What to tell service providers

The first thing to do is check whether the resources you want to access are available in the same federation(s) that you are in as this will vastly simplify things for you and them. If they are not, there are still options though.

If they are in the same federation as you

All you basically need to do is give them your entityID and scope details, and find our which attributes they need you to pass. Usually they do not need anything that you are not allready set up to pass, but sometimes they do. it is also worth asking them at this time about wayfless URLs so that you can most easily set up access for your users.

> I would like to access my subscription using federated access management [in addition to]/[instead of] my existing methods. I see we are both members of [federation].
>
> My entityID and scope are:
>
> entityID: https://idp.yourdomain.com/oala/metadata
>
> scope: yourdomain.com
>
> Please confirm which attributes you need me to release for authorisation, and any others that may enhance the user experience. Please also define your wayfless URL format including any deep linking facility.

If they are in one or more federations, but not the same ones as you

Unless their resource is very specialist it is likely that you will not be the only member of your federation that is interested in access. They will likely want to join your federation and gain access to more customers.

If they are not in a federation, but have a SAML login option

This usually applies only to internal connections such as your VLE, but can also come up for things like Adobe's Creative Cloud enterprise or Google's G Suite.

If the resource or app has published metadata, you can add it in the same way as any federation metadata via the administration console. If their metadata is not published, you must manually add it to the runtime, which is usually a job for your IT team.

It is not uncommon with this kind of resource or target that you will need configure some things on its side via an interface. Some will let you upload your metadata (which is the easiest method), but some will need you to manually specify some details.

Your metadata address will be something like "https://idp.yourdomain.com/oala/metadata". You can look it up on the overview tab in the runtime properties section:
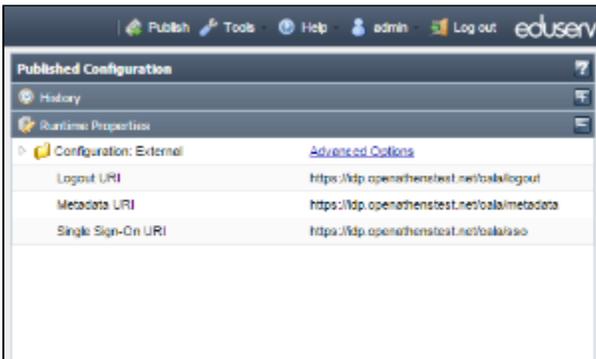
If they do not let you upload metadata, the things they might ask for include:

Item	Means	Use
SSO address	Where your users should be sent to log in	E.g. https://idp.yourdomain.com/oala/sso Can be looked up on the overview tab
Logout address	Where you users should be sent to log out	E.g. https://idp.yourdomain.com/oala/logout Can be looked up on the overview tab
Upload a signing certificate	The x509 certificate that would normally be read from your metadata	If they ask for this you will need to copy and paste some data from your metadata into a text file - see below

Specify SAML version	Use the one that came out in 2005 (SAML 2) or the older one.	SAML 2
Redirect or POST		Redirect

How to copy your certificate from your metadata

First download your metadata - the address is on the overview tab as above and will look something like "https://idp.yourdomain.com/oala/metadata". If your browser shows it in the window instead of downloading it, right click the window and select show source.

Open the downloaded file in a text reader such as notepad and look for the section that says x509:

Copy this to another file then top and tail it as follows:

```
-----BEGIN CERTIFICATE-----
MIIDXjCCAkagAwIBAgIIaKaKKRk6E6IwDQYJKoZIhvcNAQEFBQAwRjEjMCEGA1UE
CgwaVGVzdGluZyBuZXcgU0FNTCBjb25uZWN0b3IxHzAdBgNVBAMMFmlkcC5vcGVu
YXRoZW5zdGVzdC5uZXQwHhcNMTUxMDE5MTAxODQ1WhcNMjUxMDE5MTAxODQ1WjBG
MSMwIQYDVQQKDBpUZXN0aW5nIG5ldyBTQU1MIGNvbm5lY3RvcjEfMB0GA1UEAwwW
aWRwLm9wZW5hdGhlbnN0ZXN0Lm5ldDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAJ+H05q2dmGGYhGcHRCR1pz1PnzToVD341NwQleBgdtPluAkMnL+gAff
gEhUQxrdYpR/L6cLu0YoEHiKXRdvQGO8ZPb1nPqfsuX5Xt3DCN13HSGWQ5KlOjHp
PB/6xM7RNuylAMoApFmwzs3amY+4p3j2UYCXGkoXynPAeOLBTlvm1bHpkL5AzoSj
jCOlwMdmA7rLGXt/kZsX9KhwXw5WL+3ZZ2sfU4R4WviHrTkFhmeh2ol+/M/QxVdl
nPNk9+UKqRZmPGxJsQw3CcGPDkiKc43OEkkCLTUZk3Fyd6KA21+deBg1ERtUOXSP
u5rTPb2Z9d8NbC+8WMuHhlTCrsueZcUCAwEAAaNQME4wHQYDVR0OBBYEFOo9P32L
1bUJOUfJW4uRs6xvbNNhMB8GA1UdIwQYMBaAFOo9P32L1bUJOUfJW4uRs6xvbNNh
MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAEOD5HDFLpAw8FYQfHEV
J4PXmGzqxf13S6SpEQr5Fu4Q/1LnXJ30KCzYWgfAfcNe8hwCJOqXYNsjBKJdeYvc
P4LN1zrv62sc2yqeobdeZ8XuE+set0Fq7oAKmvojMQ9XqyF4MTYTzVNn7pd8Z7Ot
PJqTcKVbU30LGmWB99TeWIy/8fxD16YksJ8JjJKxvlAnDV7st+SSn7GIl0Gi40QA
wfOF2TgG4zvJvfilRZvjBgMyFSnNRFhOR8fuMQ+SBojQ2D3CdSQ+5tdP5l9HqADN
prdiPj+pI5lCSbQlTDYArrZMC6Y5H2b25vvSv1Z22TON38T0SttOFjnV8oobDCEG
IGY=
-----END CERTIFICATE-----
```

It usually doesn't matter what plain text format you save this in. Some apps may requre you to upload it as .cer file. Some may refer to it as a '.pem' file. If they do, it is still a plain text file just with a different extension. Some apps may just have a text box you paste it into.

If they are not using federated access management

In such cases, OpenAthens LA has a basic proxy server component that can be used - see Working with the proxy