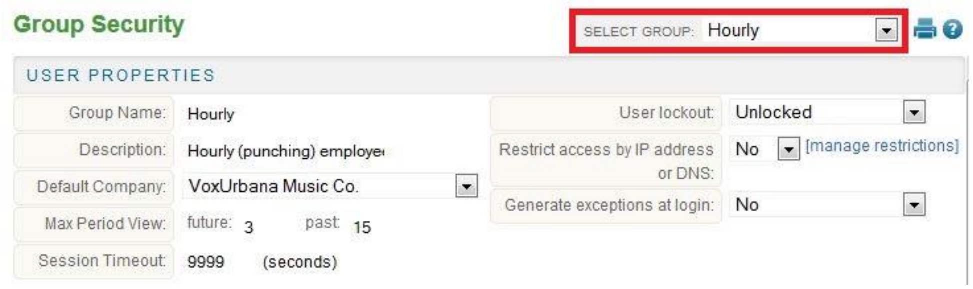
IP Address Restriction Maintenance

IP address restrictions can be a helpful tool that will prevent employees from logging in or punching in offsite. If your organization has a concern that employees are punching in from places other than their work computers and getting paid for hours they're not working, IP address restrictions can help alleviate that concern. There are two places to configure these restrictions:

1) Security Setup > User Security.
   a) This will create a list of IPs from which the individual user is permitted to access Timestar.
   b) Using this path requires that you add acceptable IP addresses to each user individually, and because that requires more upkeep and is time consuming, is <u>not the recommended procedure</u>.
1) Security Setup > Group Security.
   a) This will create a list of IPs that a group of users can use to access Timestar.
   b) Because it is much easier to maintain one list for a large group, this is the recommended procedure.
      i) To turn this feature on:
         (1) Select the desired group in the drop-down at the top.



Group Security

SELECT GROUP: Hourly

USER PROPERTIES

Group Name: Hourly

Description: Hourly (punching) employe

Default Company: VoxUrbana Music Co.

Max Period View: future: 3 past: 15

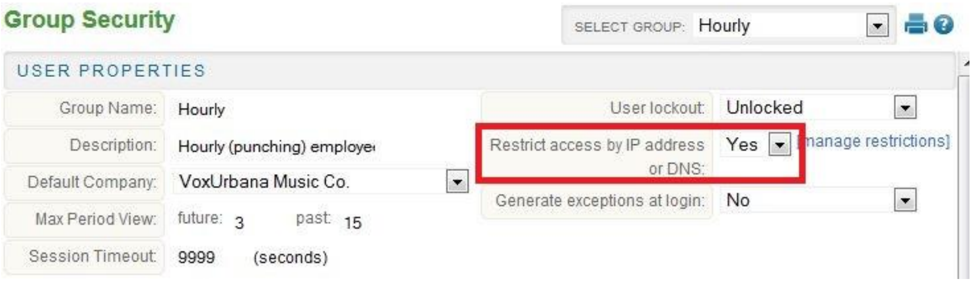
Session Timeout: 9999 (seconds)

User lockout: Unlocked

Restrict access by IP address or DNS: No [manage restrictions]

Generate exceptions at login: No

         (2) Change the option "Restrict Access by IP address or DNS" to YES.



Group Security

SELECT GROUP: Hourly

USER PROPERTIES

Group Name: Hourly

Description: Hourly (punching) employe

Default Company: VoxUrbana Music Co.

Max Period View: future: 3 past: 15

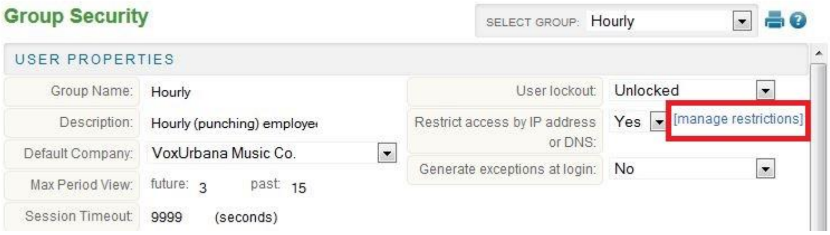
Session Timeout: 9999 (seconds)

User lockout: Unlocked

Restrict access by IP address or DNS: Yes [manage restrictions]

Generate exceptions at login: No

         (3) Click SAVE at the bottom of the page.
      ii) To add/update/remove IP addresses from a list:
         (1) Select the desired group in the drop down at the top.
         (2) Click "manage restrictions" on the right side of the page.



Group Security

SELECT GROUP: Hourly

USER PROPERTIES

Group Name: Hourly

Description: Hourly (punching) employe

Default Company: VoxUrbana Music Co.

Max Period View: future: 3 past: 15

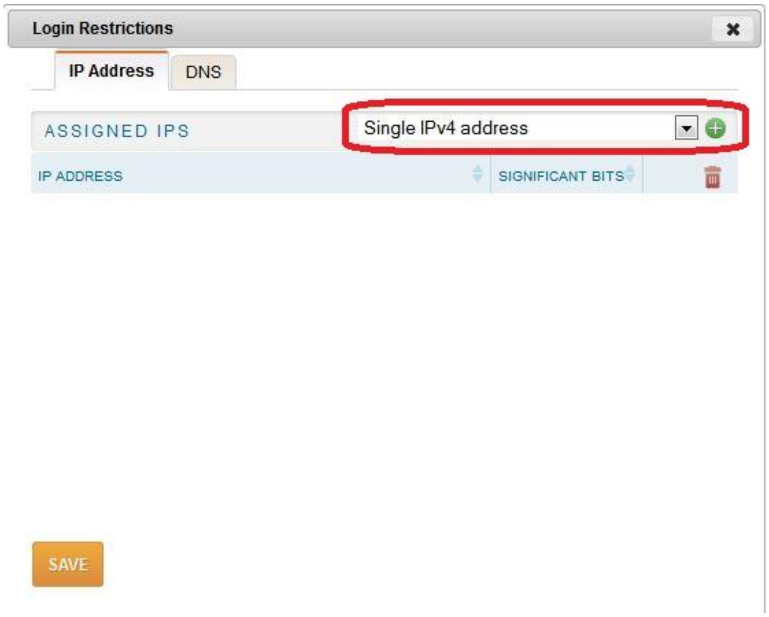
Session Timeout: 9999 (seconds)

User lockout: Unlocked

Restrict access by IP address or DNS: Yes [manage restrictions]

Generate exceptions at login: No

(3) If you only have one address to add, select "Single IPv4 address" and click the green plus sign. Then, type in the address you want to add.

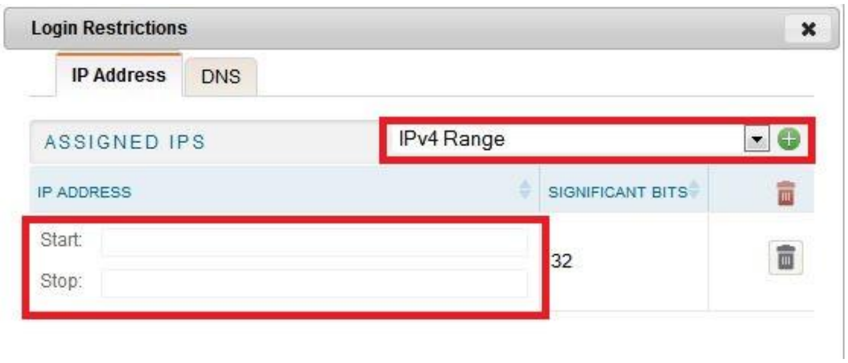


Login Restrictions

ASSIGNED IPS: Single IPv4 address

IP ADDRESS	SIGNIFICANT BITS

(4) If you want to add a large range of consecutive addresses, select "IPv4 range". Enter the first and last addresses in the range.



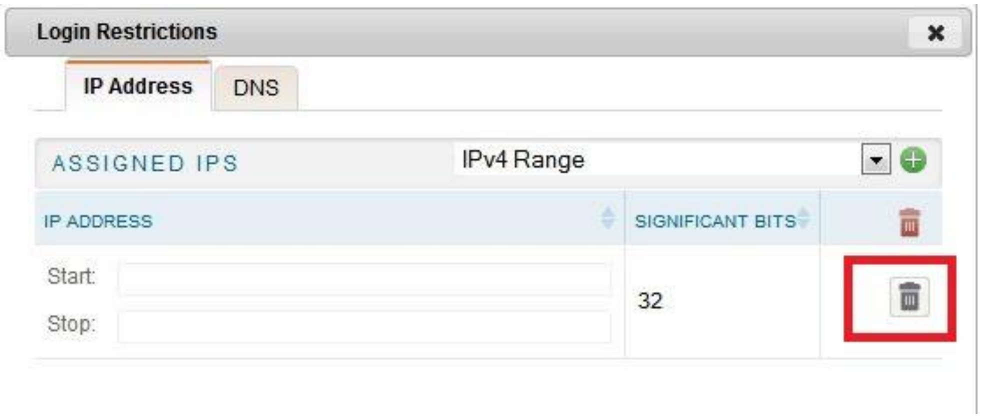
Login Restrictions

ASSIGNED IPS: IPv4 Range

IP ADDRESS	SIGNIFICANT BITS
Start: Stop:	32

(5) Click SAVE at the bottom of the "manage restrictions" screen.

iii) To delete an IP address, click the trash can icon on the right side of the “manage restrictions” screen.



*There is no option to delete multiple addresses at once: they must be deleted individually.

IP address restrictions aren’t something that every company will need to utilize, but they are a boon to those that do. If you have any questions about IP address restrictions that aren’t addressed by the above, please contact Technical Support , and we will be happy to help you!