# Integrations installation guide

MFA Plugin for NPS

MFA Plugin for ADFS

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

Add MFA integration in Dashboard

• Add service in dashboard

Uninstall the plugin

Configure Claims Xrav

Uninstall the plugin

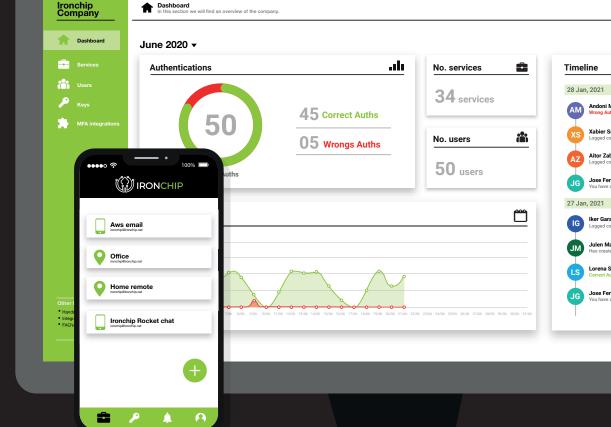
Error FAQ's

Install the plugin

Test the plugin

• Install the plugin

• Test the plugin



#### 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 RA-DIUS 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.



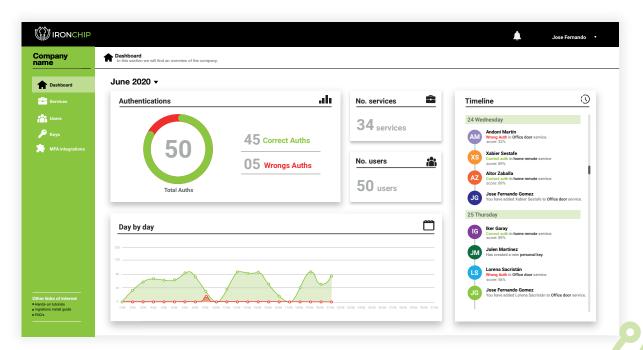
## **MFA Plugin for NPS**

#### 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.



						ل الم	e Fernando
ompany	Services Services management. You can creat	e services, add users in the services, explore your serv	ices				
Dashboard	Service list	click here				Service brief	
	+ New service		Q. Find se	rvice		ironchip	
Vsers Keys MFA integrations	Service	Type of service	Integration	Remove	Add users	January 2021 👻	
MFA integrations	Ironchip	Personal device	OIDC O	ŵ	+ Add User		_
	Home remote	Safe zone	API KEY 🛛	ŵ	+ Add User	No. of users	5
						Authentications	
						67	
						67	
						Month correct auths	42
							25
						Month wrong auths	25

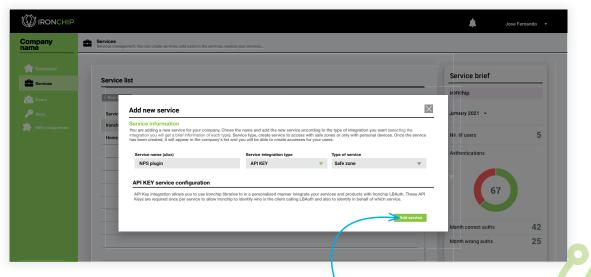
Go to the services section of your dashboard and click on New service to start.

#### We have next fields:

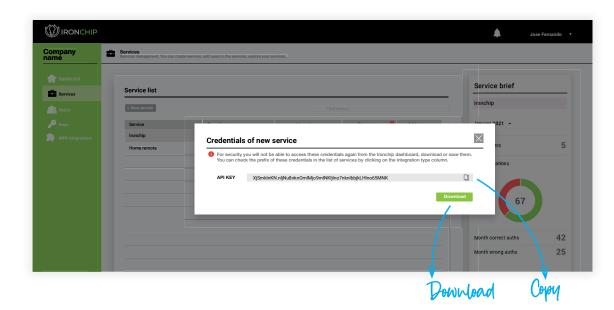
**Service name (alias):** Should be declarative for service we are adding.

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.



Click add service to add



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 co-lumn** in the future when you need it.

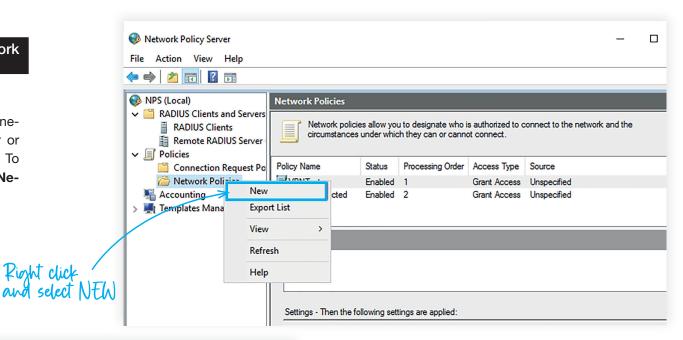
Once the service is added,	it will appear in
your list of services.	

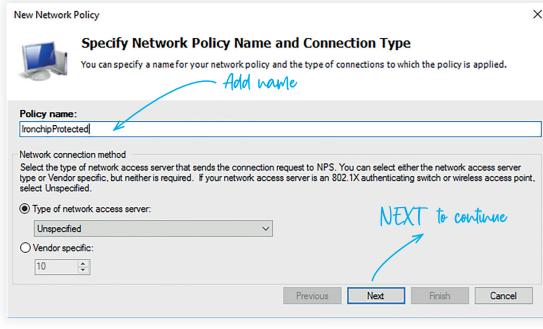
You will be able to have metrics of user interaction with this service by accessing to the service by clicking on the name in that list. To add users to this service refer to the applications manual linked in dashboard> other links of interest> Hands on tutorials.

Ame     >> Oericles instagement, fou car create services, add cars in the services, explore you services.       Ame     Service list       Service     • New service       > Keys     Service       Service     Type of service       Integration     Remove       Add users						
Service     Service list            Service            C	Company name	Services Services management. You can create s	services, add users in the services, explore your services	han .		
Service     Type of service     Integration     Remove     Add users       Settings     Ironchip     Personal device     OIDC     Image: Control of the control of th		Sarvico list				
Settings Ironchip Dersonal device OIDC 💼 + Add User					Q. Find user	
· · · · · · · · · · · · · · · · · · ·	🔑 Keys	Service	Type of service	Integration	Remove 🕕	Add users
NPS Plugin Specific location APIKEY 📆 + Add User	Settings	Ironchip	Personal device	OIDC	ŵ	+ Add User
		NPS Plugin	Specific location	APIKEY	ŵ	+ Add User

# 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**.





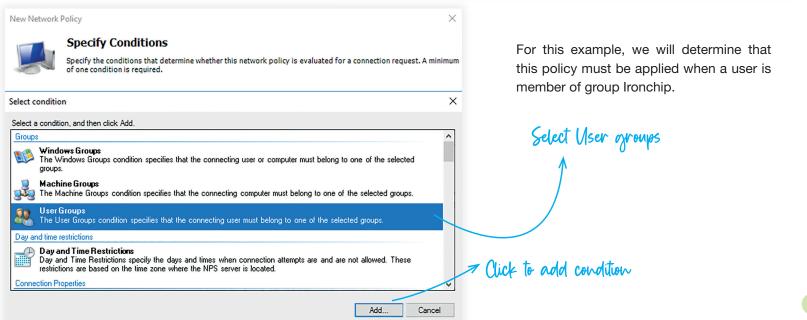
#### Provide a name to the policy.

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



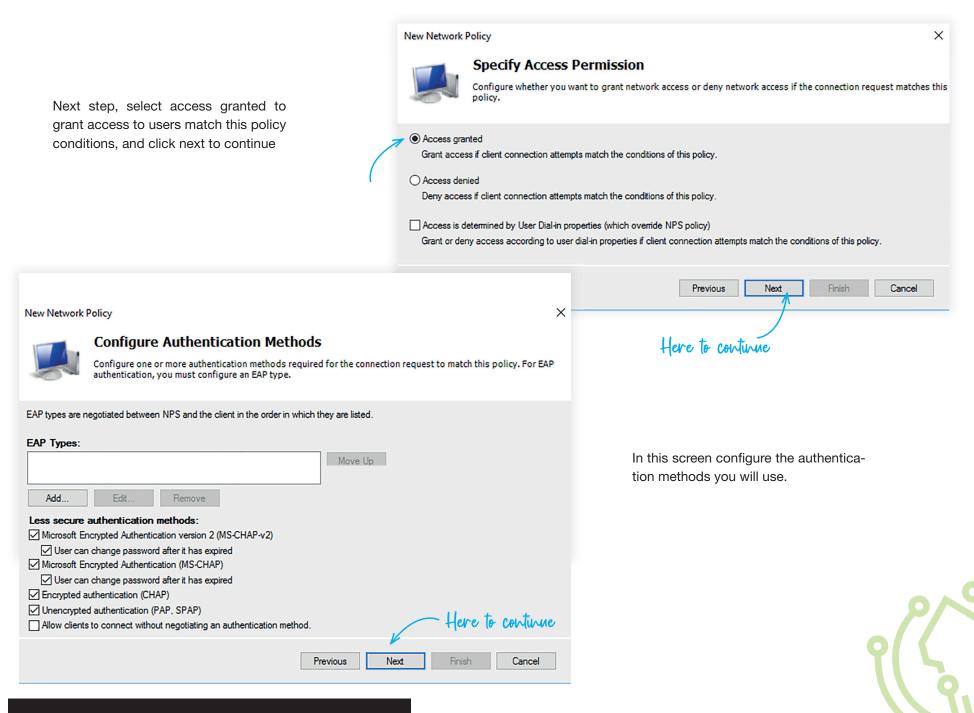
Here you can add all the conditions you want to determine for who and when will be applied this policy.

New Network	Policy						×
	Specify the	r Conditions conditions that determ dition is required.	ine whether th	is network poli	cy is evaluated fo	r a connection re	quest. A minimu
Conditions:	1	Value					
		Click here	to add	condition	NS		1
Condition desc	iption:				Add	Edit	Remove
				Previous	Next	Finish	Cancel





When you press add a new screen will appear, follow the steps below to proceed with the configuration.	Specify the group membership required to match this policy. Groups Add Groups Remove OK Cancel	Select Group Select this object type: Group From this location: ironchip net Enter the object name to select (examples): Ironchip Write here the name of the group Advanced OK	X Object Types Locations Check Names
New Network Policy	×	Click here to continue	
Specify Conditions	this network policy is evaluated for a connection request. A minimum	m Once added and configured you next result. Click next to continue.	
User Groups IRONCHIPAD\Ironchip	belong to one of the colorid groups	next result. Click hext to continue.	
The User Groups condition specifies that the connecting user must	Add Edit Remove	Here to continue	
Ironchip integrations installation guide			(Jil)



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.

#### New Network Policy

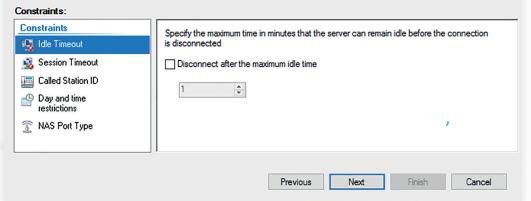


#### Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

#### Configure the constraints for this network policy.

If all constraints are not matched by the connection request, network access is denied.



#### New Network Policy



#### **Configure Settings**

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy ar matched.

Configure the settings for this network policy.

If conditions and constraints match the connection request and the policy grants access, settings are applied.

s				

RADIUS Attributes	then click Edit. If you	tributes to RADIUS clients, select a RADIUS standard attribute, and do not configure an attribute, it is not sent to RADIUS clients. See locumentation for required attributes.	
🗾 Vendor Specific	your habitus cient c	ocumentation for required attributes.	
Routing and Remote Access			
💑 Multilink and	Attributes:		
Bandwidth Allocation Protocol (BAP)	Name	Value	
TP Filters	Framed-Protocol	PPP	
	Service-Type	Framed	
Encryption	[ ]		
🦂 IP Settings			
	Add	Edit Remove	
	1	Previous Next Finish Cancel	

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



X

				×		
A summary of the configuration will appear. Check that everything is OK and		New Network Policy Completing New Network Policy				
click "Finish".		You have successfully created IronchipProtected	the following network policy:			
		Policy conditions:				
		Condition Value				
		User Groups IRONCHIPAD	Ironchip			
		Policy settings:				
		Condition	Value	^		
		Authentication Method Access Permission Framed-Protocol Service-Type Ignore User Dial-In Properties BAP Percentage of Capacity	Unencrypted authentication (PAP, SPAP) OR Encryption authentication (CHAP) OR MS-CHAP v1 Grant Access PPP Framed False Reduce Multilink if server reaches 50% for 2 minutes	~		
Network Policy Server		To close this wizard, click Finish	ı			
File Action View Help			Previous Next Finish Cancel			
🔶 🏟 🖄 💼 🛛 🖬			<i>n</i> .			
<ul> <li>NPS (Local)</li> <li>RADIUS Clients and Servers</li> <li>RADIUS Clients</li> <li>Remote RADIUS Server</li> <li>Policies</li> <li>Connection Request Po</li> <li>Network Policies</li> <li>Accounting</li> <li>Templates Management</li> </ul>	Network Policies           Image: Network policies allow you to designate who is authorized to connect to the network circumstances under which they can or cannot connect.           Policy Name         Status           Policy Name         Status           Processing Order         Access Type           Source         Image: Status           Policy Name         Enabled           Image: VPNTest         Enabled           Image: VPNnoprotected         Enabled           Image: Imag	rk and the	Click here th finish. You are ready to install the phozin			
	VPNTest					
	Settings - Then the following settings are applied:           Setting         Value           Extensible Authentication Protocol Configured Ignore User Dial-In Properties         True	^	You have added your network policie and everything is ready for install the plugin.			
< >>	Access Pemission Grant Access	× × ×				



Ironchip integrations installation guide

<

#### Install the plugin

To install the plugin, you need the zip file lronchip\_MFA\_ ADFS\_Plugin, which you can download from:

B

https://www.lronchip.net/pluginslronchip-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.

twork Policies					
		u to designate who th they can or cann		connect to the netwo	rk and the
licy Name	Status	Processing Order	Access Type	Source	
VPNTest	Enabled	1	Grant Access	Unspecified	
VPNnoprotected	Enabled	2	Grant Access	Unspecified	_
Ironchip Protected	Enabled	3	Grant Access	Unspecified	
VPNTest					
VPNTest Settings - Then the fo	ollowing sett	ings are applied:			
	ollowing sett		Value		
Settings - Then the fi					
Settings - Then the for	cation Proto	col Configuration			
Settings - Then the for Setting Extensible Authentii Ignore User Dial-In Access Permission	cation Proto	col Configuration	Configured		
Settings - Then the fr Setting Extensible Authentii Ignore User Dial-In	cation Proto	col Configuration	Configured True		



"host": "dev.api.Ironchip.com",

"apiKey": "vlBN03.WM2AbQoqM2BSbED1T1Up aZA050tqCrbSQBMqb2qRhrVLWzzQg",

"protectedpolicyname":"IronchipProtected"

}



# 3

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:

Your plugin is already installed. Now test the plugin!

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

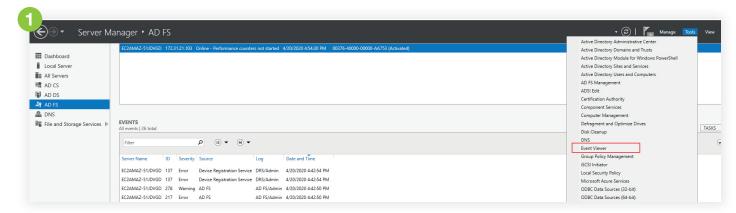


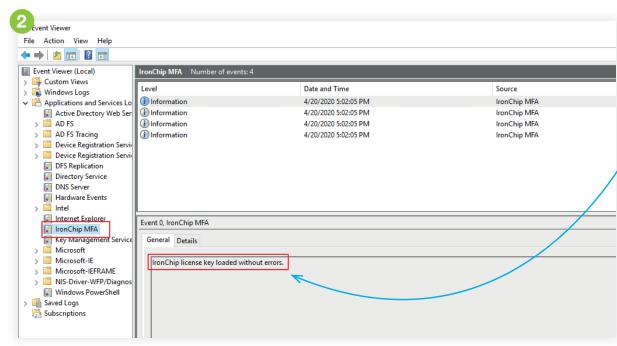
#### **MFA Plugin for NPS**

#### Test the plugin

1 Access Event Viewer to see Ironchip MFA

Plugin logs.





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:

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:

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 <sup>3</sup>

# 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" }

<b>A</b>		AD FS		
<ul> <li>§ File Action View Window Help</li> <li>← ➡ 2 III II III</li> </ul>				
<ul> <li>AD FS</li> <li>✓ Service</li> <li>Endpoints</li> <li>Certificates</li> <li>Claim Descriptions</li> <li>✓ Trust Relationships</li> <li>Claims Provider Trusts</li> <li>Claims Provider Trusts</li> <li>Attribute Stores</li> </ul>	Relying Party Trusts           Display Name           Device Registration Service           ClaimsXrav	Enabled Yes Yes	Type WS-Trust / S WS-Trust / S	Identifier um:ms-drs:der ao 3 um:microsoft uts:d

#### Test X-Ray

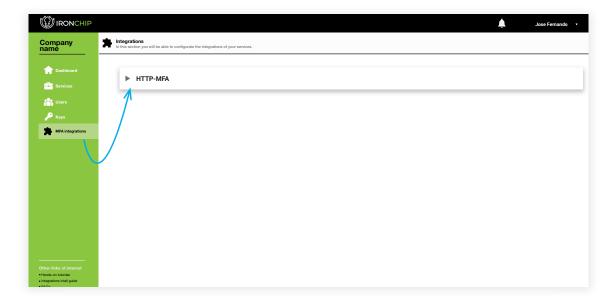
You can use the tool to test adfs. After that, configure it as you can see in next image 1:

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

	obtain a token, and finally disp	n/ClaimsXray/TokenRequest
1. Spec	tify your federation service name	
2. Selec	ct the authentication method	
3. Selec	ct the token request type	
Note: if	you want to force fresh authen	tication for your request, you need to turn that feature on using the toggle switch below.
Federat	tion instance	https:// ec2amaz-51jdvgd.ironchip.net
Authen	tication type	O Default Policy
		Forms
		O Windows Integrated Authentication
		O Certificate
		O Multifactor Authentication
Token r	request	O oAuth
		● SAML-P (SAML 2.0)
		O WS-FED (SAML 1.1)
V For	ce fresh authentication	
By click	ing on Test Authentication you	agree to our Terms of Use and Privacy Agreement.
cy ener		
	Authentication	

# Add ADFS as Multifactor Authentication in Ironchip Dashboard

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



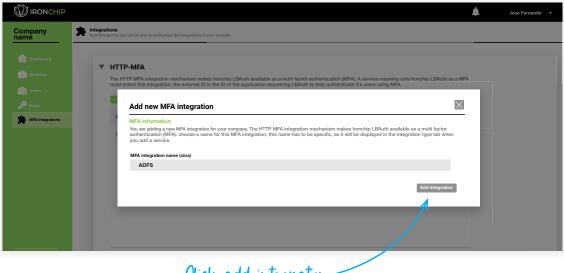
# , Click here to add

					Jose Fernando 🔹
Company name	from th	rations his section you will be able to co	infigurate the integrations of your services.		
n Dashboard		HTTP-MFA			
Services		The HTTP MFA integ	ration mechanism makes Ironchip LBAuth available as a gration. the external ID is the ID of the application reques	multi factor authentication (MFA). A service requiring only Ironchip ting LBAuth to help authenticate it's users using MFA.	p LBAuth as a MFA
🗥 Users 🔎 Keys		+ New integration			
MFA integrations		Name	Hint	Remove	0
		prueba	UWlgvd	i.	
Hands-on tutorials					

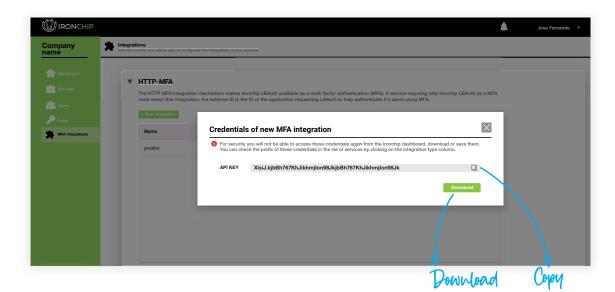
Click on **new integration**, and a new tab will be displayed so that you can add the new integration in your company.



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



Click add integration.



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 co-lumn** 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:

B

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 /down-loaded from the dashboard) in the apiKey value, inside double-quotes, as you can see in this example **1**.

"host": "testing.api.Ironchip.com",

"apiKey":"Shu2Zo.ORG0UlbkEnci3wwuhNkBt1kVX48jK6ntwX5NN0ZI0JBp2fuK7yaQ-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.

<sup>2</sup> The script will prompt the results in a Power-Shell 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 \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ v4.0.30319 C:\Windows\Microsoft.Net\assembly\GAC 64\ True 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 registered 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 pluzin is now installed

#### Test the plugin

• Access Event Viewer to see Ironchip MFA Plugin logs.

		Active Directory Administrative Center
	EC2AMAZ-51JDVGD 172.31.21.103 Online - Performance counters not started 4/20/2020 4:54:30 PM 00376-40000-00000-AA753 (Activated)	Active Directory Domains and Trusts
Dashboard		Active Directory Module for Windows PowerShell
Local Server		Active Directory Sites and Services
All Servers		Active Directory Users and Computers
AD CS		AD FS Management
AD DS		ADSI Edit
ND FS		Certification Authority
ONS		Component Services Computer Management
File and Storage Services 👂	EVENTS	Defragment and Optimize Drives
ile and storage services P	All events   26 total	Disk Cleanup
	Filter P (II) • (R) •	DNS
	Hiter P (III + H) +	Event Viewer
	Server Name ID Severity Source Log Date and Time	Group Policy Management
		iSCSI Initiator
	EC2AMAZ-51JDVGD 137 Error Device Registration Service DRS/Admin 4/20/2020 4:42:54 PM	Local Security Policy
	EC2AMAZ-51JDVGD 137 Error Device Registration Service DRS/Admin 4/20/2020 4/42/54 PM	Microsoft Azure Services

🗢 🏟 🞽 🖬 🚺 🖬			
🛃 Event Viewer (Local)	IronChip MFA Number of events:	4	
> 📑 Custom Views	Level	Date and Time	Source
<ul> <li>Windows Logs</li> <li>Applications and Services L</li> </ul>		4/20/2020 5:02:05 PM	IronChip
Active Directory Web Se	r i) Information	4/20/2020 5:02:05 PM	IronChip
> A AD FS	(i) Information	4/20/2020 5:02:05 PM	IronChip
> AD FS Tracing	(i) Information	4/20/2020 5:02:05 PM	IronChip
> Device Registration Service		, 20, 2020 5102105 1 111	
> 📋 Device Registration Serv			
DFS Replication			
Directory Service			
DNS Server			
Hardware Events			
> 📔 Intel	I		
Internet Explorer	Event 0, IronChip MFA		
IronChip MFA			
Key Management Servic	General Details		
> Microsoft-IF	In the Chie Research we have been done in	L	
Microsoft-IEFRAME	IronChip license key loaded wit	nout errors.	
> NIS-Driver-WFP/Diagno	s		
Windows PowerShell			
> 🛱 Saved Logs			

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:

<sup>3</sup> If you see the message "Unable to load Iron-Chip 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.



# 1

#### 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:

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 Files\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.

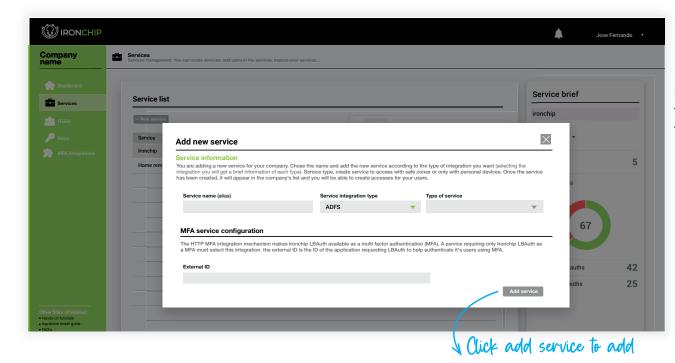
Removed IronchipMFA from AD FS server YOUR-MACHINE-NAME

#### 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.

						Jos	e Fernando
Company name	Services Services management. You can crea	ite services, add users in the services, explore your servi	ces				
Dashboard	Service list					Service brief	
tusers	+ New service	click here	Q. Find se	rvice		ironchip	
📸 Users 🔎 Keys	Service	Type of service	Integration	Remove 🕕	Add users	January 2021 👻	
MFA integrations	Ironchip	Personal device	OIDC O	Ŵ	+ Add User		_
	Home remote	Safe zone	API KEY 🛛	ŵ	+ Add User	No. of users	5
						Authentications	
						67	
						Month correct auths	42



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

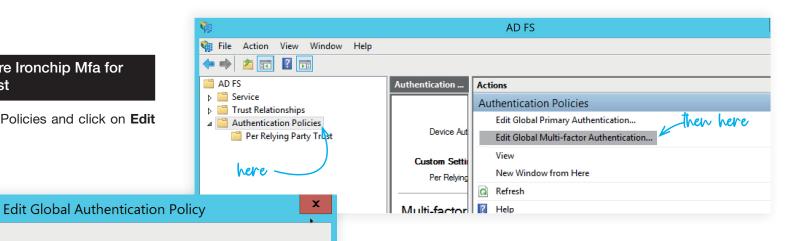
-External Id: must match with ADFS identifier

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.



Configure multi-factor authentication (MFA) settings. Users/Groups

MFA is required for the following users and groups:

Devices MFA is required for the following devices: Unregistered devices Registered devices Locations MFA is required when accessing applications from the following locations:

Extranet

Primary Multi-factor

Intranet

Select additional authentication methods. You must select at least one of the following methods to enable MFA:

<u>A</u>dd... Remove

Certificate Authentication here IronChipMFAAdapter

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.** 

📔 AD FS
⊿ 🧮 Service
Endpoints
Certificates
📔 Claim Descriptions
⊿ 📔 Trust Relationships
📔 Claims Provider Trusts
📔 Relying Party Trusts
📔 Attribute Stores
Authentication Policies
📔 Per Relying Party Trust

 Per Relying Party Trust

 Relying Party

 Relying Party Trusts with global authentication settings only

 ClaimsXray
 Edit Custom Multi-factor Authentication...

 Relying Party T
 Edit Custom Primary Authentication

 Device Regist
 Properties

 Help

Edit Authentication Policy for ClaimsXray
Primary Multi-factor
Configure multifactor authentication (MFA) settings.
Global multi-factor authentication settings will apply to this relying party trust.
Users/Groups MFA is required for the following users and groups:
Add <u>R</u> emove
MFA is required for the following devices: Unregistered devices
Registered devices
Locations MFA is required when accessing applications from the following locations: Extranet Intranet
What is 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.

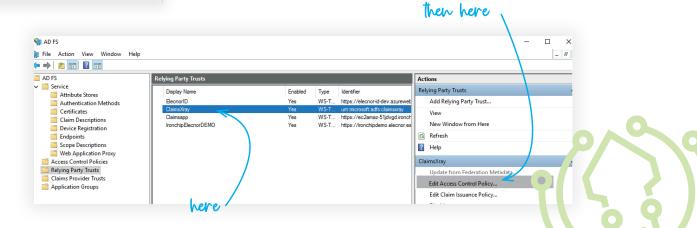
Image: Second		- C ×
🛗 AD FS	Authentication Methods	Actions
✓ I Service I Attribute Stores	Authentication Methods Overview	Authentication Methods
Authentication Methods Certificates	You can configure primary authentication methods and multi-factor authentication methods.	Edit Primary Authentication Methods Edit Multi-factor Authentication Methods
Claim Descriptions Device Registration Endpoints	Learn more AD FS Help	View New Window from Here
Scope Descriptions Web Application Proxy Access Control Policies	Primary Authentication Methods Primary authentication is required for all users trying to access applications that use AD FS for authentication. You can use options below to configure settings for primary authentication methods.	Refresh     Help
Relying Party Trusts	Extranet Forms Authentication, Edit	I

then here /

Primary       Multi-factor         Select additional authentication methods. You must select at least one of the following methods to enable MFA:         Certificate Authentication         Azure MFA         IronChip/MFAAdapter
to enable MFA:
Azure MFA

Iti-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.



X Edit Access Control Policy for ElecnorID Issuance Authorization Rules The following authorization rules specify the users that will be permitted access to the relying party. When the list does not contain a rule, all users will be denied access. In the opened window, in the bottom, you will Order Rule Name Issued Claims Permit Access to All Users Permit 1 Add Rule ... Remove Rule ... Edit Rule ... Use access control policy Edit Access Control Policy for ClaimsXray OK Cancel Apply Access control policy Choose an access control policy:

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

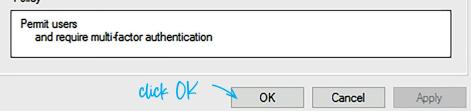
Apply and **Ok**. Now this service is protected with Ironchip MFA.



# see use access control policy. Click on it.

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and requir
Permit everyone and require MFA for specific g	Grant access to everyone and requir
Permit everyone and require MFA from extranet	Grant access to the intranet users an
Permit everyone and require MFA from unauth	Grant access to everyone and requir
Permit everyone and require MFA, allow autom	Grant access to everyone and requir
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more

#### Policy



#### 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.

service, obtain a token, and fina	.com/ClaimsXray/TokenRequest
1. Specify your federation servi	ce name
2. Select the authentication me	thod
3. Select the token request type	2
Note: if you want to force fresh	authentication for your request, you need to turn that feature on using the toggle switch below.
Federation instance	https:// ec2amaz-51jdvgd.ironchip.net
Authentication type	O Default Policy
	• Forms
	O Windows Integrated Authentication
	○ Certificate
	O Multifactor Authentication
Token request	O oAuth
	SAML-P (SAML 2.0)
	O WS-FED (SAML 1.1)
Force fresh authentication	
By clicking on Test Authenticati	on you agree to our <u>Terms of Use</u> and <u>Privacy Agreement</u> .
Test Authentication	

Sign in with your organizational account
someone@example.com
Password
Sign in

Ironchip 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**.

# Ironchip ADFS For security reasons, we require additional information to verify your account (jose@ironchip.net) To access this service, you need to authenticate in fonchip. Go to fonchip Authenticator and click cards. User: GeW USEH Service: unimicrosoft;adfs:claimsxray. submit Justice

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-4200-008000000f0	
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	

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 Iron-Chip support mail, info@ironchip.net, providing error log printed in Event Viewer Iron-Chip MFA logs.





Todos los derechos reservados. La propiedad de las imágenes y contenidos de esta documento corresponden a Ironchip Telco SL.