FrameFlow

Security Best Practices Guide

Table of Contents

Steps to Secure your FrameFlow Installation

Introduction

Network and system security are now more important than ever. This document presents a series of best practices for the secure deployment of FrameFlow.

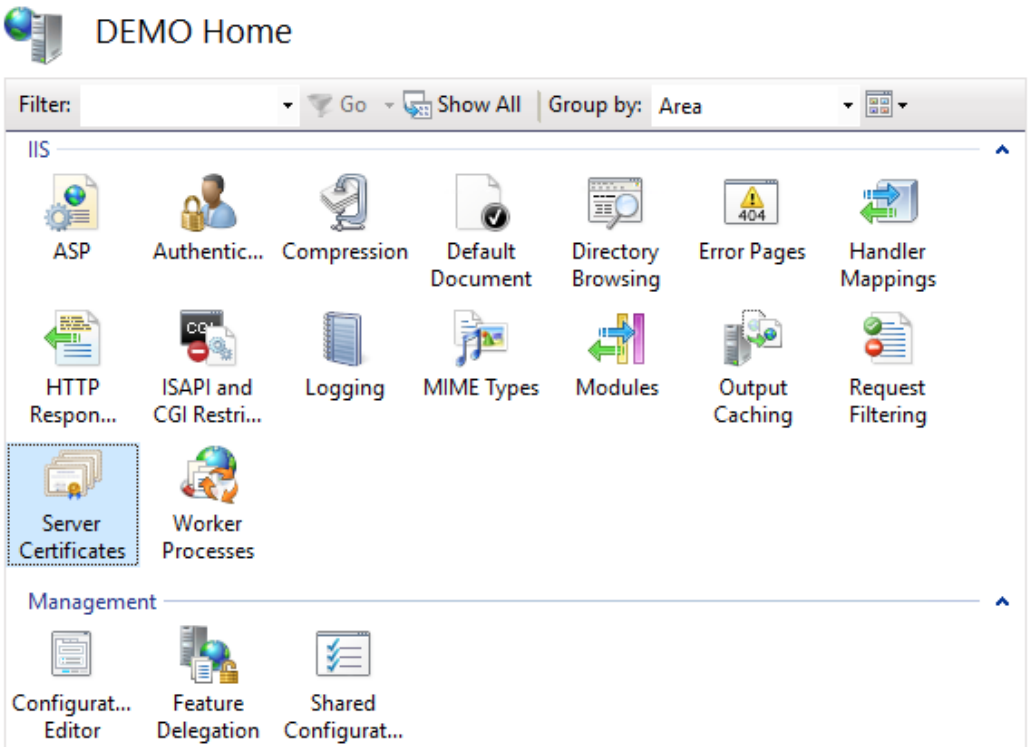
We focus on the configuration of FrameFlow and the systems on which it runs.

It assumed that other general best practices, such as robust auditing and timely installation of patches, are already in place.

About the **Main Console**

The main console is the web-based interface that you use to configure and manage your monitoring configuration. For ease of installation, FrameFlow includes an integrated web server.

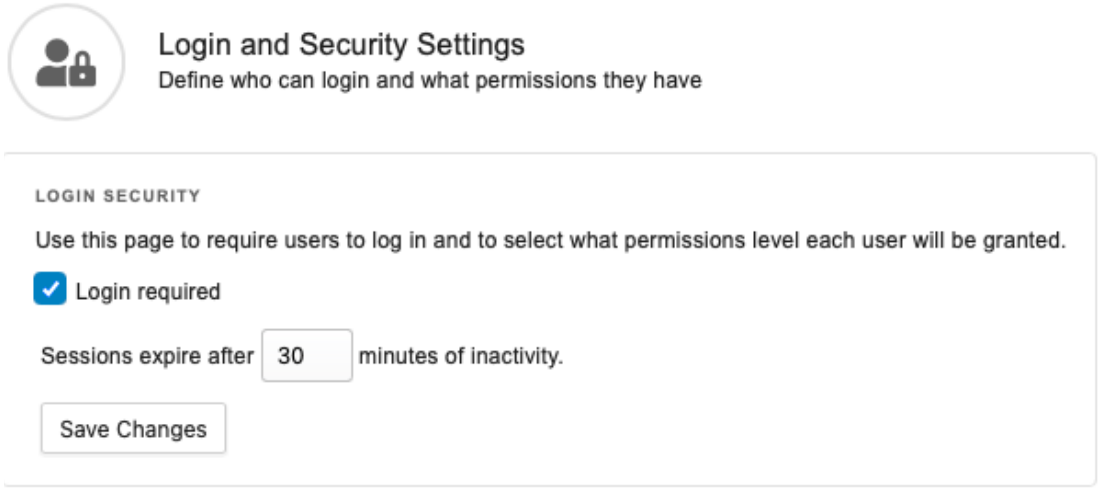
This helps you get up and running in an evaluation environment but in production, you should switch to running the interface on IIS.



To migrate to IIS, see this guide on our website.

Main Console: Enable Login Security

After installing FrameFlow on a new system, go to the “Settings” section and select “Login and Security Settings”. There, you can enable login security and define a list of users who will have access to the FrameFlow interface.



Main Console: Use Security Roles

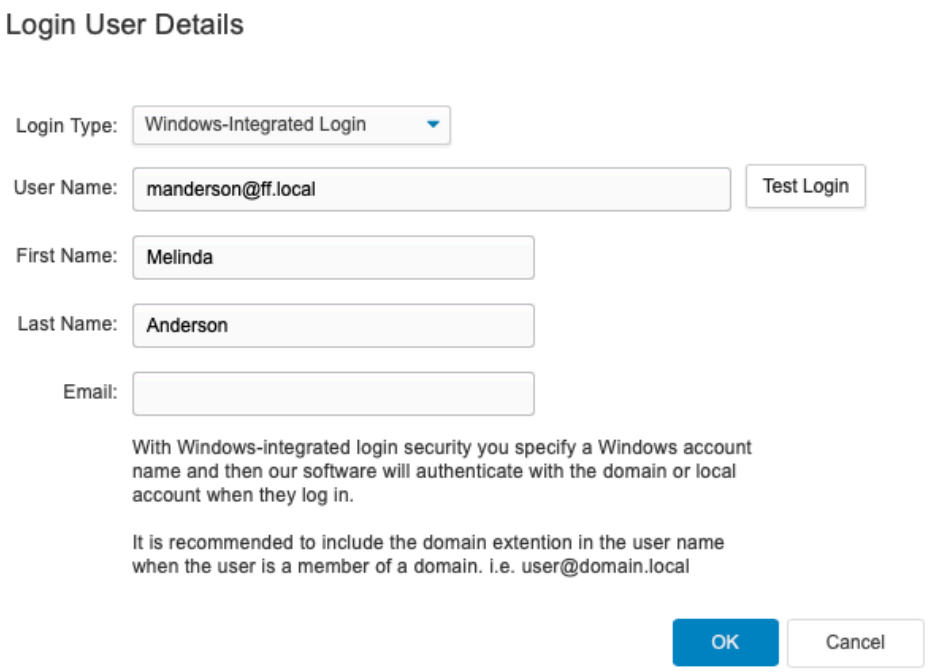
The first account that you create in FrameFlow will be assigned the Administrator role and will have full access to your monitoring configuration.

FrameFlow allows you assign restricted roles to specific accounts so that users only have access to the features and functionality that they require.

For example, users with a View Only role can see the monitoring configuration but cannot make changes to it. Users with the Dashboards Only role, have access to only that part of the FrameFlow interface.

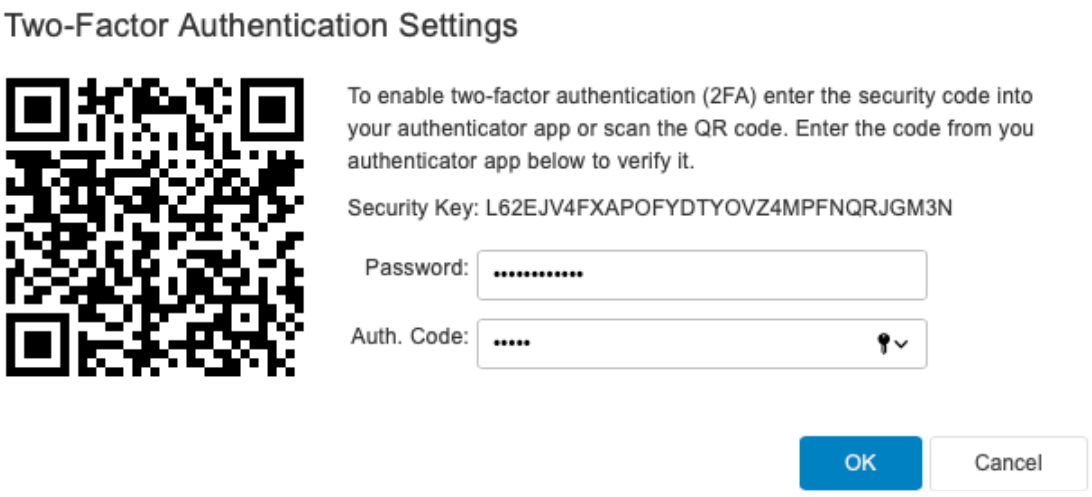
Main Console: Windows Integrated Security

We recommend that you use the “Windows Integrated” login type. With the Windows integrated type, you log into FrameFlow using your Windows domain account. FrameFlow validates your credentials with your domain controllers and only allows access to the interface if the authentication request is approved.



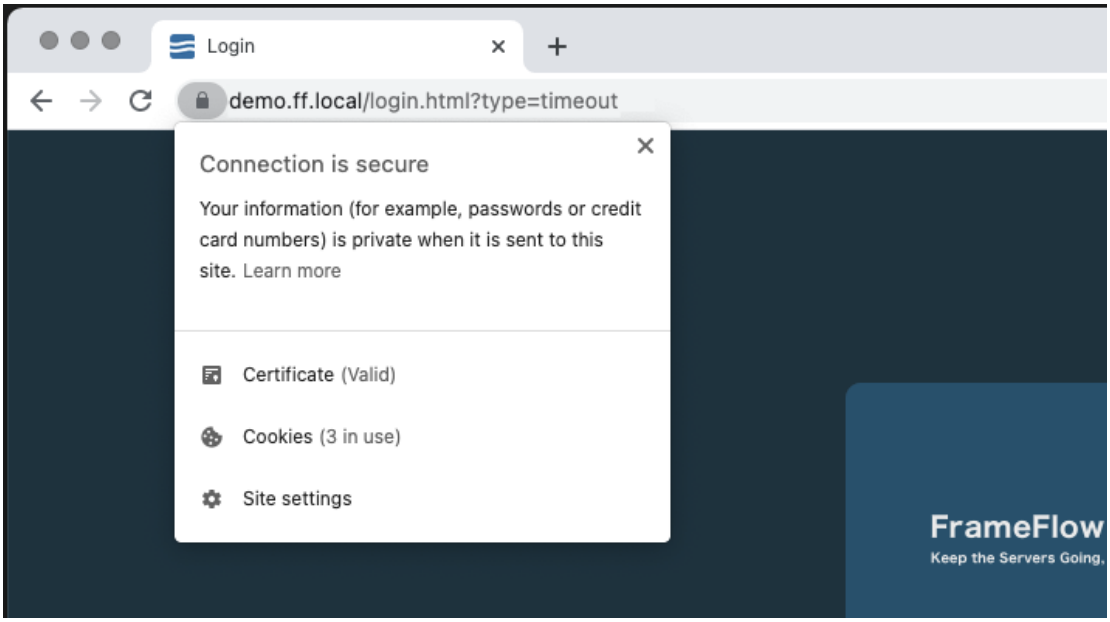
Main Console: Two-Factor Authentication

For additional security, we recommend that all FrameFlow users enable two-factor authentication. To enable two-factor authentication, you will scan a QR code using your preferred authentication application (for example Google Authenticator or Microsoft Authenticator). Then, after logging into FrameFlow, you will be prompted for a login code that is generated by your authentication app.



Main Console: Use HTTPS

As part of migrating to HTTPS, you should add an SSL certificate to IIS and disable HTTP. Using the IIS Manager, you can easily add a self-signed certificate; however, we highly recommend that you use a full certificate.



Main Console: Inbound Access

We recommend that you control access to the FrameFlow console. If you have allowed access to the console from the internet, for example for multi-site monitoring, we strongly recommend that you implement IP-based restrictions to control where the interface can be accessed from.

For additional security, you can use IIS to implement challenge-response authentication. While configuring your remote nodes, you can specify the credentials for this authentication.

Main Console: Outbound Access

We recommend that you lock down the main console system so that it does not have direct access to the internet.

Many kinds of malware and ransomware rely on access to the internet in order to communicate with their command and control servers. Disabling outside access can help to mitigate malware risks.

By disabling outside access, you will no longer be notified in the FrameFlow interface when a new version is available for download. Instead, you can subscribe to our monthly email newsletter to stay up to date about new features and releases. Or you can optionally allow outside access to https://www.frameflow.com.

If you are using our mobile apps and Telemetry service, you will need to allow outside access to https://cloud.frameflow.com. If you have a FrameFlow subscription license, you will need to allow outside access to https://licensing.frameflow.com.

Some FrameFlow customers use our software to monitor their websites and other public-facing services. To do so, you will need to allow outside access to those domain names and/or IP addresses.

Remote Nodes: Outbound Access

Many FrameFlow customers take advantage of our multi-site monitoring features. To enable multi-site monitoring, install FrameFlow on another system and during the installation select the “Remote Node” install type.

As with your main console, we recommend that you lock down outbound internet access from the remote node.

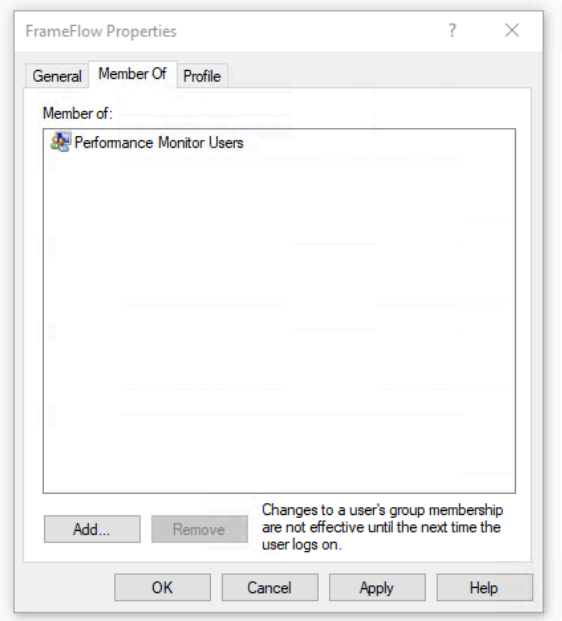
The only outbound connection it requires is HTTPS access to your main console.

Remote Nodes: Inbound Access

FrameFlow remote nodes do not require any inbound access. All communications with the main console are initiated by the remote node and are outbound only.

Monitoring: Agentless Monitoring

FrameFlow is a 100% agentless monitoring system which means you never need to install anything on the systems being monitored. Instead, it connects using credentials that you supply and therefore complies with your existing network security rules.



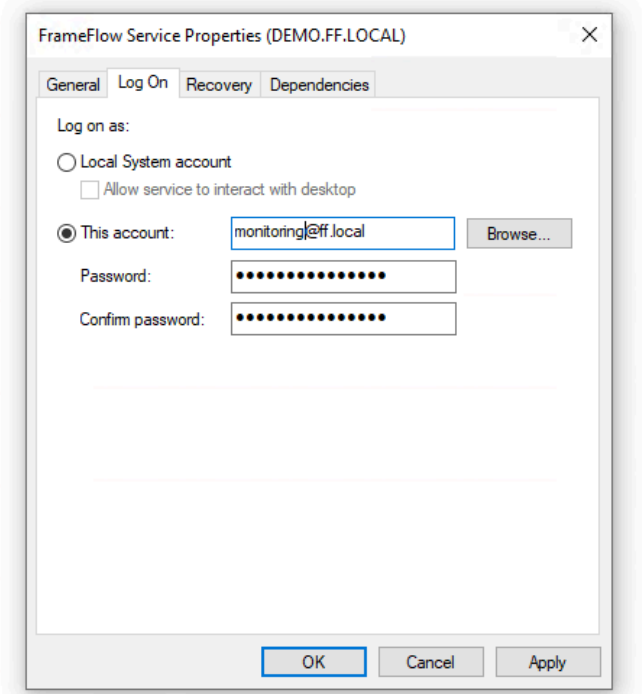
FrameFlow is a multi-purpose monitoring system which means it often needs different credentials for different types of monitoring. We recommend that you use an account with the minimum required permission for the types of monitoring that you require.

Many types of monitoring can be performed using an account that is a member of the Domain Users group or the Performance Monitor Users group. Some other types of monitoring, for example, Windows Service monitoring, require administrator permissions. FrameFlow allows you to use both domain and local admin accounts, helping you to choose the account type that best fits your requirements.

Our Event Monitor Reference Library shows complete details about which protocols are used by each event and which rights are required as well.

Monitoring: Service Account

Many event monitor types have an authentication option called “Use the Monitoring Service Account”. With that selected, FrameFlow does not need credentials to collect monitoring data. Instead, it inherits the rights of the account that the service is running in.



By default, FrameFlow runs in the “Local System” account that is built into Windows. That account has broad access to the local machine but almost no permissions to access other systems. Instead, you can use the Windows Service Manager to set the service to run in a different account that has domain or network rights.

There are two advantages to doing this. First, the account credentials are managed and secured by Windows. Secondly, since FrameFlow no longer needs to send an explicit authentication request, some types of monitoring will proceed more quickly and efficiently.

Summary

These tips, combined with other security measures like frequent patch installation, will help you keep a tight lock on your monitoring environment. To maintain a state of maximum security, refer back to this document frequently.

Want to learn more about authentication and make sure you're not giving away too many permissions?

Take a look at our case-by-case Event Monitor Reference Guide to check the permissions you're giving to each event monitor in your FrameFlow configuration.