How do I better user access security in NetScaler MAS?

NetScaler Management and Analytics System is a centralized network management, analytics, and orchestration solution. From a single platform, administrators can view, automate, and manage network services for their distributed NetScaler deployments. In addition to reducing operational costs and simplifying tasks, MAS provides real-time analytics to help administrators identify and address application performance and security issues across the application infrastructure. Further, NetScaler MAS provides application-level visibility through the lifecycle and integration with external orchestration systems.

A system like NetScaler MAS is accessed by many administrators and it is important that some user access security aspects are taken care of to ensure the MAS system is protected.
Here are some of the things an administrator can configure/enable to better MAS user access security.

1) Enabling Strong Password

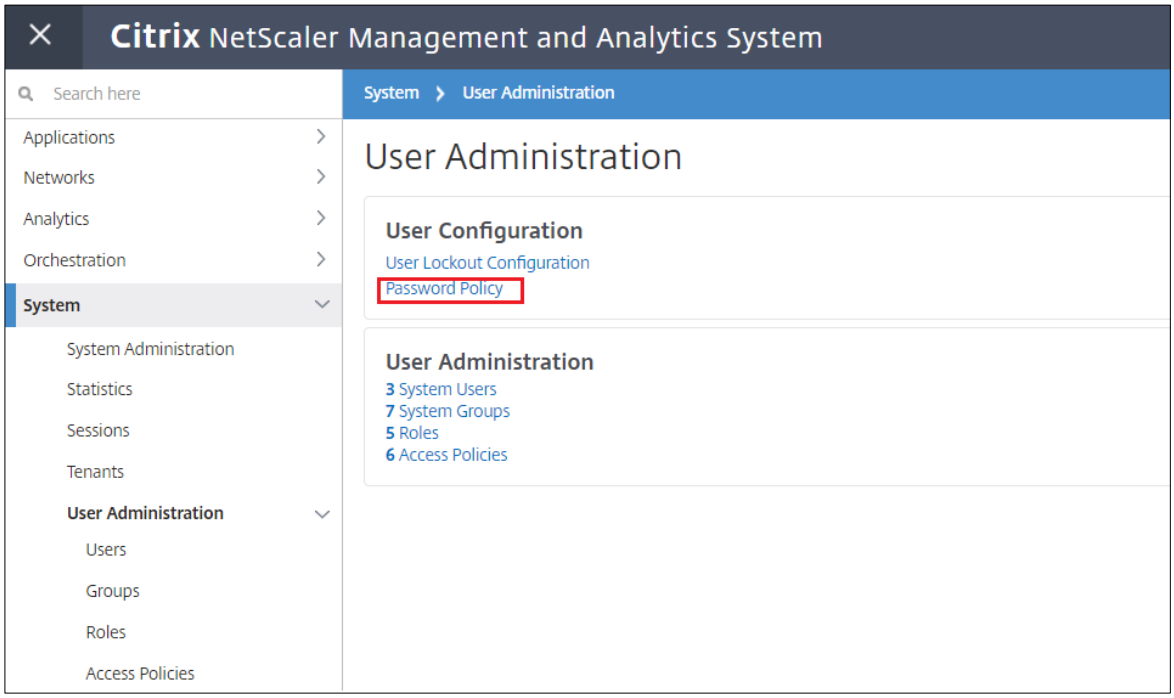
A strong password policy ensures that a MAS user's password is complex thereby making it more secure. The complex password policy feature includes two types of checks:

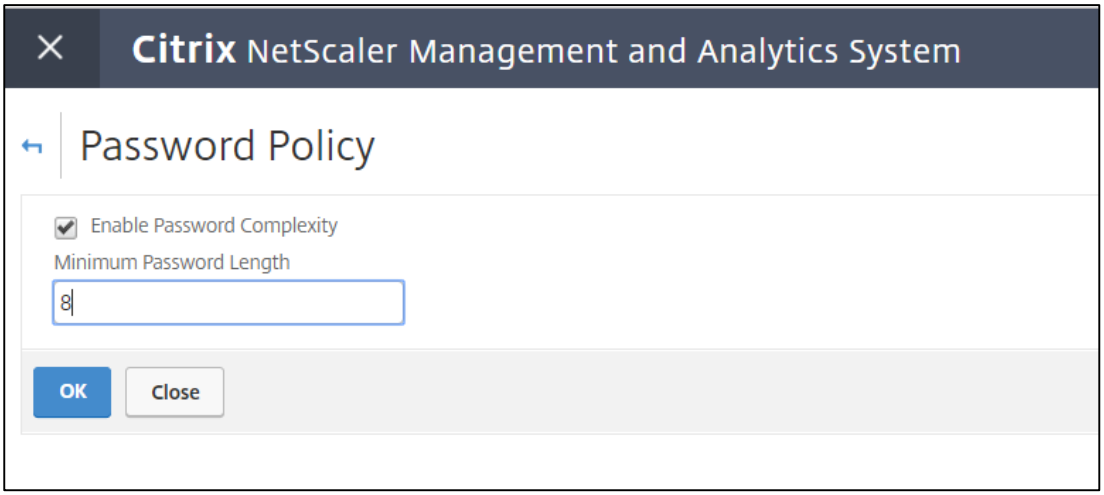
a) Character based check:
These checks ensure that required character types such as uppercase, lowercase, numeric, etc. are part of the password.
If password complexity is enabled, MAS checks for the following in the password:
- At least one lower case character,
- At least one upper case character,
- At least one numeric character,
- At least one special character

b) Length based check
This check ensures that the length of the password is above the minimum value.
If password complexity is enabled, MAS checks for the length of the password to be minimum four. The minimum password length is a configurable option in MAS.
(Maximum length is 128)

NOTE: This setting is applicable only for local users.

To configure strong password, you need to enable password policy.
Go to MAS UI and navigate to System module under User Administration. Select Password Policy and check the 'Enable Password Complexity' checkbox. You may also choose to configure minimum password length.





2) Configure User Lockout Scenario

One way to avoid hacking attempt is to configure a user lockout setting wherein based on the number of failed authentication attempts, a user is locked out of the system. The user remains locked out for a certain period of time which is configurable in system.

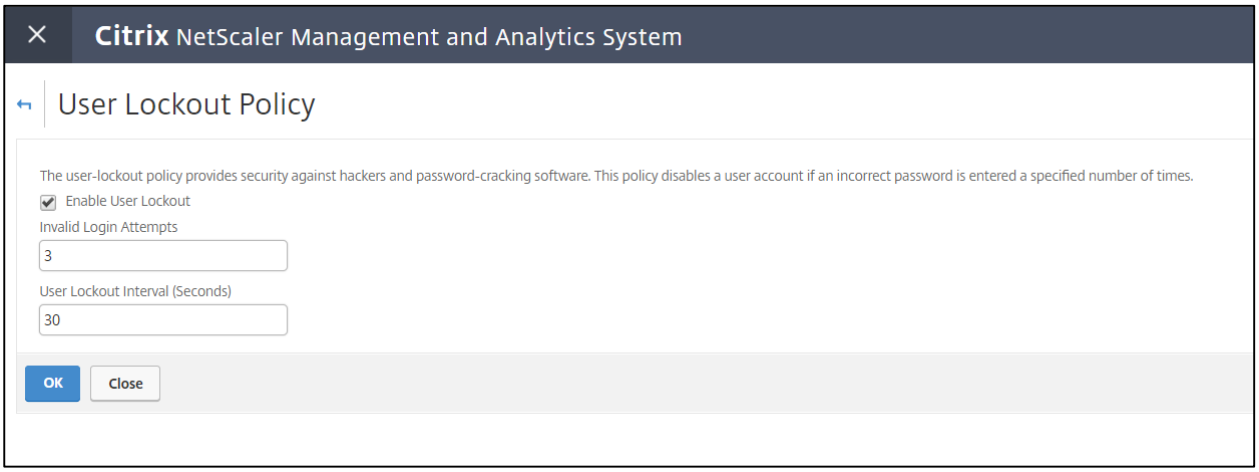
Example: If a user has x invalid login attempts, then he will be locked out for y seconds.

Default values are: 3 for invalid login attempts (maximum 10) and 30 seconds for user lockout interval

NOTE: This setting is applicable only for local users.

To configure user lockout,

Go to MAS UI and navigate to System module under User Administration. Select user lockout configuration and check the ‘Enable User Lockout’ checkbox. You can then configure the ‘Invalid Login Attempts’ and ‘User Lockout Interval’ values

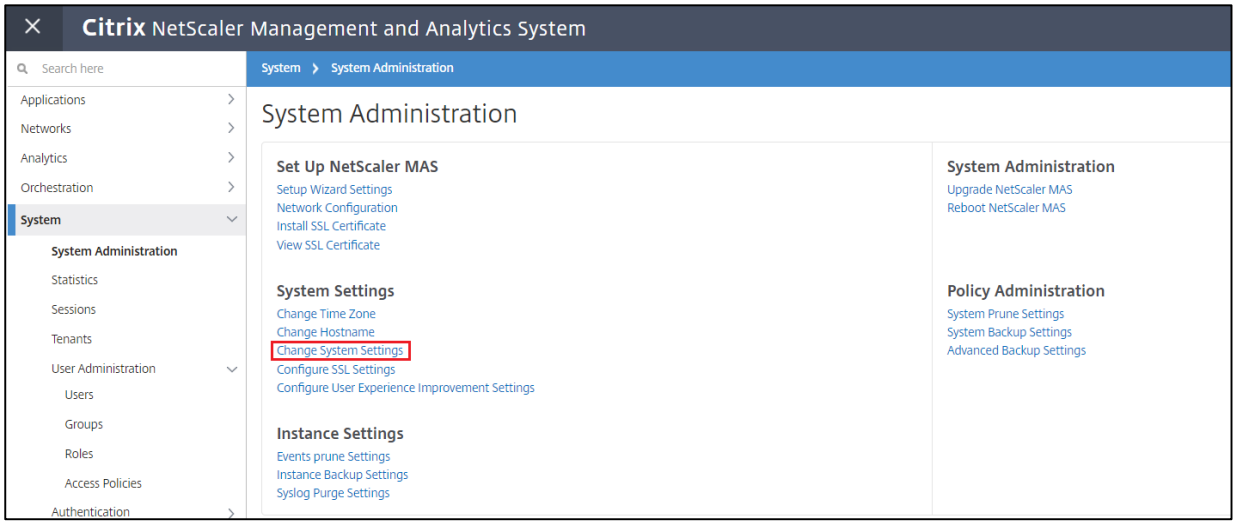


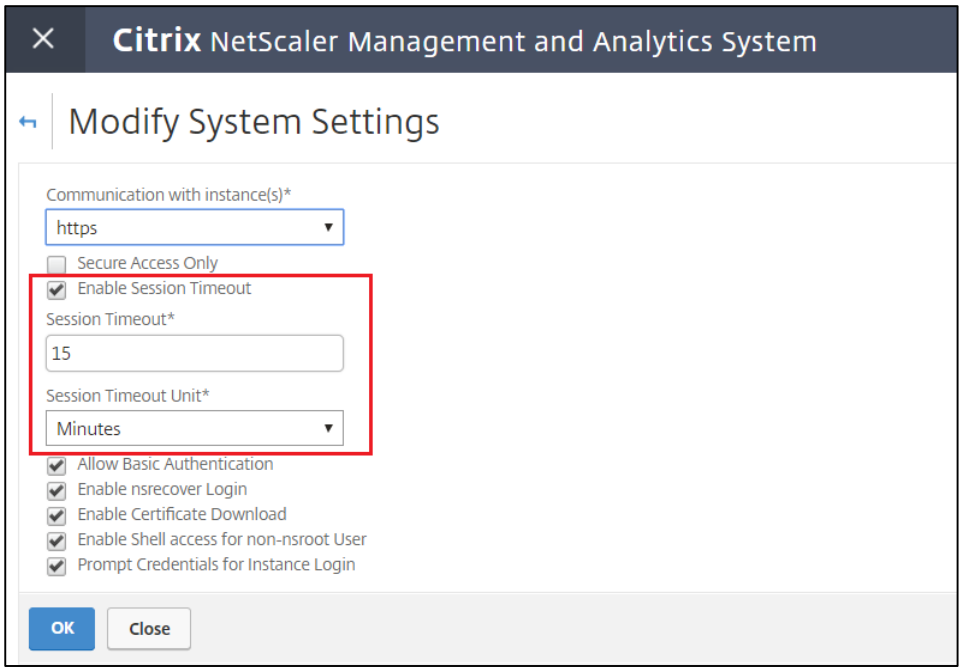
3) Configure Session Timeout

This is particularly helpful to proactively prevent any unauthorized users from taking control of system if the session is unattended for long time.
You can configure session timeout settings to ensure that a user is logged out if his session remains inactive/idle for x minutes.

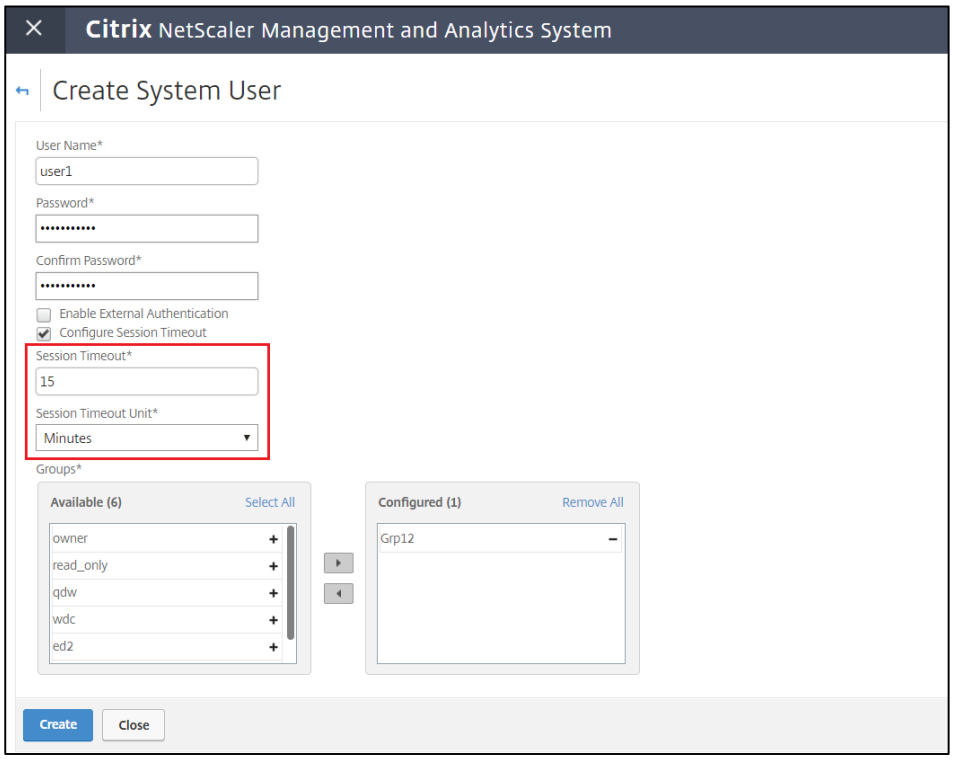
To configure session timeout, you can either do it at system level or per user level

a) System level settings:
Go to MAS UI and navigate to System module under System Administration. Select ‘Change System Settings’. In the next UI Enable checkbox ‘Enable Session Timeout’ and input the values for session timeout. This setting will be applicable to all users.





b) User level settings:
Go to MAS UI and navigate to System module under User Administration. Select ‘User’ and click on Add button. In the next UI enable checkbox ‘Configure Session Timeout’ and input the values for session timeout. This will be applicable to that specific user.


Citrix NetScaler Management and Analytics System
Create System User
User Name*
user1
Password*
Confirm Password*
Enable External Authentication
Configure Session Timeout
Session Timeout*
15
Session Timeout Unit*
Minutes
Groups*
Available (6)
Select All
owner
read_only
qdw
wdc
ed2
Configured (1)
Remove All
Grp12
Create
Close