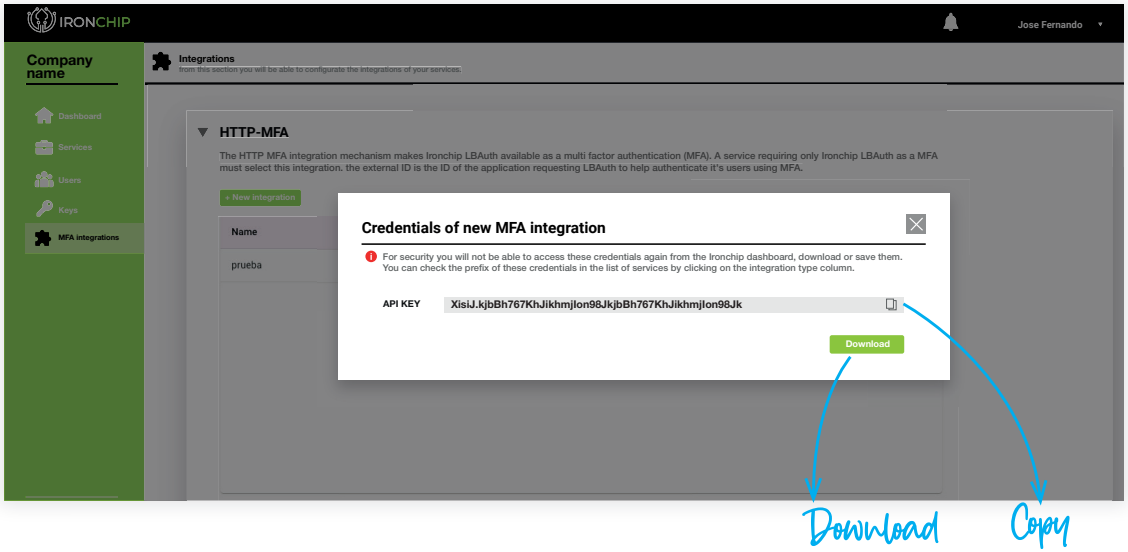




Click on **new integration**, and a new tab will be displayed so that you can add the new integration in your company.

Add name for the new integration and click on **Add integration** button.





When you press add you will get the following screen.

IMPORTANT! Be careful, you will receive an API KEY.

Download/save this data, you will not have access to it again.

You will be able to consult the Hint in the services table in the **Integration type column** in the future when you need it.

Install the plugin

To install the plugin, you need the IronChip_MFA_ADFS_Plugin zip file, that you can download from:

https://www.ironchip.net/plugins/ironchip-mfa-adfs-installer.zip

Unzip the folder in your desired path. We recommend to use: **C:\\Program Files\Ironchip MFA ADFS Plugin**

Go to that folder. In the folder you can see this files:

- IronChipADFSPlugin.dll
- Install-Script.ps1
- Uninstall-Script.ps1
- License.json

Use any text editor to change the content of IronchipRadiusCFG.json file, filling Your **company API key** (credentials saved /downloaded from the dashboard) in the apiKey value, inside double-quotes, as you can see in this example 1.

1

```
{
  “host”: "testing.api.Ironchip.com",
  “apiKey”:"Shu2Zo.ORG0UlbkEnci3wwu-hNkBt1kVX48jK6ntwX5NN0ZIOJBp2fuK7yaQ-VzcMXZ0w"
}
```

After that, you can execute the Install-Script.ps1 as Administrator. Just right-click the file and click over Run with PowerShell:

You will be prompted to trust the script. Type A and press enter.

The installation script will execute the setup process, that will:

1. Check permissions. If you are not executing the script as Administrator user, script will fail and ask you to execute as Administrator.
2. Check if ADFS service is installed and configured.
3. Ensure that you have your License.json configured.
4. Configure the logs, and publish them to Event Viewer
5. Install the plugin in GAC.
6. Restart the ADFS service to detect GAC new libraries.
7. Register plugin installed in ADFS.
8. Configure the ADFS Auth Methods and policies to select that MFA script as default when MFA is allowed for a service.
9. Restart the ADFS service to load registered plugin.

2 The script will prompt the results in a PowerShell console, that allows you to check the steps:

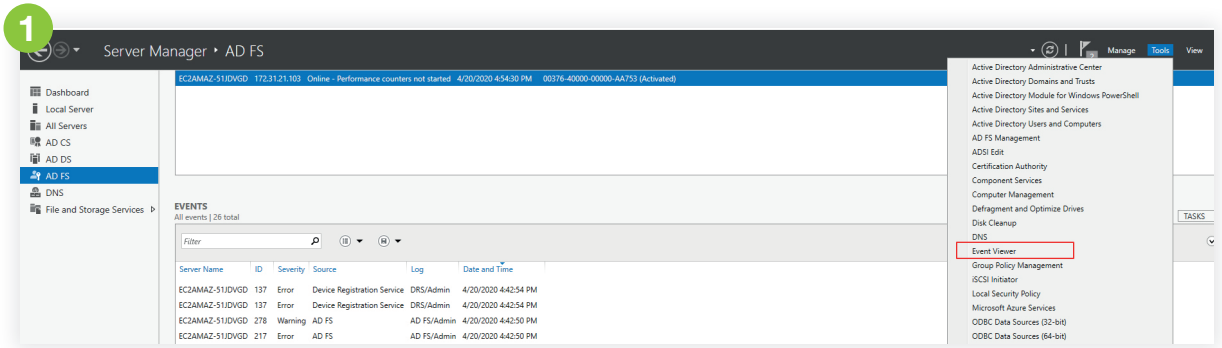
2

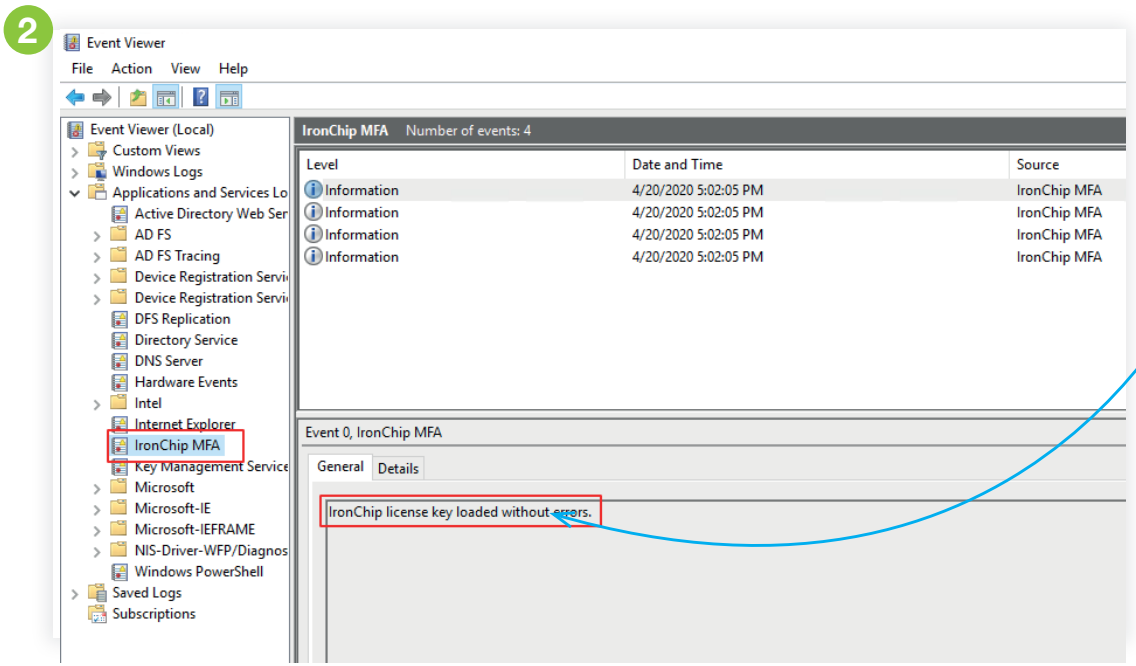
```
PS C:\Users\Administrator> C:\Program Files\IronchipADFSPlugin\
Install-Script.ps1
Activating event logs for plugin
Creating eventlog 'ADFS Ironchip Plugin'
Activated event logs.
Installing assemblies in GAC

GAC    Version        Location
---    -------        ---------

True    v4.0.30319      C:\Windows\Microsoft.Net\assembly\GAC_64\
System.EnterpriseServices\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.
EnterpriseServices.dll
Stop AD FS Service
Installing assemblies: IronchipADFSPlugin.dll
Installing IronchipADFSPlugin.dll on C:\Program Files\IronchipAD-
FSPlugin\IronchipADFSPlugin.dll
Copied assemblies to GAC
Start AD FS Service
WARNING: PS0105: No authentication provider with name 'IronchipM-
FA' is present in the policy store.
C:\Program Files\IronchipADFSPlugin\IronchipADFSPlugin.dll
Install IronchipMFA on YOUR-MACHINE-NAME
Register Ironchip MFA plugin in ADFS
Install IronchipMFA on YOUR-MACHINE-NAME
WARNING: PS0114: The authentication provider was successfully re-
gistered with the policy store.  To enable this provider, you must
restart the AD FS Windows Service on each server in the farm.
Ironchip MFA plugin registered. Restarting AD FS
Finished publishing IronchipMFA to YOUR-MACHINE-NAME
Ironchip MFA Plugin installed
```

Your plugin is now installed

Test the plugin

1 Access Event Viewer to see Ironchip MFA Plugin logs.





2 If everything is OK, you must see **"IronChip ADFS Plugin"** in Application and Services Logs list. Click on it, and if plugin is installed you must see "IronChip license key loaded without errors." in logs as you can see here:

3 If you see the message "Unable to load IronChip license key. Check that it is the correct license and try again. If problem persist contact IronChip support for help.", go to FAQ's chapter at the end of this guide.

Uninstall the plugin

Execute the Uninstall-Script.ps1 as Administrator. Just right-click the file and click over Run with PowerShell:

You will be prompted to trust the script. Type A and press enter.

The installation script will execute the setup process, that will:

1. Check permissions. If you are not executing the script as Administrator user, script will fail and ask you to execute as Administrator.
2. Check if ADFS service is installed and configured.
3. Ensure that you have your License.json configured.
4. Remove logs and config on Event Viewer
5. Remove the plugin in GAC.
6. Restart the ADFS service to detect GAC removed libraries.
7. Unegister plugin installed in ADFS.
8. Delete Auth Methods and policies to select IronChip MFA.
9. Restart the ADFS service to unregister plugin.

1 The script will prompt the results in a PowerShell console, that allows you to check the steps:

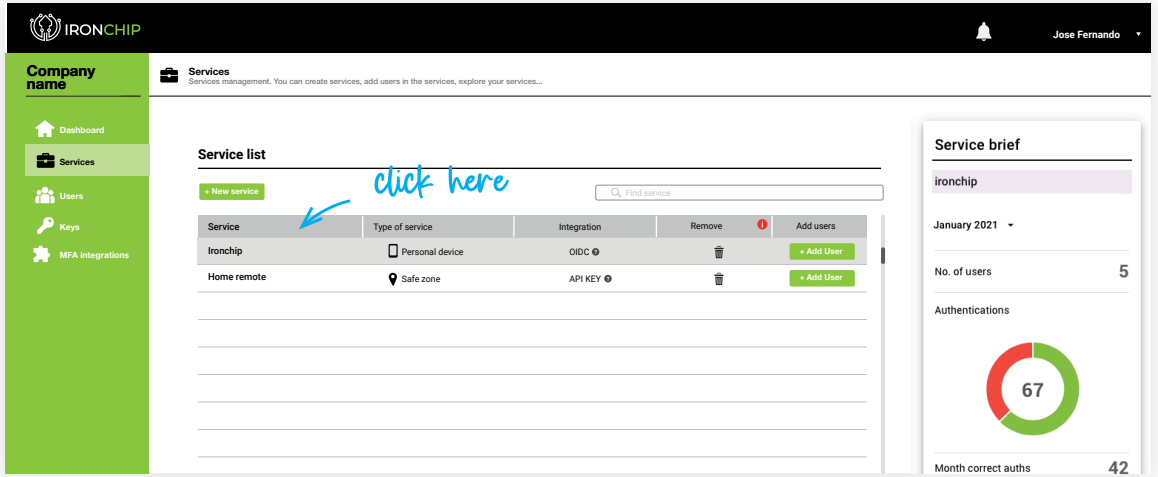
1

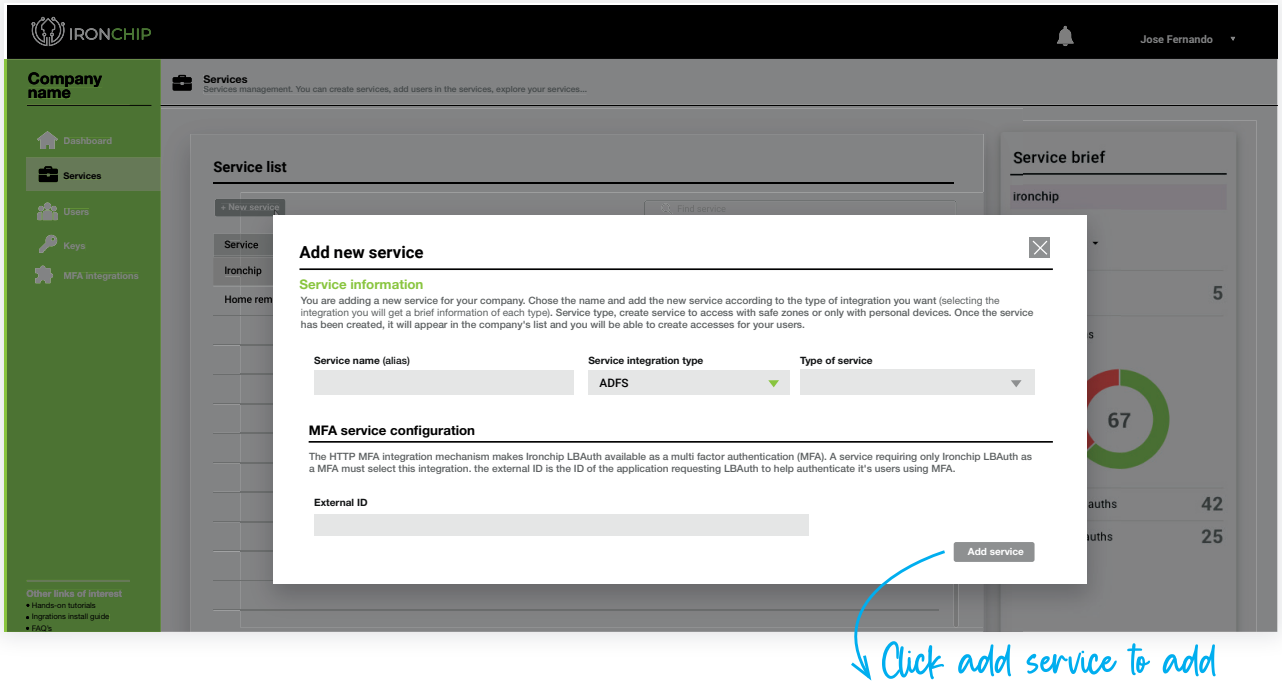
```
PS C:\Users\Administrator> C:\Program Files\
IronchipADFSPlugin\Uninstall-Script.ps1

Removing eventlog 'ADFS Ironchip Plugin'

Removing assemblies in GAC

GAC    Version    Location


---    -------    --------


True     v4.0.30319         C:\Windows\Microsoft.
Net\assembly\GAC_64\System.EnterpriseServices\
v4.0_4.0.0.0__b03f5f7f11d50a3a\System.
EnterpriseServices.dll

Stop AD FS Service

Removing IronchipADFSPlugin.dll on C:\Program Fi-
les\IronchipADFSPlugin\IronchipADFSPlugin.dll

Removed assemblies to GAC

Start AD FS Service

True

WARNING: PS0103: The authentication provider was
successfully unregistered from the policy store.
Restart the AD FS Windows Service on each server
in the farm.

Removed IronchipMFA from AD FS server YOUR-MACHINE-
NAME
```

Add Claims XRay as new Service

In this step we have to configure a new service in Ironchip Dashboard using ADFS integration Method.

In our **Dashboard**, we have to go to **Services** section and click in **new service** button.





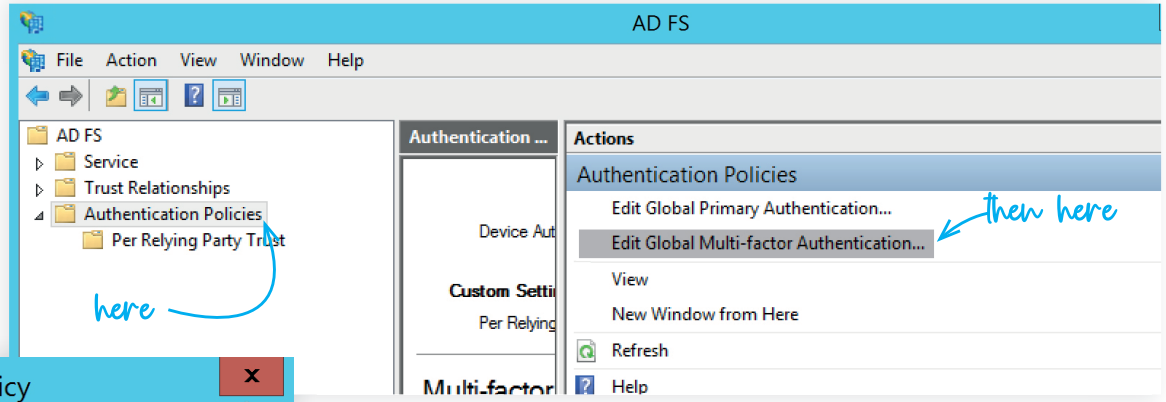
In this step we have select the new integration type we have create, **ADFS,** and complete the next fields:

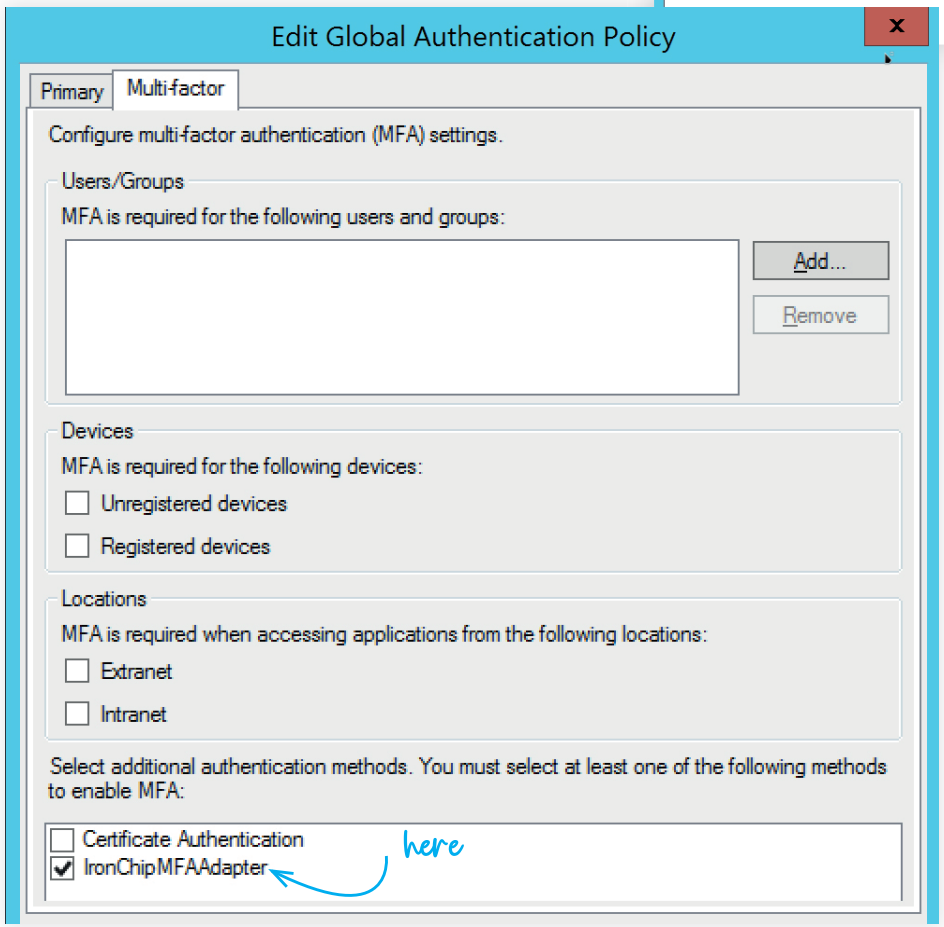
-**External Id:** must match with ADFS identifier

Then click add service and a new service will appear in our service list.

ADFS 3.0 Configure Ironchip Mfa for a relying party trust

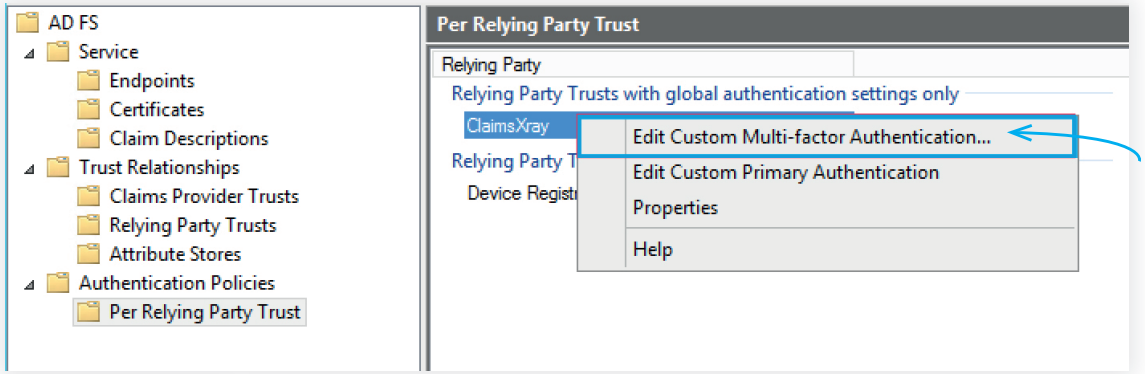
Go to Authentication Policies and click on **Edit Global MFA.**

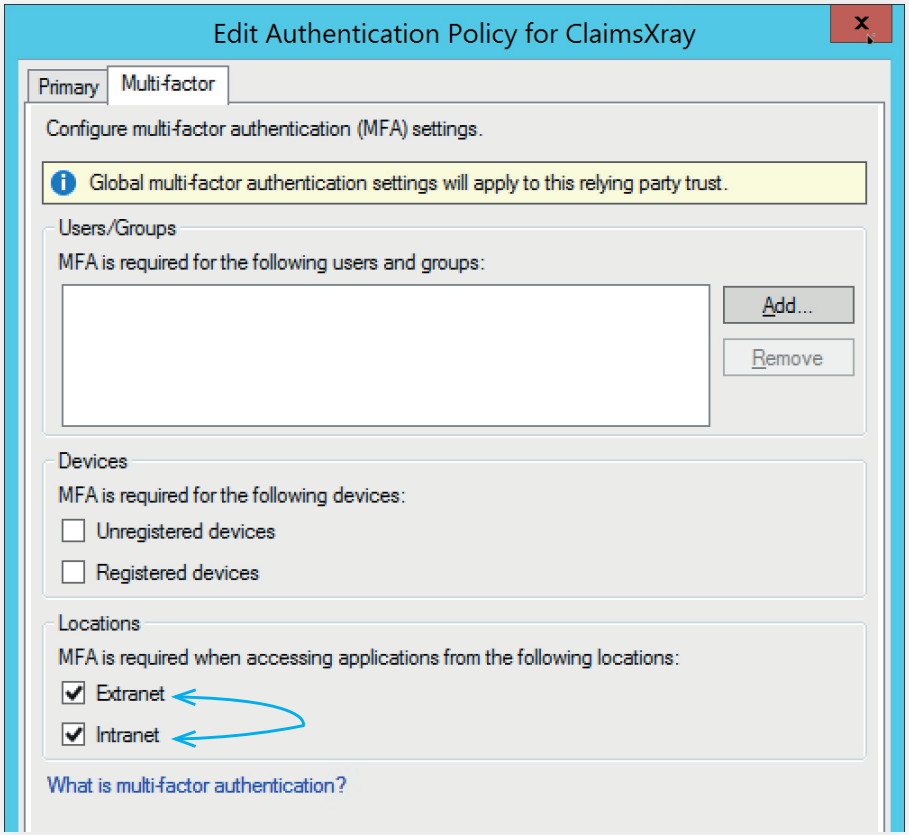




Here select **Ironchip MFA Adapter** as desired Multi Factor Authentication Method.

After that, we must enable the Multi Factor Authentication for an specific service, in this example we will require MFA for ClaimsXRay access. Go to per relying party trust and right click on service to protect. Click on **edit custom multi-factor authentication.**

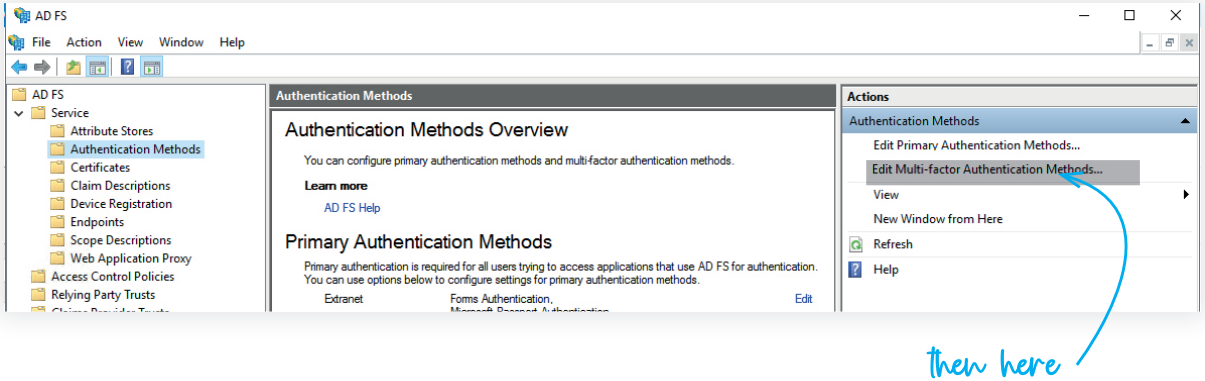


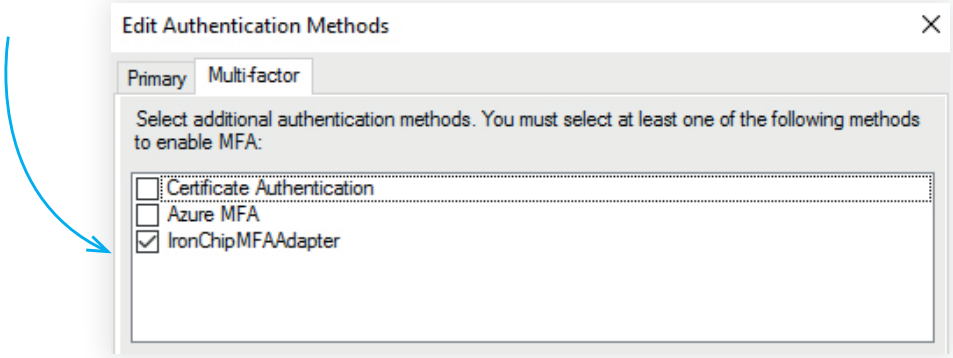


Enable MFA for **intranet**, **extranet** or both.

ADFS 4.0 Configure Ironchip Mfa for a relying party trust

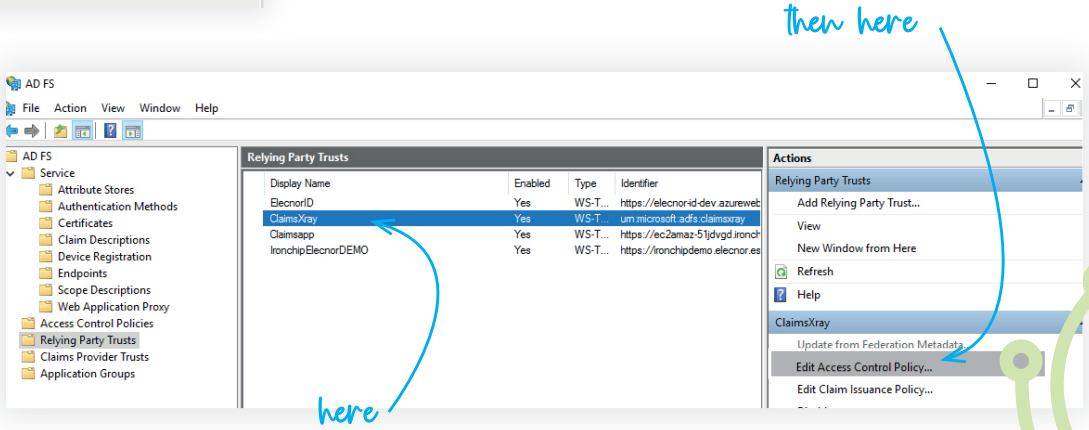
Go to Service > **Authentication Methods**. Here go to the right menu and click over **Edit Multi-Factor Authentication Methods.**



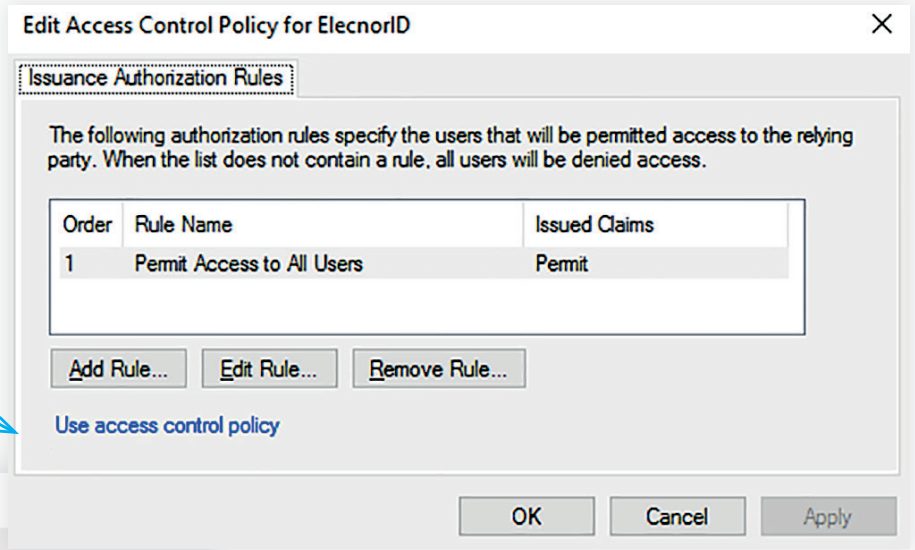


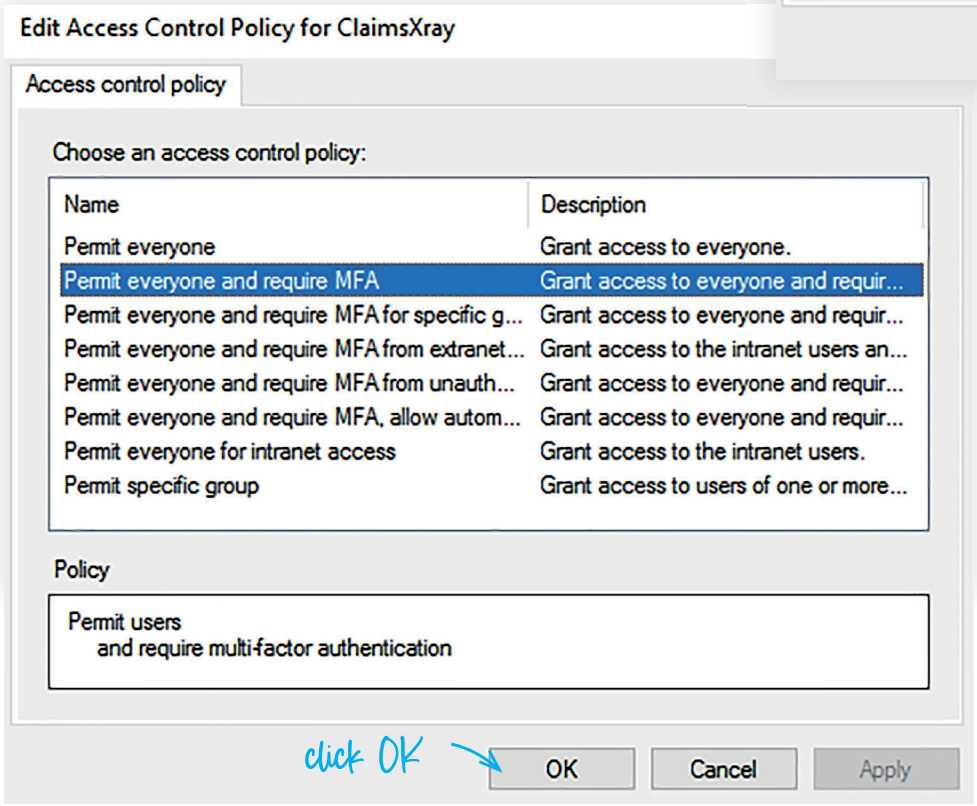
In Multi-factor tab, select Ironchip **MFA Adapter.**

Apply and Ok. After that, go to Relying Party Trusts and select **ClaimsXray service**. On right menu, click over **Edit Access Control Policy**.



In the opened window, in the bottom, you will see **use access control policy**. Click on it.





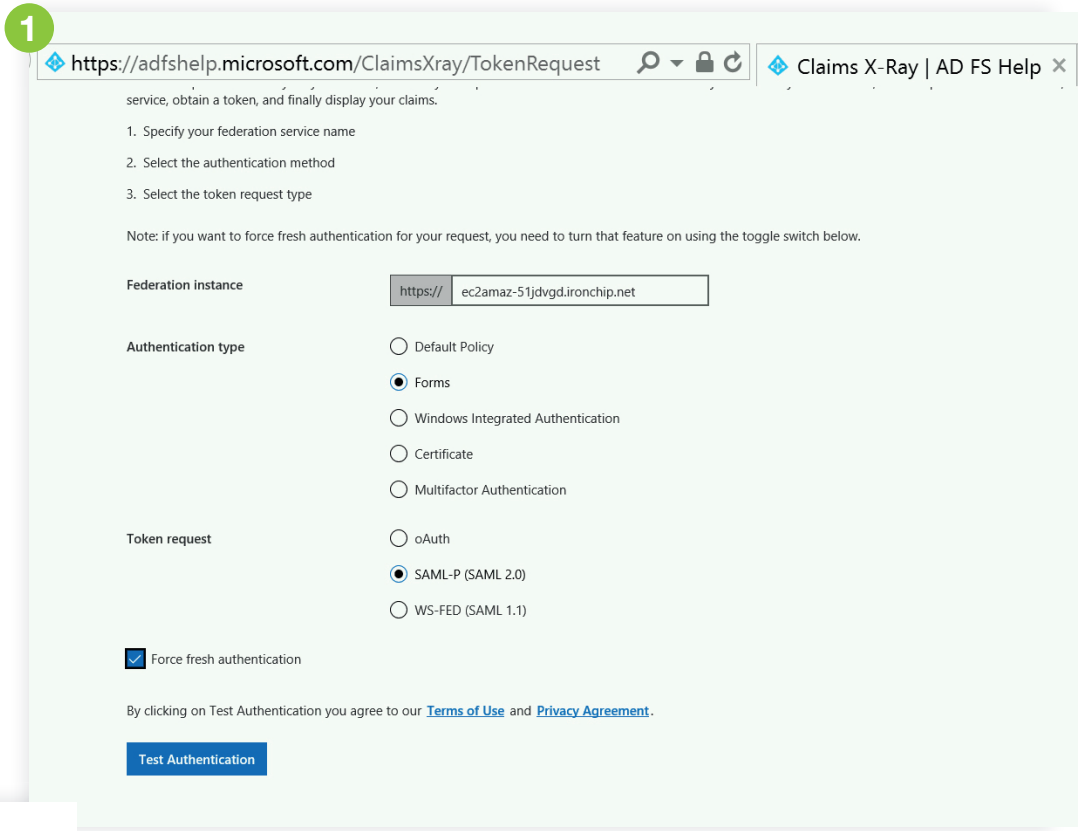
In prompted windows, select **permit everyone and require MFA**. You can apply this configuration only to an specific user group if you want.

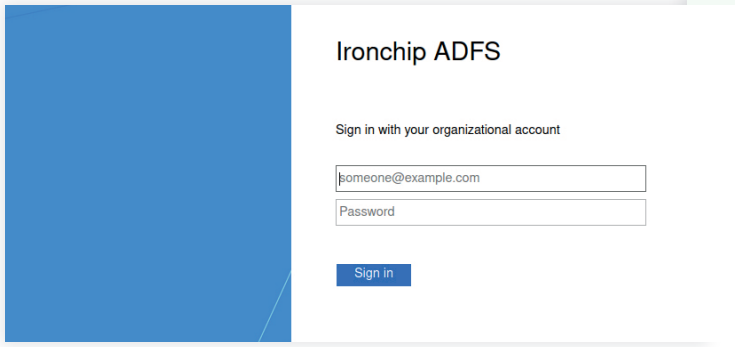
Apply and **Ok**. Now this service is protected with Ironchip MFA.

Test the plugin

You can use the Claims X-Ray tool to test Ironchip MFA. Configure it as you can see in next image 1 .

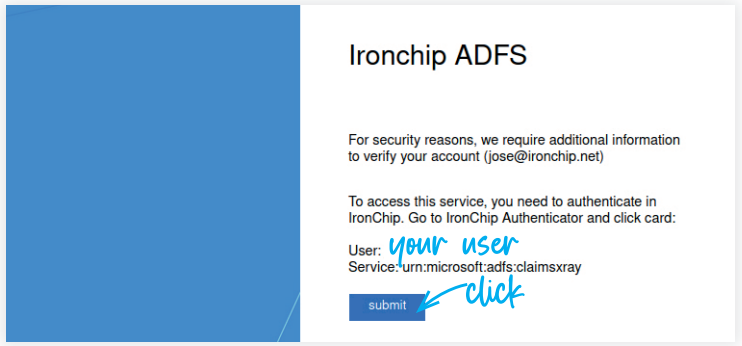
When you click on **Test Authentication**, you will be redirected to your ADFS.



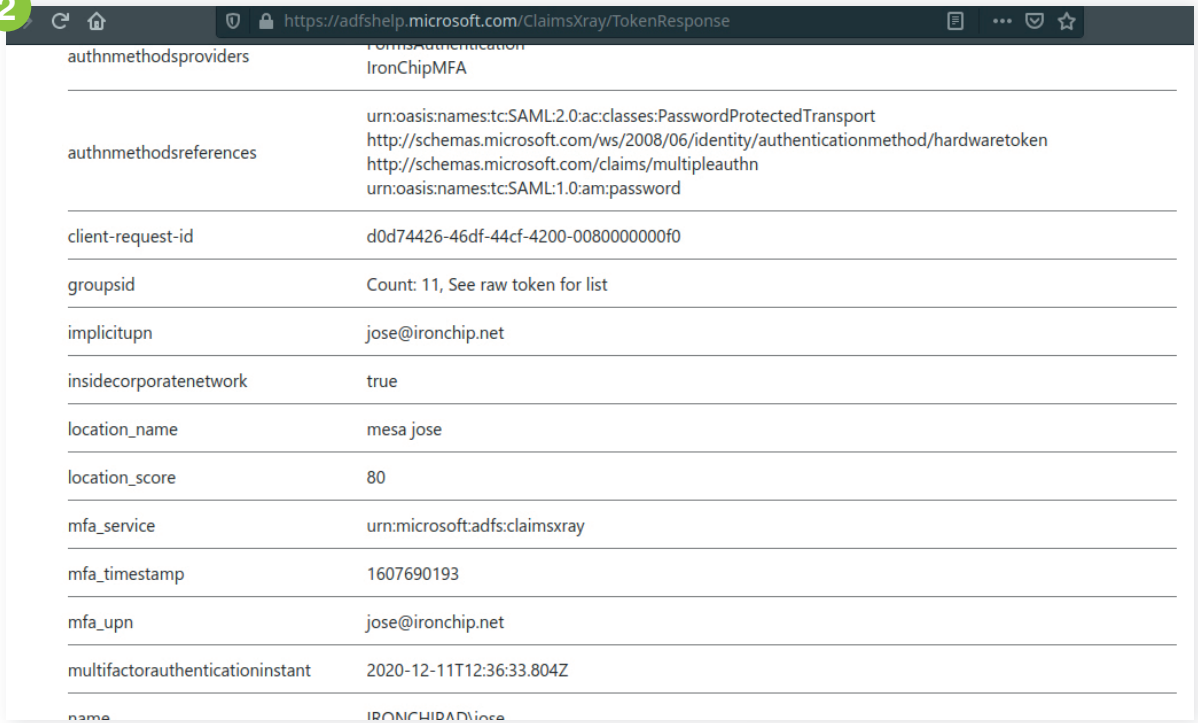


First, introduce your user and password.

After that you will be prompted to require **MFA.** Click on **submit**. You will recive a **push notification** in application to authenticate using Ironchip Authenticator (mobile app). Click on push and **authenticate**.



2



authnmethodsproviders	IronChipMFA
authnmethodsreferences	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/hardwaretoken http://schemas.microsoft.com/claims/multipleauthn urn:oasis:names:tc:SAML:1.0:am:password
client-request-id	d0d74426-46df-44cf-4200-0080000000f0
groupsid	Count: 11, See raw token for list
implicitupn	jose@ironchip.net
insidecorporatenetwork	true
location_name	mesa jose
location_score	80
mfa_service	urn:microsoft:adfs:claimsxray
mfa_timestamp	1607690193
mfa_upn	jose@ironchip.net
multifactorauthenticationinstant	2020-12-11T12:36:33.804Z
name	IRONCHIPAD\jose

If everything is Ok you will be redirected to this final page 2 .

Error FAQ's

"User XXX is not authenticated in service XXX. Please, try again."

The user is not authenticated, or authentication has not been valid. Just try again authentication in same page.

"Authentication protocol used is not compatible. Contact IronChip support providing error printed in EventViewer."

If this error is prompted when authenticating a user, the service provider is misconfigured and is not sending the service in the authentication request. If you see this error, contact IronChip support mail, info@ironchip.net, providing error log printed in Event Viewer IronChip MFA logs.

"Unable to load IronChip license key. Check that it is the correct license and try again. If problem persist contact IronChip support for help."

This error means that the license format is not valid. Please, contact info@ironchip.net with the error, and we will validate the license key used and provide a valid one if not valid.

"The API-Key provided is not valid. Please, contact IronChip support and send logs for assistance."

This error means that the license has the correct format, but is old or invalid. Please, contact info@ironchip.net with the error, and we will validate the license key used and provide a valid one if not valid.

"Ironchip has failed. Sorry. Contact support to allow us to solve the problem."

This error means that some strange thing has happened. If you see this error, contact IronChip support mail, info@ironchip.net, providing error log printed in Event Viewer IronChip MFA logs.