GRANICUS

GOVSERVICE SUITE

| Search our Knowledge Articles | Search |

HOME (/S/)    CONTACT SUPPORT (/S/CONTACTSUPPORT)    SYSTEM STATUS (HTTPS://STATUS.GRANICUS.COM/)    MY SUPPORT CASES (/S/CASE/          )000045000004

Home
(https://support.granicus.com/s)
/   govService UK (https://support.granicus.com/s/article-group/a8C4A000000PIphUAG)
/   General (https://support.granicus.com/s/article-group/a8C4A0000008SjKUAU)

**FAM overview and setup (Federated Authentication Module)**

The FAM enables users of an Active Directory domain to use Firmstep cloud-based solutions without the need to use separate login credentials enabling single sign on

https://support.granicus.com/customersupport/s/article/fam-overview-and-setup-federated-authentication-module (https://support.granicus.com/customersupport/s/article/fam-overview-and-setup-federated-authentication-module)

https://granicus.my.salesforce.com/ka24A0000001ujc (https://granicus.my.salesforce.com/ka24A0000001ujc)

General (/s/article-group/a8C4A0000008SjKUAU/general)

ℹ
New Article

ℹ

ℹ

ℹ
govService Suite

ℹ

- Introduction
- Installation - Important key facts
- Installation - FAQs
- P

> Granicus Issue Notification:    ✕
> Some govAccess- Vision...
> Last updated 16 minutes ago
> View latest updates

**Introduction**

The FAM enables users of an Active Directory domain to use Firmstep cloud-based solutions without the need to use separate login credentials, enabling single sign on.

For example:

1. A user requests to login or access secured content on the Firmstep solution
2. The cloud redirects the user to the FAM which is on their local intranet.
3. The user authenticates with the FAM website - normally using pass-thru so there is no prompt to login
4. The FAM then redirects the user back to the cloud, with their encrypted credentials
5. The cloud then knows the user has been authenticated, and can show them the requested content.

All of the credential details sent from the FAM to the cloud is encrypted using AES256. This method of authentication is a standard - Security Assertion Markup Language (http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language).

## Installation - Important key facts

The FAM is typically installed by Firmstep consultants on a server prepared by the customer to meet these prerequisites:

- Windows Server OS (any version) that is a member of your domain
- IIS (any version)
- ASP.net (http://ASP.net) 3.5 (Features>.Net Framework 3.5 Features - install this AFTER IIS is installed)
- Windows Authentication role service for IIS
- To be able to authenticate users on your local domain(s). This may require a windows service account.

Once all of this is in place our consultants can complete the installation remotely while you watch using GotoMeeting, the process takes approximately one hour. This will involve downloading a ZIP file containing the software.

## What information do I need to provide to Firmstep before a FAM installation?

You need to confirm that the server is ready, so generally a yes/no to the following:

- IIS is installed.
- ASP.Net (http://ASP.Net) 3.5 is installed and enabled on IIS (Web Server> Application Development > ASP.NET (http://asp.net/) 3.5 and Features>.Net Framework 3.5 Features).
- FAM server is on the same domain as your users.
- Does the domain controller allow anonymous read-only LDAP queries?

 You will need to provide these details:

- URL that can access the FAM from the local network.
- Active Directory fully qualified domain name for LAN users.
- Active Directory search base for users (normally this is derived from the AD FQDN)
- Host name or IP for your domain controller.
- If the domain controller does not accept anonymous LDAP queries provide username/password for a service user that can run the LDAP query.

## Installation - FAQs

Q) Will the FAM work on a Virtual Machine?

Yes t    ▷  Granicus Issue Notification:        ✕
             Some govAccess- Vision...

Q) C     Last updated 16 minutes ago

         View latest updates

Yes,                                          a local intranet website. You will need to configure IIS (and/or your proxy) with the necessary
certificates if you want to use SSL.

Q) Can I cluster the FAM?

Yes, although it does a tiny amount of computation so this is not necessary for scalability. VM infrastructure normally provides sufficient fault tolerance, however the standard Network Load Balancing features of Windows will work just fine.

Q) How should I setup IIS Application pools / Virtual directories?

The FAM is normally installed with its own application pool and in a virtual directory called 'firmstepfam' which maps to program files\firmstep\fam. We will normally setup this for you.

Q) Does the FAM need a dedicated server?

No, it does a very small amount of computation

Q) Shall I put my FAM in the DMZ or on my LAN?

The LAN. It does not interact directly with the cloud system or anything on the internet, and it must be installed on a member server of your domain.

Q) What server specification is required?

The FAM does a tiny amount of computation and requires nothing more than the minimum recommended specifications quoted by Microsoft for your server OS.

Q) Does the FAM need to be backed up?

Not regularly. Backups need only be taken after installation or configuration changes.

Q) What information about my users does the FAM expose to the cloud

Their full name, windows login name, email address, and group memberships. You can limit the group memberships that are exposed in configuration.

Q) A FAM login involves browser redirects from cloud to FAM and back. What exactly are the steps and how does information flow between the systems involved?

The platform site passes a SAML request to the FAM. The FAM reads the request, runs an LDAP query against your AD, and returns a SAML response to the platform site. This all happens in the user's browser session, there is no direct connection between the FAM server on your network and the cloud.

This diagram should help illustrate the steps.
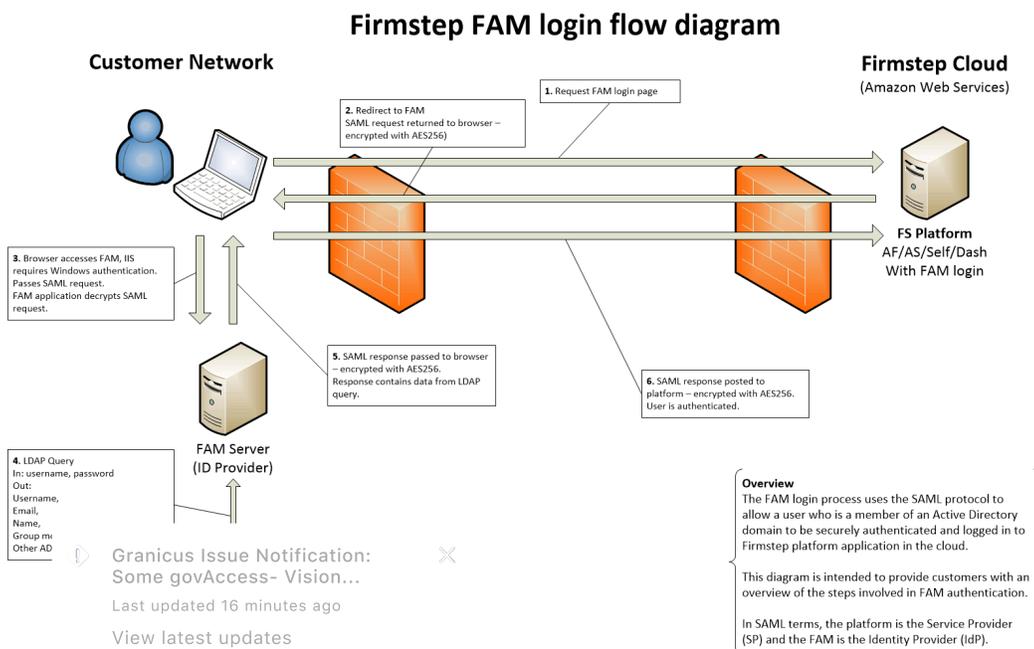


Q) Can I manage the permissions a user has in the Firmstep solution using AD group memberships

Yes. You can cut down on administration overhead of your Firmstep platform system by managing user permissions for your internal users in Active Directory. (/s/article/using-active-directory-groups-to-restrict-user-access)

Q) Can I get more info out of my Active Directory, such as phone numbers and line manager relationships?

Yes, but not using the FAM.

Q) Can I use multiple separate FAMs to allow the cloud to authenticate users on separate networks?

Yes. The easiest way to do this is to use DNS 'A' records to map a common hostname (e.g. http://firmstepfam.local (http://firmstepfam.local/)) to the appropriate FAM server. Do not use CNAME records – these can cause problems with the authentication. You will also need to ensure that the site is considered part of your local intranet for pass-through authentication to work.

Q) I don't use Windows domains. Can I write my own FAM to do authentication differently?

Sure, it's based on the SAML (http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language) standard and we can provide example C#.net code upon request.

---

## Preparation

1. Prepare a new server so that it meets the installation prerequisites as described above
2. Ensure the new LIM server can serve content to your internal users
3. Firmstep will then install and configure the latest FAM software over a gotomeeting session. You must have access to the desktops of both old and new FAM servers to facilitate this.
4. If you are running the LIM or FAM application with logging enabled, please ensure that appropriate measures are taken to ensure log files are not remotely accessible. The simplest way to do this is to ensure log files are stored in a location outside the IIS directory structure

## Switch

When you are ready, Firmstep consultants will update the configuration records of your platform sites to use the new FAM. The changes take effect immediately and there will be no downtime. The FAM installation on your old server is no longer in use and can be decommissioned.

body {<br /> font-size: 15px;<br /> line-height: 22px;<br /> }<br /> <br /> li {<br /> padding-bottom: 10px<br /> }<br />

Further useful reading:

- LIM Setup (/s/article/lim-overview-and-setup-local-integration-module)

- Information security (/s/article/information-security)

- Introduction to the platform (/s/article/firmstep-deployment)

Granicus Issue Notification:
Some govAccess- Vision...
Last updated 16 minutes ago
View latest updates

When a user logs in for the first time the system recognises that an account does not exists and creates one for them. However, when this occurs, the point where we check if the user has profile data has passed, therefore the FAM profile data is not read and added to the profile. The next time the user logs in, the account is then updated with profile data from the FAM.

•

Rebooting the FAM server will prevent authentication whist the restart takes place – but existing logged in users will be unaffected.

ℹ

ℹ

ℹ

ℹ

ℹ

CONTACT SUPPORT

## Article Feedback

Did this article help resolve your problem?

Yes    No

## Not finding what you need? Get in touch with us.

Submit a Ticket(/s/contactsupport)

OR CALL

(800) 314-0147 (US)
+44 (0) 800 032 7764 (Europe)

Granicus Issue Notification:
Some govAccess- Vision…
Last updated 16 minutes ago

View latest updates