VSA Two-Factor Authentication Master Admin Guide

VSA User Guide | November 2019

VSA Two-Factor Authentication Master Admin Guide

Release 9.5.0.24 | Version 1.0

Copyright Agreement

Contents

Two-Factor Authentication at Server Level 4
Two-Factor Authentication 4

Two-Factor Authentication at Server Level

Two-Factor Authentication

About

With the first release of VSA 2FA, the 2FA Enrollment is optional. This means that each tenant can make a decision whether or not to require 2FA to login to the VSA.

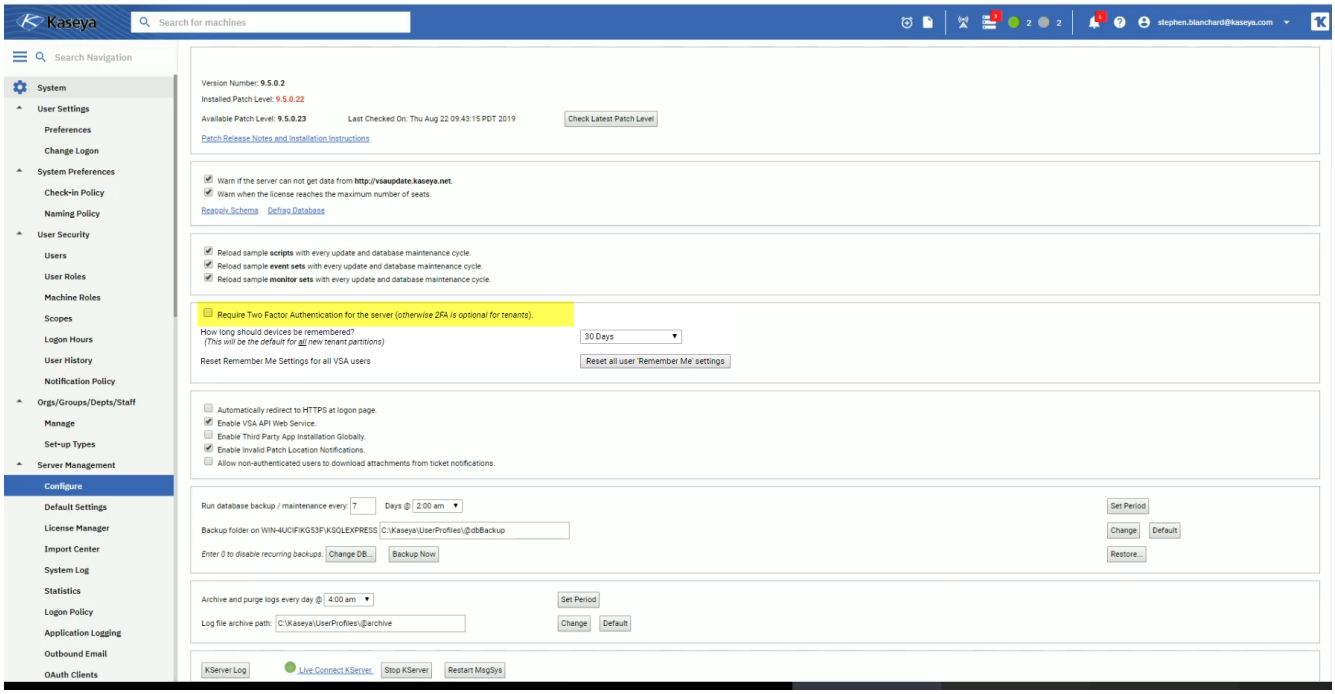
Note: VSA 2FA will become mandatory for all tenants on 31st December 2019.

For this reason, there is a mechanism on Kaseya side, where Master Admin can enforce VSA 2FA throughout all the tenants by making the necessary changes on the server.

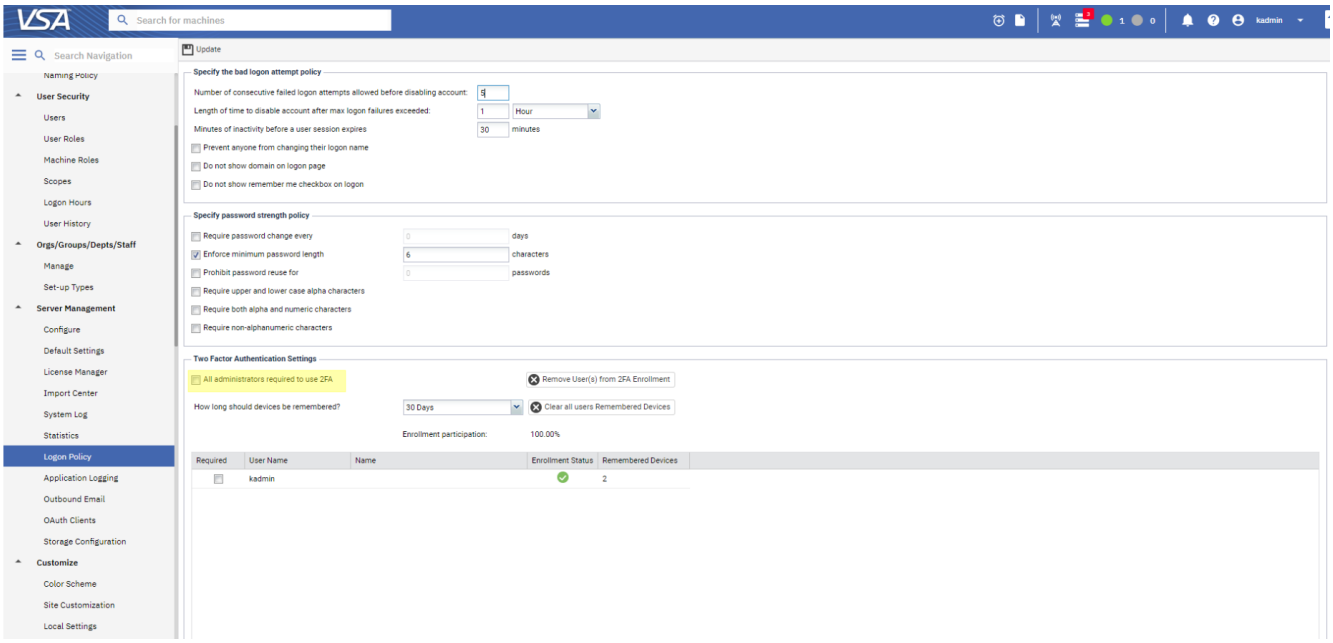
Note: Master Admin – a VSA User with read-write access to System > Server Management > **Configure** page.

Mandatory VSA 2FA Setup

1. Log into the VSA as a Master Admin.
2. Navigate to System> Server Management > **Configure** page.
3. Enable the **Require Two-Factor Authentication (Otherwise 2FA is Optional)** checkbox.



Note: When the setting is enabled, tenants will be disabled to require 2FA for particular users and the **All administrators are required to use 2FA** checkbox becomes disabled for tenants.



Note: Tenant users who have completed 2FA Enrollment Process, will not be required to complete it again after the **Require Two-Factor Authentication (Otherwise 2FA is Optional)** setting is enabled.

Server VSA 2FA Configuration

Master Admin can configure VSA 2FA in the following ways:

- Configure the number of days 2FA Devices are remembered by default for all users of all tenants a particular Master Admin is responsible for.
- Remove remembered 2FA devices for all users among the tenants a particular Master Admin is responsible for.

To configure the server changes:

1. Log into the VSA as a Master Admin.
2. Navigate to System> Server Management > **Configure** page.