VSA User Guide | November 2019

VSA Two-Factor Authentication User Guide

Release 9.5.0.24 | Version 1.0



Copyright Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement.

Contents

	-
About Two-Factor Authentication in VSA	4
Two-Factor Authentication at User Level - Standard Role Admin	4
Two-Factor Authentication Enrollment Process	4
Two-Factor Authentication Subsequent Login	10
Two-Factor Authentication Skip Flow	12
Two-Factor Authentication Security Rules	13
Authenticator application Set up and Configuration for VSA 2FA	14
Two-Factor Authentication at Tenant Level - Master Role Admin	20
Two-Factor Authentication Configuration and Monitoring	20

About Two-Factor Authentication in VSA

Two-factor authentication in VSA Admin Portal has been designed to facilitate and empower security access for users. The feature is meant to prevent unauthorized users from accessing VSA account data.

About 2FA

Enabled 2FA feature obliges a user to provide not only the credentials (username and password), but to submit a Timebased, One-Time Password (TOTP) in order to access the VSA account.

TOTP is an authorization code generated by an Authenticator application and is valid for a limited time. We recommend using the following Authenticator applications:

- Google Authenticator
- Microsoft Authenticator

Note: The Authenticator should be configured prior to enrolling into 2FA in VSA. (See <u>Authenticator application Set</u> up and Configuration for VSA 2FA for more information on the Authentication application configuration.)

2FA in VSA can be configured at three levels:

- at User Level
- at Tenant Level
- at Server Level

Two-Factor Authentication at User Level -Standard Role Admin

Two-Factor Authentication Enrollment Process

2FA enrollment flow

Once the 2FA feature is toggled as required for an entire tenant by Tenant Admin or for particular users within a tenant by System Role user, such a user within the tenant that logs in the VSA Admin Portal must enroll in 2FA:

- 1 Download the TOTP Authenticator application on a mobile device OR add Authenticator Extension in the Chrome browser.
- 2 Launch VSA Admin Portal application and enter credentials as usual.

VSA
Welcome Back
Username
Password
Remember me on this computer
Forgot Password?

3 Click **Next** in the Your Security Matters screen.

VSA
Your Security
Matters
With two-factor authentication (2FA) you will protect your account using both something you know (your password) and something you have (like your mobile phone).
2FA will become mandatory for VSA on 31 Dec 2019.
Let's get started.
No Thanks Next

- 4 Launch the Authenticator application.
- 5 Add your VSA Admin Portal account to the Authenticator application:
 - a. by scanning the QR code displayed in the VSA with the Authenticator application.

١	LSA	74
 Download and I Authenticator A Open the app. Pair your app by 	install a support pp y scanning the control of the control of the t scan the bar	orted TOTP e QR Code below.
4. Verifying the pa below Authentication Code	iring by enter	ing the code
	Back	Submit

b. by manually entering the Alphanumeric Code displayed in the VSA in the Authenticator application.

 Download and Install a supported TOTP Authenticator App Open the app. Pair your app by scanning the QR Code below. 	
Your TOTP Authenticator code	
GBWSNDUUAWHWMTM2K4W4 JXT2IOHBXSNG	
View QR code	
 Verifying the pairing by entering the code below 	
Authentication Code	
Back Submit	

6 Enter Authentication Code generated by your Authenticator application into VSA Admin Portal screen and click enabled **Submit** button.



- **Note:** The Authentication Code should be entered within the 30-second period. Otherwise, you should enter the next non-expired Authentication code displayed in the Authenticator application. The code expiration is tracked in the Authenticator application.
- 7 Click **Done** button to access VSA home page.



been closed by accident, the user will restart from scratch the enrollment process upon next login attempt.

Note: If a user is unable to access the mobile device, System Role User within their tenant has the ability to reset the 2FA status. This will enable the user to go through the 2FA enrollment again.

Two-Factor Authentication Subsequent Login

Once you have enrolled in VSA 2FA, you will have to walk through 2 steps to access your VSA account each time you login the VSA Admin Portal:

1 Provide credentials at the 1st authentication step, as usual.

Welcome Back
Username
Password
Remember me on this computer
Forgot Password?

2 Provide Authentication Code generated in the configured Authenticator application, at the second step to access your VSA.

Thank you for using 2FA. In the TO Authenticator App, select your acc should see a 6-digit code. Type the code below.	TP ount and you authentication
Authentication Code	
I	
Remember Me on this compute	r

3 Access the VSA Admin Portal.

Two-Factor Authentication Skip Flow

If the 2FA enrollment is toggled as optional for an entire tenant or particular users within a tenant, these VSA Users can skip the two-factor authorization process:

- **1** Enter credentials in the VSA Admin Portal page.
- 2 Select No, Thanks button.

VSA ^{**}	
Your Security	
Matters	
With two-factor authentication (2FA) you will protect your account using both something you know (your password) and something you have (like your mobile phone).	
2FA will become mandatory for VSA on 31 Dec 2019.	
Let's get started.	
No Thanks Next	

3 Access the VSA Admin Portal.

WARNING! Two-factor Authentication Enrollment will be mandatory for **all VSA users for all tenants** starting on 01/01/2020.

Two-Factor Authentication Security Rules

- 1 Once enrolled in 2FA, users will have to provide Credentials each time they login VSA. The TOTP-entry step can be skipped, if users choose to remember their device(s) for the time defined at the tenant level.
- 2 If a user fails 2FA verification the number of attempts defined by the Lockout Settings at the tenant level, the user's account will be locked out.

- **Note:** The Lockout will occur, if user enters incorrect values the number of times that exceeds the number of attempts defined by Lockout Settings in either the login page or TOTP-entry screens.
- 3 If a user fails 2FA verification cycle (entering the credentials and the Time-based, One-Time Code) the number of times defined by the tenant Lockout Policy, the User Account will be locked out. To unlock it, please contact a System Role User in your tenant.
- **Note:** Users with active AAoD accounts and AAoD Module enabled for their tenant will be able to continue using the same authentication procedure.

Authenticator application Set up and Configuration for VSA 2FA

Authenticator application is a software designed to generate Time-based, One-Time passwords (TOTP). The TOTP is used as a separate verification step in the 2-factor authentication process to login VSA Admin portal (see <u>Two-Factor</u> Authentication Enrollment Process).

To have the Authenticator application generate the TOTP for VSA Admin Portal, users have to add the VSA account to the Authenticator application during the 2FA enrollment process only. Afterwards, Authenticator application will automatically generate authorization codes for user's subsequent logins.

Authenticator application for mobile devices

To set up a mobile Authenticator app, please follow the following steps:

1 Download and install one of the following applications in App Store for iOS and in Google Play for Android OS:

IOS:

- Google Authenticator: <u>https://apps.apple.com/us/app/google-authenticator/id388497605</u>
- Microsoft Authenticator: https://apps.apple.com/app/microsoft-authenticator/id983156458

Android:

- Google Authenticator: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
- Microsoft Authenticator: https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en
- 2 Launch the installed mobile Authenticator application.
- 3 Select the option to add an Account to the mobile app.

Release 9.5.0.24 | November 2019

^{13:34} Authenticator		'¶ ⇒ : #1
		•
	•	

4 Scan the QR code displayed in the VSA.



5 Find the VSA Account in the Accounts list in the mobile Authenticator application.

Release 9.5.0.24 | November 2019



021804

Tap to Copy



6 Enter the Time-based, One-Time Password (TOTP) displayed in the Authenticator application in the VSA and click the Submit button.



Note: The Authentication Code should be entered within the 30-second period. Otherwise, you should enter the next non-expired Authentication code displayed in the Authenticator application. The code expiration is tracked in the Authenticator application.

Note: The VSA Account should be displayed on the Accounts list in the mobile application.

(See Two-Factor Authentication Subsequent Login for more information.)

Workaround for mobile Authenticator application setup

If you have issues at scanning the QR code, you can add your VSA Account manually in a mobile Authenticator application:

- **1** Select Add an Account option in the installed mobile application.
- 2 Enter Username and the Key.
- Note: To view the Key, click the I can't scan the bar code option in the VSA application. The key will be displayed as Your TOTP Authenticator code in the VSA application instead of the QR code.

Release 9.5.0.24 | November 2019

15:21		-11l 🤶 💷
← .	Add Account	
by Kaseya	Enter your secret key to add your account.	
user@c	ompany.com	
Secret k	Key	
	SUBMIT	



3 Enter an authorization code generated by the Authenticator application into the VSA and click the Submit button.

Issue you may face during the Authenticator application setup on a mobile device

- If you have added your VSA account to the Authenticator application, but the generated code does not work, make sure that the Authentication Code has not expired. If it has, enter a new valid authentication code while it is valid.
- If you have added your VSA account to the Authenticator application and have entered a valid Authentication code, delete your VSA Account in the mobile Authenticator application and complete 2FA steps from again.

Two-Factor Authentication at Tenant Level -Master Role Admin

Two-Factor Authentication Configuration and Monitoring

Users in the System and Master Role can configure 2FA feature within their tenant.

VSA Users that have read-write access to System > Server Management> Logon Policy settings can also view and configure the 2FA feature, depending on their role permissions.

2FA configuration in VSA includes the following functions:

- Enforce VSA 2FA for a tenant when logging the VSA Admin Portal. 2FA enforcement can be applied to particular Users within a tenant organization.
- Monitor VSA 2FA enrollment process status within a tenant.
- Reset VSA 2FA for a User or multiple Users within a tenant.
- Reset VSA 2FA devices for a User or multiple Users within a tenant.

VSA 2FA Enforcement

By default, 2FA is set to optional for all VSA tenants. To add security to user accounts within a tenant, it is recommended that each tenant configures 2FA as a mandatory login process.

To enforce 2FA in VSA for all user within a tenant:

- **1** Login to VSA with the corresponding permissions.
- 2 Navigate to System > Server Management> Logon Policy page.
- 3 Enable the All administrators are required to use 2FA checkbox.

Release 9.5.0.24 | November 2019

VSA Q Search	for machines		🗑 🖿 👷 🟪 🧕 15 🌑 39 🗍 🌲 🖓 😝
E Q Search Navigation	Update		
	Specify the bad logon attempt policy		
System	Number of consecutive failed logon attempts allow	d before disabling account: 3	
 User Settings 	Length of time to disable account after max logon f	ilures exceeded: 1 Hour	
Preferences	Minutes of inactivity before a user session expires	30 minutes	
Change Logon	Prevent anyone from changing their logon name		
 System Preferences 	Do not show domain on logon page		
Check-in Policy	Do not show remember me checkbox on logon		
Naming Policy	Specify password strength policy		
A Hear Sacurity	Require password change every	davs	
- User Security	Enforce minimum password length	6 characters	
Users	Prohibit password reuse for	passwords	
User Roles	Require upper and lower case alpha characters		
Machine Roles	Require both alpha and numeric characters		
Scopes	Require non-alphanumeric characters		
Logon Hours			
User History	Two Factor Authentication Settings		
Notification Policy	All administrators are required to use 2FA	Remove user(s) from 2FA enrollment	
 Orgs/Groups/Depts/Staff 	How long should devices be remembered?	30 Days 👻 😵 Clear all users remembered devices	
Manage		Excellencer excellence 102.1	
Set-up Types		Emotiment pertraperon. 1.72.4	
 Server Management 	Required User Name Nam	Enrollment Status Remembered Devices	
Configure	auto0@test.com user	est X 0	
Defende Costinues	auto1@test.com user	est X 0	
Default Settings	auto10@test.com user	est 0	
License Manager	auto11@test.com user	est 0	
Import Center	auto12@test.com user	est X 0	
System Log	auto13@test.com user	est X 0	
Statistics	auto14@test.com user	est X 0	
Logon Policy	auto15@test.com user	est X 0	
Application Logging	auto16@test.com user	est 🗶 0	
	auto17@test.com user	est 🗶 0	

4 Save the changes.

Now every user within the tenant will have to follow the 2FA process to login their VSA account.

To enforce 2FA in VSA for particular user(s) within a tenant:

- **1** Login VSA app with the corresponding permissions (see above).
- 2 Navigate to System > Server Management> Logon Policy page.
- 3 Select the users within a tenant that you would like to oblige to follow the 2FA process.

VSA Q Search	n for machin	es					
Search Navigation	💾 Updat	te					
	Specif	fy the bar	d logon attempt policy				
System	Numb	er of con	secutive failed logon attemp	its allowed befo	re disabling account: 3		
 User Settings 	Length	h of time	to disable account after max	logon failures	exceeded: 1	Hour	*
Preferences	Minute	es of inai	ctivity before a user session e	expires	30	minutes	
Change Logon	Pre	went any	one from changing their logo	n name			
* System Preferences	Do I	not show	/ domain on logon page				
Check-in Policy	Do I	not show	remember me checkbox on	logon			
Naming Policy	Specif	ly passw	ord strength policy				
▲ Hear Security	E Reg	ouire pas	sword change every			davs	
user security	Enf	orce min	imum password length		6	characters	
Users	Pro	hibit pas	sword reuse for			passwords	
User Roles	Req	quire upp	er and lower case alpha char	acters			
Machine Roles	Req	quire both	h alpha and numeric characte	trs			
Scopes	Req	quire non	-alphanumeric characters				
Logon Hours							
User History	Two F	actor Aut	thentication Settings				
Notification Policy	E Alla	administ	rators are required to use 2FA	A		😢 Remove u	ser(s) from 2FA enrollment
 Orgs/Groups/Depts/Staff 	Howle	ong shou	Id devices be remembered?		30 Days	Clear all user	s remembered devices
Manage							
Set-up Types					Enrollment participation:	1.92 %	
A Server Manadement	Requi	ired	User Name	Name		Enrollment Statu	s Remembered Devices
- Server Hanagement	l		auto0@test.com	user test		×	0
Configure	l		auto1@test.com	user test		×	0
Default Settings	(auto10@test.com	user test		×	0
License Manager	(auto11@test.com	user test		×	0
Import Center	(auto12@test.com	user test		×	0
System Log			auto13@test.com	user test		×	0
Statistics	I		auto14@test.com	user test		×	0
Logon Policy			auto15@test.com	user test		×	0
Application Lotting	-		auto16@test.com	user test		×	0
Approaried Logging	(auto17@test.com	user test		×	0

Note: If you do not have the checkboxes to select particular users, please make sure you have the All administrators are required to use 2FA checkbox unselected.

4 Save the changes.

Now the selected user within the tenant will have to follow the 2FA process to login their VSA account.

2-Factor Authentication Enrollment Process Monitoring

VSA Users with the corresponding permissions can monitor the status of 2FA enrollment process by Enrollment Status per each user within a tenant.

Currently, there are three 2FA Enrollment Status available:

- × user is not enrolled in VSA 2FA.
- I user is successfully enrolled in VSA 2FA.

• user is partially enrolled in VSA 2FA. It means that user has not completed the 2FA enrollment process by entering the TOTP for some reason. These users will have to complete the 2FA enrollment process upon next log in.

To monitor 2FA Enrollment Status of each user:

- **1** Login VSA app with the corresponding permissions.
- 2 Navigate to System > Server Management> Logon Policy page.

Release 9.5.0.24 | November 2019

Required	User Name	Name	Enrollment Status	Remembered Devices
	bd	bd user	×	0
	cecilia.osborn@kaseya.com	Cecilia Osborn	×	0
	daria.kovsharova@kaseya.co	I Daria Kovsharova	0	0
	kadmin		0	0
	kseniia	kseniia p	0	0
	sduser	sd user	×	0
	stephen.blanchard@kaseya.c	Stephen Blanchard	0	1
	Valentina.Pristavka@kaseya.	Valentina Pristavka	0	0

2FA Rest Options

VSA Users with the corresponding permissions can reset the 2FA enrollment status for each user within a tenant in any 2FA Enrollment phase. This is helpful, for example, if users have completed the 2FA enrollment process, but for some reason they cannot log into VSA successfully.

There are 2 ways for a Master or System Role User to modify a user's 2FA enrollment:

Step 1: By removing 2FA Remembered Devices for *all users* within a tenant.

- **Note:** Removing user's devices will not unenroll the User from 2FA. The user will have to enter a one-time password.
- Step 2: By unenrolling a particular user or multiple users. This will also remove the user's remembered devices.

To remove 2FA Remembered Devices for all users

- **1** Log into VSA with the corresponding permissions.
- 2 Navigate to System > Server Management> Logon Policy page.
- 3 Click the Clear all users remembered devices button.

	for machino-		· · · ·			
Search	ior machines					
E Q Search Navigation	Update					
	Specify the t	oad logon attempt policy				
system	Number of c	onsecutive failed logon attem	npts allowed befo	re disabling account: 3		
 User Settings 	Length of tin	ne to disable account after m	ax logon failures	exceeded: 1	Hour	Y
Preferences	Minutes of in	nactivity before a user session	n expires	30 m	minutes	
Change Logon	Prevent a	nyone from changing their log	on name			
 System Preferences 	Do not sh	ow domain on logon page				
Check-in Policy	Do not sh	ow remember me checkbox o	on logon			
Naming Policy	Specify pass	word strength policy				
 User Security 	Require p	assword change every		0 da	ays	
lieere	Enforce m	ninimum password length		6 ct	haracters	
users .	Prohibit p	assword reuse for		0 pt	asswords	
User Holes	Require up	pper and lower case alpha ch	aracters			
Machine Roles	Require b	oth alpha and numeric charac	ters			
Scopes	Require no	on-alphanumeric characters				
Logon Hours						
User History	- Two Factor A	Authentication Settings			-	
Notification Policy	All admini	istrators are required to use 2	'FA		Remove us	ter(s) from 2FA enrollment
 Orgs/Groups/Depts/Staff 	How long sh	ould devices be remembered	?	30 Days 🛩	 Clear all users 	remembered devices
Manage				Encolment participation:	1.02.%	Cle
Set-up Types						
 Server Management 	Required	User Name	Name		Enrollment Status	Remembered Devices
Confidure		auto0@test.com	user test		X	0
Default Settings		auto1@test.com	user test		×	0
Deleur Sertings		auto10@test.com	user test		×	0
License Manager		auto11@test.com	user test		×	0
Import Center		auto12@test.com	user test		X	0
System Log		auto13@test.com	user test		×	0
Statistics		auto14@test.com	user test		X	0
Logon Policy		auto15@test.com	user test		×	0
Application Logging		auto16@test.com	user test		X	0
Outbound Email		auto17@test.com	user test		×	0

Note: The 2FA Enrollment Status for all users within a tenant will stay unchanged after clicking the **Clear all users** remembered devices button.

To unenroll a particular user or multiple users

- **1** Log into VSA with the corresponding permissions.
- 2 Navigate to System > Server Management> Logon Policy page.
- 3 Click the **Remove user(s) from 2FA Enrollment** button.

VSA Q Search fo	r machines	() D 👷 🛃 🖕 15 () 39 🔺 🥐 😝 TWteam 👻 Ҟ			
Search Navigation	🛄 Update					
	Specify the bad logon attempt policy		A			
🔅 System	Number of consecutive failed logon attempts allowed be	fore disabling account: 3				
 User Settings 	Length of time to disable account after max logon failure	s exceeded: 1 Hour 🛩				
Preferences	Minutes of inactivity before a user session expires	30 minutes				
Change Logon	Prevent anyone from changing their logon name					
↑ System Preferences	Do not show domain on logon page					
Check-in Policy	Do not show remember me checkbox on logon					
Naming Policy	Specify password strength policy					
 User Security 	Require password change every	0 days				
Lisers	Find the second	6 characters				
Liser Poles	Prohibit password reuse for	0 passwords				
Marking Dates	Require upper and lower case alpha characters					
Plachine Roles	Require both alpha and numeric characters					
scopes	Require non-liphanumetic characters					
Logon Hours	- Two Factor Authentication Settings					
User History	All administrators are required to use 2EA	Remove user(s) from 7E5 expollment				
Notification Policy						
 Orgs/Groups/Depts/Staff 	How long should devices be remembered?	30 Days 🗙 Clear all users remembered de Unevcoll single or multiple users from 2FA				
Manage		Enrollment participation: 1.92 %				
Set-up Types	Required User Name Name	Frontiment Status Remembered Devices				
 Server Management 	auto0@test.com user test		*			
Configure	auto1@test.com user test	× •				
Default Settings	auto10@test.com user test	× 0				
License Manager	auto11@test.com user test					
Import Center	auto12@test.com user test	× •				
System Log	auto13@test.com user test					
Statistics	auto14@test.com user test					
Logon Policy	auto15@test.com user test	× 0				
Application Logging	auto16@test.com user test	× 0				
Outbound Email	auto17@test.com user test	× 0	-			

4 Select user(s) you would like to reset 2FA enrollment for.

C. Section Lengthange Revision Provide Revision Provide United Instance Instance Provide Provid	VSA Q Search			
Name yeaky Serve Have the adve manual serve have a serve have the adve status yeak and the serve have the adve status ye		Update		
 Jes Gauly Jes Gauly Jes Gauly (and called up due table state state) (and the state) (and the state state)	Naming Policy	Specify the bad logon attempt policy		
Uns Long the shore s	 User Security 	Number of consecutive failed logon attempts allowed before disabling account:		
Unr folde Mained with solution that solution to state a solution to solutio solution to solutio solution to solution to solution to solution		Length of time to disable account after max logon failures exceeded:	Hour	
 Protection <		Minutes of inactivity before a user session expires	Remove User(s) from 2FA Enrollment	
In Critical Actions In Critical Actions (Depart (Section (Depa		Prevent anyone from changing their logon name		
Seriest Cost down remember me detabling in thights: Cost down remember me detabling in thights: Seriest Hategement Cost down at makes: Cost down at makes: Co		Do not show domain on logon page		
Light Nors Werk Jassend Hengin pair/ Defayl Seasend Hengin pair/ Defayl Seasend Hengin bala/		Do not show remember me checkbox on logon	Select users to remove from 2FA enrollment.	
User Natary Import Party Staff • Org/Scoreg/Optph/Staff Import Party Staff Marage Import Party Staff Server Management Import Party Staff Optph/Staff Import Party Staff Server Management Import Party Staff Default Settings Import Party Staff Lineue Management Import Party Staff Justifiers Import Party Staff Staffiers Import Party Staff St	Logon Hours	- Specify password strength policy		
 Org/ Occus/ Deput/ Staff Accuse Server Maagement Configure Server Maagement Configure Configure	User History	Dequire assword channe every	V User Name	
Marge Marge Beter Marge Colligie Colligie Colligie Colligie Colligie Astrinistic durations derives of a softward to astring Colligie Colligie Colligie Astrinistic durations Static Colligie Astrinistic durations Static Colligie Colligie <t< td=""><td> Orgs/Groups/Depts/Staff </td><td>Require password change every</td><td>V kadmin</td><td></td></t<>	 Orgs/Groups/Depts/Staff 	Require password change every	V kadmin	
Server Management Report goop and borr case alpha charactes Report charactes	Manage	Prohibit password reuse for		
 Berver Management Geolupical de la d	Set-up Types	Require upper and lower case alpha characters		
<pre>configre configre character cha</pre>	 Server Management 	Require both alpha and numeric characters		
Defaults straigs License Manager License Manager License Manager License Manager Jataministrator required to use 25A Batoministrator required to use 25A Staticist Staticist Staticist Application Loging Cottoming Statistict	Configure	Require non-alphanumeric characters		
Learce Marger Ligence				
A privation long and a second	Licenze Manader	Two Factor Authentication Settings		
Application Bysim Building Building Building Application Outbound finali Outbound finali Outbound finali Outbound finali Building Color Scheme Sile Cutomisation Sile Cutomisation<	Transi Gardan	All administrators required to use 2FA		
Badina Logi Encomment participation Statistics Encomment participation Application Loging Request Application Loging Request Outbound Email Remove Statistics Remove Statistics Remove Statistics Remove Statistics Remove Statistics Remove Statistics Remove	Import Center	How long should devices be remembered? 30 Days		
Applications Request Losen Nations Application Logging Request Losen Nations Request	System Log			
Lagon Palary Pagund User Name Application Laging International set in the set in	Statistics	Enrollment participation	X	
Application Logging k domin Obtaind Email is address Obtaind Email is address Obtaind Email is address Storage Configuration is address Cotor Scheme is address Storage Catternization is address Storage Catternization is address Star Gate Sternige is address	Logon Policy	Required User Name Name		
Outbound Email Outbound Email Outbound Email Starse Configuration Color Scheme Ste Customization Ste Customization Leal Settings	Application Logging	E kadmin		
Okubo Clients Remove Cancel Storge Configuration Remove Cancel Color Scheme Stor Scheme Stor Scheme Stor Scheme Lead Settings Lead Settings	Outbound Email			
Storage Configuration Remove Cancel * Costomize Color Scheme Sine Customization Sine Customization Sine Settings Sine Settings Sine Customization Sine Customization	OAuth Clients			
Customize Color Scheme Site Customization Loss Bettings	Storage Configuration		Remove Cancel	
Color Scheme Site Customication Local Settings	▲ Customize			
Site Outstomication Local Settings	Color Scheme			
Local Settings				
	Line Connect			

5 Receive unenrollment confirmation for the select user(s).

🦄 Kaseya	Q Search for machines	(Ö 🕒 🔤 😾 🚟 🌍 2 🌑 2 🗍 🤽 🥹 stephen.blanchard@kacsyn.com 👻 🔣
🗮 🔍 Search Navigatio	Update Update	
 System User Settings Preferences Change Logon System Preferences Check-in Policy 	Specify the bad logon attemp policy Number of consecutive failed logon attempts allowed before Length of time to dealer activation attem max logon failure are Minuses of inactivity before surver setsion explore Prevent anyone fram changing their logon name Do not show remember me checkbox on logon	Xing account:
Naming Policy * User Security Users User Roles Machine Roles Scopes Logon Hours User History Notification Policy	Specify password strength policy Require password thronge every Enforce minimum password length Public password rever for Require uper and lower case splits characters Require both alpha and numeric characters Require to monipharumeric characters Madi Factor Authentication Settings Al administrators required to use 2FA	days dharacters passwords V 1 use(s) were removed from MFA Envolment:
Orgs/Groups/Depts/St Manage Set-up Types Set-up Types Set-up Types Set-up Types Default Settings License Manager Import Center System Log Statistics Legen Policy Legen Policy Outboard Email Outboard Email Outboard Email Outboard Email	How long should devices be remembered? Required User Name Name Ø bill scrivt/gkaseys.com Bill Scrivt Ø bill scrivt/gkaseys.com Bill Scrivt Ø demo demo demo Ø demo demo demo demo Ø kadmin estrofen: blanchard@kaseys.com Bill Scrivt Scrivt Ø test/nen: blanchard@kaseys.com Strofen: blanchard@kaseys.com Bill Scrivt Scrivt Ø test/nen: blanchard@kaseys.com Strofen: blanchard@kaseys.com	Contrast a laters Bernember Me settings Eventment Status Remember of Davids C 1 C 2 C 0 C 0 C 0 C 0 C 0 C 0

Note: Users removed from the 2FA Enrollment will have to complete the 2FA enrollment process next time they log into the VSA.