Virtual Home

What is the Tuakiri Virtual Home?

Most users of Tuakiri belong to a Tuakiri subscriber organisation, are in the organisation’s identity management system, and can use that organisation’s identity provider to log into connected services. This is known as their Home Organisation. For example, NIWA is a Tuakiri subscriber. If I am a staff member of NIWA, I can log into Tuakiri-connected services using NIWA's identity provider, and NIWA is known as my Home Organisation.

However, in some cases it is desirable for users who don’t otherwise have an identity provider to be able to log into services via Tuakiri. Because they have no Home Organisation within the federation, these users can become part of the Tuakiri Virtual Home (VH).

The Tuakiri Virtual Home is an identity management system for individuals who need to access services via Tuakiri, but who do not have an account with a Tuakiri identity provider.

Who can have an account in the VH?

The VH can be used in the following cases:

1. Your organisation has joined Tuakiri but doesn’t have an identity provider (IdP) yet. There may be a few users who need to access services now, before you have a chance to get your IdP up and running. You can add these users to the VH.
2. Your organisation has joined Tuakiri but has only a small number of users and does not intend to run an IdP. You can add your users to the VH. This case includes service providers who need to access the Federation Registry or to test access to their own services.
3. Your organisation has joined Tuakiri and has its own IdP up and running. However, there are a few individuals who are not in your identity management system who need to access Tuakiri-connected services in order to collaborate with other users in your organisation. You can in effect sponsor these individuals and add them to the VH. This enables them to access Tuakiri-connected services without having an account in your identity management system.

If anyone can be in the VH, doesn’t that negate the trust in the federation?

No. In the cases above you will notice that an individual with an account in the VH is always sponsored by an organisation that has joined Tuakiri. This means the organisation is bound by the Federation Rules. By adding the individual to the VH, that organisation takes on the identity provider’s responsibilities with respect to that individual.

How is the VH organised?

Tuakiri participant organisations each have their own section in the VH where they manage their users. For every organisation that is created on the Tuakiri Federation Registry, a section is created on the VH automatically. This means that if your organisation runs an IdP and / or one or more SPs in Tuakiri, the VH carries a section for your organisation. If you would like to become a manager for your organisation's section, please send a request to support@tuakiri.ac.nz.

Who manages my organisation’s section of the VH?

When your organisation joins Tuakiri, they nominate an administrator who will manage their section of the VH. This person can then delegate the authority to others in your organisation. Subsections can also be added by their own administrators. You might want to do this, for example, if one of your university’s faculties or research centres needs to add users to the VH. You must request the addition of a subsection within your organisation’s section via a request to support@tuakiri.ac.nz.

What attributes can be populated about users in the VH?

The VH supports all of Tuakiri's core attributes. It is possible to have additional attributes added. Please contact support@tuakiri.ac.nz with information about the attribute name, URN, description, and an explanation of how it is expected to be used.

Will the users in my section of the VH appear to come from my organisation?

No. For these users the value of the schacHomeOrganization attribute will be virtualhome.tuakiri.ac.nz. It is however possible to change the value of this attribute for users in your section of the VH, adding a prefix corresponding to your organization (and possibly also another prefix corresponding to the user group). Please contact support@tuakiri.ac.nz if you would like to have this setting changed. Also, note that the value of the Organization Name attribute would be matching the (human readable) name of your organization as registered in the Federation Registry.

Does the VH handle group management?

No. In the grid community, the term virtual organisation means a group of users authorised to share a set of files and resources. This can create some confusion with the term Virtual Home. The VH is not used for group authorisation. It is simply a surrogate identity provider for users who don’t otherwise have one.

It sounds like I can use the VH as an alternative to running my own IdP. Is this a good idea?

Usually not. Using the VH in this way is only an option if you have a very small number of users who need to access Tuakiri-connected services. If you have your own user directory or identity management system and more than a few of these individuals need to access services, it will be better for you to run your own IdP. An important benefit of Tuakiri is that it allows the user’s credentials, issued by their home organisation, to be accepted in more places. Users in the VH miss out on this benefit because they will have an additional username and password to remember. You will also have additional overhead in provisioning, deprovisioning, and maintaining users in the VH. It will be easier for you if this information is automatically populated to your IdP from your internal user directory or identity management system.

What happens if I added a user to the VH and now I want to put them in my organisation’s own IdP?

There is currently no defined process or tools for this. Transferring a user and ensuring their continuity of service will vary from SP to SP. For SPs that use the auEduPersonSharedToken as a unique ID to identify their users, a transfer of the Shared Token will be required. The user’s Shared Token is visible within the VH administration tool. It needs to be imported into the organisation’s identity system on behalf of the user. For SPs that use the eduPersonTargetedID the user, when transferred, will look like a new user to the service.