FACTSET 〉 SEE THE ADVANTAGE

FactSet Web & Workstation: Authentication Security Zones

FactSet is committed to assuring the confidentiality, integrity and availability of all data entrusted to us by our clients and vendors. As part of that commitment, FactSet deploys data privacy controls, interactive sign-on and Single Sign-On processes defined by internal security policies and aligned with industry best practices.

Default settings assure the continued safe storage of client data and operation of client products and services, whilst allowing clients to customize the user experience through control of two-factor authentication frequency, session timeouts, password settings and trusted IP range Security Zones.

FactSet Web

Single Sign-on + Interactive Authentication

Clients can establish SAML2.0 federations directly with FactSet to enable Single Sign-On (SSO) for their FactSet Web users. A Single Sign-On federation will mitigate the need for username, password and two-factor authentication interactions whilst continuing to restrict access based on the defined IP address ranges. Clients should reach out to their account team if they wish to deploy SSO for their web-based users.

Defining Security Strength

The Security Zones and settings described below apply to a range of FactSet web products such as FactSet Web, Issue Tracker, Control Center, CallStreet, Developer.

FactSet delivers a four zone trust model consisting of **Low Trust**, **Medium Trust** (default), **High Trust** and **No Trust**. Client IT, market data and security teams can use our self-service portal - Control Center - to define which source IP ranges fall under which Security Zone. All changes to these definitions are logged and auditable. Where an IP address is configured across multiple Security Zones, the highest Security Zone will take precedence.

Please reach out to your account team to manage which individuals at your firm have access to configure Security Zones within Control Center.

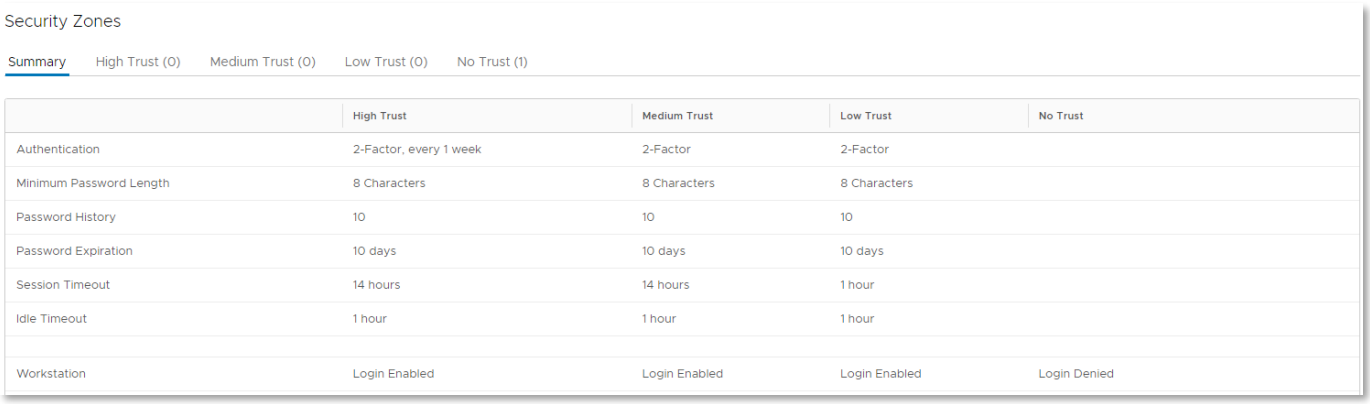
Low Trust enforces 2FA on every logon and has a short (15 minute) idle timeout with 1 hour session timeout.

Medium Trust enforces 2FA on every logon, has a 60 minute idle timeout, and a 14 hour session timeout – meaning a user can actively use the site all day without being logged out.

High Trust enforces 2FA logons periodically (once every 1, 2, 3, or 4 weeks); logons between these intervals only require username and password. High Trust has a longer, 60 minute, idle timeout along with a 14-hour maximum session.

No Trust means that all logons are denied.

Copyright © 2021 FactSet Research Systems Inc. All rights reserved.


Security Zones

Summary | High Trust (0) | Medium Trust (0) | Low Trust (0) | No Trust (1)

	High Trust	Medium Trust	Low Trust	No Trust
Authentication	2-Factor, every 1 week	2-Factor	2-Factor	
Minimum Password Length	8 Characters	8 Characters	8 Characters	
Password History	10	10	10	
Password Expiration	10 days	10 days	10 days	
Session Timeout	14 hours	14 hours	1 hour	
Idle Timeout	1 hour	1 hour	1 hour	
Workstation	Login Enabled	Login Enabled	Login Enabled	Login Denied

FactSet Workstation

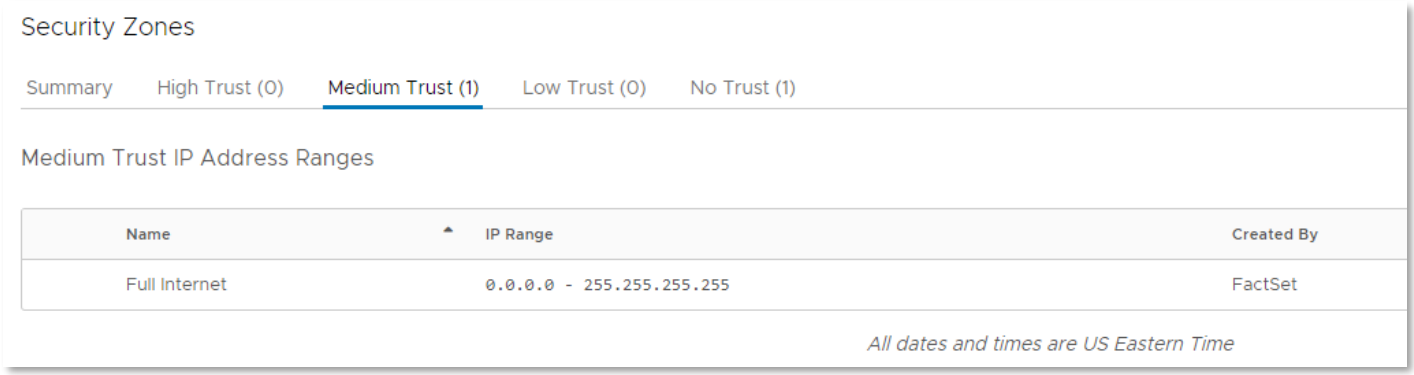
Defining Security Strength

Access to the FactSet Workstation requires an initial two factor authentication per user, per device. The user's IP address will then be validated against the IP ranges contained in the four Security Zones described above. Access to the Workstation will be granted to any IP address configured in the Low, Medium, or High Security Zones. Access to the Workstation will be denied if the user's IP address is found in No Trust and there is no equivalent address defined in the Low, Medium, or High zones.

For example, if corporate IPs are added to Low, Medium, or High, and "0.0.0.0-255.255.255.255" only appears in No Trust, Workstation and Web connectivity would only be allowed when coming from corporate IPs.

Default Settings

The default Interactive Sign-on - Web and Workstation settings include all IP networks in the **Medium Trust** Security Zone. The Medium Trust model is enforced as default to accommodate a variety of client working environments and to prevent malicious actors from using stolen credentials from an unknown source. Depending on the sensitivity of the data being uploaded to FactSet, and the corporate security model of the firm using FactSet, CISO's and InfoSec Administrators can enforce a policy that is compliant with their needs. For more information on Security and Cyber Risk, please see sections within the FactSet Technology Overview Guide


Security Zones

Summary | High Trust (0) | Medium Trust (1) | Low Trust (0) | No Trust (1)

Medium Trust IP Address Ranges

Name	IP Range	Created By
Full Internet	0.0.0.0 - 255.255.255.255	FactSet

All dates and times are US Eastern Time

Copyright © 2021 FactSet Research Systems Inc. All rights reserved.

Managing Security Zones within Control Center

Control Center allows clients to manage their FactSet configuration within one convenient web portal. The instructions below walk through the steps to modify settings for each security zone and the IPs associated with those zones.

Control Center - Security - Interactive Sign-on

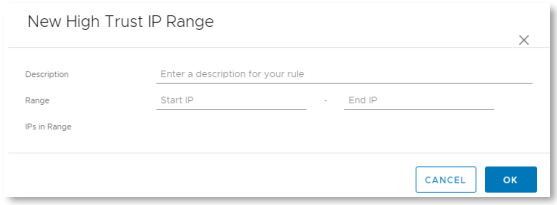
1. Browse to https://controlcenter.factset.com/ within a web browser
2. Login using your corporate email address or factset.net ID
3. Within Control Center, navigate to **Security - Interactive Sign-on**

Managing IPs

Control Center allows individual IPs or IP ranges to be added to each security zone.

Create New Rule

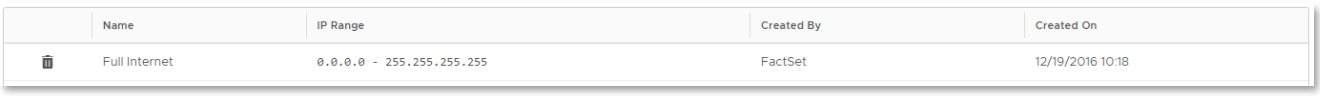
1. Click on the Security Zone you wish to modify
2. Enter a description in the 'New IP Range' dialog
3. Enter the first and last IP address from the range. The number of IPs in the range is listed for reference
    - If only a single address is needed, enter the IP as both the first and last within the range



4. Click 'Add Rule'. The new range is listed in the 'IP Address Ranges' table for the given Security Zone. New rules are active within 30 minutes

Remove Existing Rule

1. Click on the Security Zone you wish to modify
2. Click the trash can symbol next to the rule you wish to delete
3. Click 'OK' to the prompt to confirm you wish to remove the rule



Copyright © 2021 FactSet Research Systems Inc. All rights reserved.

Important Notes

- If an IP address is found to match within multiple zones, FactSet will use the following preference:
    1. High Trust (highest preference)
    2. Medium Trust
    3. Low Trust
    4. No Trust (lowest preference)
- At least one zone must contain the range 0.0.0.0 – 255.255.255.255 to represent 'The rest of the Internet'.

Security Zone Settings

The following settings can be customized in High, Medium and Low Security Zones to match your organization's needs. Note that these settings will only apply to FactSet Web products

- **Session Timeout**: The maximum length a session may last before another authentication is required
- **Idle Timeout:** The maximum time a session can be idle before the session is ended and re-authentication is required

Password Settings

The following FactSet Web password settings can be modified. Password settings apply regardless of security zone.

- **Password Expiration:** The maximum number of days before a password must be changed
- **Password History:** The number of unique passwords required before a password can be reused

Copyright © 2021 FactSet Research Systems Inc. All rights reserved.