



---

# User Administration

---

**Quick Start Guide**

Version R95

English

August 19, 2021

## **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



# Contents

<b>Organizations</b> .....	<b>i</b>
<b>Scopes</b> .....	<b>i</b>
<b>User Roles</b> .....	<b>iii</b>
<b>Machine Roles</b> .....	<b>iii</b>
<b>Users</b> .....	<b>iv</b>
<b>Create a New Master User</b> .....	<b>iv</b>
<b>Sharing User-Owned Objects</b> .....	<b>v</b>
<b>VSA Logon Policies</b> .....	<b>vi</b>
<b>Preferences</b> .....	<b>vii</b>
<b>Change Logon</b> .....	<b>ix</b>
<b>Logon Policy</b> .....	<b>ix</b>
<b>Logon Hours</b> .....	<b>xviii</b>
<b>Logon Page</b> .....	<b>xix</b>
<b>System and User Logs</b> .....	<b>xix</b>
<b>Learning More</b> .....	<b>xxi</b>
<b>Index</b> .....	<b>23</b>



---

# Organizations

Typically an organization is a customer, but an organization could also be a business partner. Most user defined objects in the VSA belong to an organization. Every managed machine, managed device and VSA user belongs to an organization. They are optionally associated with scopes, tickets and service desks.

## Organizations and Managed Machines

Each agent installed on a managed machine is assigned a unique **machine ID / group ID / organization ID**. All machine IDs belong to a machine group ID and optionally a subgroup ID. All machine group IDs belong to an organization ID. An organization typically represents a single customer account. If an organization is small, it may have only one machine group containing all the machine IDs in that organization. A larger organization may have many machine groups and subgroups, usually organized by location or network. For example, the full identifier for an agent installed on a managed machine could be defined as `jsmith.sales.chicago.acme`. In this case `sales` is a subgroup ID within the `chicago` group ID within the organization ID called `acme`. In some places in the VSA, this hierarchy is displayed in reverse order. Each organization ID has a single default machine group ID called `root`. Group IDs and subgroup IDs are created using the System > Orgs/Group/Depts/Staff > Manage > Machine Groups page.

## Pre-Defined Organizations

Three pre-defined organizations are provided:

- `myOrg` is the organization of the service provider using the VSA. All other organizations in the VSA are second party organizations doing business with `myOrg`. The default name of `myOrg`, called `My Organization`, should be renamed to match the service provider's company or organization name. *This name displays at the top of various reports to brand the report.* Agents installed to internally managed machines can be assigned to this organization. *VSA user logons are typically associated with staff records in the `myOrg` organization.* `myOrg` cannot be assigned a parent organization.
- `Kserver` is the org assigned to agents installed on your Kaseya Server. This makes it easy to apply specialized settings to the Kaseya Server, which is typically maintained differently from other agent managed machines.
- `Unnamed` is the default organization to assign an agent. Maintaining multiple agent install packages in Agent > Manage Packages, one for each organization, can be time consuming. Instead some server providers use a single agent package for the unnamed organization and perform all installs using this package. System > Naming Policy can reassign new agents to the correct organization.group ID automatically—the first time the agents check in—based on each managed machine's IP or connection gateway. Agent > Copy Settings may be used afterwards, to manually copy specific kinds of agent settings by machine ID template to the type of machine revealed by the initial audit.

---

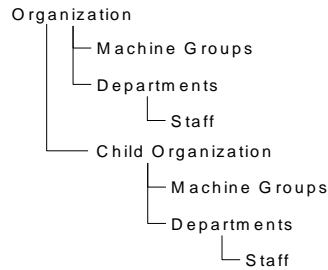
# Scopes

## Scope Data Objects

There are six types of data objects that can be assigned to scopes. Each are defined outside of scopes before being assigned to scopes.

- **Members** - Assign users to the selected scope.
- **Organizations** - An organization is typically a customer but not necessarily only customers. An organization record contains certain general information, such as its name and address, number

of employees and website. An organization also defines a hierarchy of additional information, as illustrated below, representing all the machine groups and personnel within that organization. Organizations are defined using System > Orgs/Groups/Depts/Staff > Manage.



- **Machine Groups** - Machine groups are groups of managed machines within an organization. Machine Groups are defined using System > Orgs/Groups/Depts/Staff > Manage > Machine Groups.
- **Machines** - A managed machine is a computer with an agent installed on it. Each machine has to belong to a machine group. Machines are typically created using the Agents > **Manage Packages** page.
- **Departments** - A department is a group of staff members within an organization. A staff member is not necessarily the same as a machine user. Departments and staff members are defined using System > Orgs/Groups/Depts/Staff > Manage > Departments.
- **Service Desk** - A service desk processes tickets using the **Service Desk** module. Service desks are defined using Service Desk > Desk Configuration > Desk Definition.

## Scopes

The **Scopes** page defines *visibility* of certain types of user-defined data objects throughout the VSA. For example, a user could see some machine groups, but not be able to see other machine groups. Once a scope has made a data object visible to a user, the functions the user can perform on that data object are determined by user role. Scopes enables VSA users responsible for user security to create different scopes of data objects and assign them to different populations of users.

**Note:** A user logs on with both an assigned role (the functions they can perform) and an assigned scope (the data they can see). Membership in a role and membership in a scope are independent of each other.

## Scope Assignment

The parent-child relationships between data structures affect how scopes are maintained.

### *Implicit Assignment*

Assigning any parent record to a scope *implicitly* assigns all child records to that same scope. For example, assigning an organization to a scope includes the following in that same scope:

- Child organizations.
- Machine groups of the organization and any child organizations.
- Machines of the machine groups in that organization and any child organizations.
- Departments in the organization and any child organizations.

### *Explicit Assignment*

The only way to include a top level organization in a scope is to manually add it to that scope, because no parent record exists to include it. This is called explicit assignment. You can also explicitly assign a lower level object in scope, *but only if the lower level object is not already assigned implicitly to the scope through its parent*. For example, you could include a machine group explicitly, without adding the machine group's parent organization. You can also explicitly include individual machines and departments in a scope without including their parent records.



The **Scopes** function provides an **All in Scope** button, when appropriate. The button displays a window that lists all records in a particular Scope tab, regardless of whether records are assigned implicitly or explicitly.

---

## User Roles

User roles determine what functions a *user* can access.

### Role Types

Kaseya licensing is purchased by role type. There are separate role types for licensing users by *user role type* and licensing machines by *machine role type*. Each role type enables selected functions listed in the User Roles > Access Rights tab and Machine Roles > Access Rights tab. The number of role type licenses purchased displays in the System > License Manager > Role Type tab. Each role type license specifies the number of *named users* and *concurrent users* allowed.

### User Roles Types

Every user role must be assigned to at least one user role type. If a user role is assigned to more than one role type, access to a function is enabled if any one of the role types enables access to that function. Function access can be optionally limited further by user role or machine role. Examples of user role types include, but are not limited to:

- **VSA Admin** - Includes both master users and standard users.
- **End Users** - Provides limited access to selected functions in the VSA. Primarily intended for customers of service providers. Customers can logon to the VSA and print reports or look at tickets about their own organizations.
- **Service Desk Technician** - Can edit **Service Desk** tickets and run reports, but not configure service desks, support tables or service desk procedures.
- **Service Desk Admin** - Can do anything in **Service Desk**.
- Additional SaaS user role types are defined and depend on the bundle purchased.

---

## Machine Roles

### Machine Roles

The **Machine Roles** page creates and deletes machine roles. The user access window displays when a *machine user double-clicks the agent icon in the system tray of their managed machine*.

Within the **Machine Roles** page you can select:

- **Members** - Assign or remove machines for a machine role.
- **Access Rights** - Select the access rights for a machine role. Access rights determine the functions a *machine user* can access.

**Role Types** - Assign or remove role types for a machine role. Currently there is only one machine role type provided and no access rights are restricted.

### The Default Machine Role

**A predefined Default machine role is provided when the VSA is installed. Newly created machine ID accounts are automatically assigned to the Default machine role when the account is created. If you create other machine roles, you can re-assign machine ID accounts to these other machine roles. You might want to do this if you want to limit machine user access to**

functions on the [Portal Access](#) page for different populations of machine users. Each machine ID account can only belong to a single machine role.

### Machine Role Types

Kaseya licensing is purchased by role type. There are separate role types for licensing users by *user role type* and licensing machines by *machine role type*. Each role type enables selected functions listed in the **User Roles > Access Rights** tab and **Machine Roles > Access Rights** tab. The number of role type licenses purchased displays in the **System > License Manager > Role Type** tab. Each role type license specifies the number of *named users* and *concurrent users* allowed.

Every machine role must be assigned to a machine role type. *For the initial release of Kaseya 2, there is only one machine role type.* The machine role type determines the type of *machine-based-license* to apply to machines included in a machine role. For example, if you create a machine role called **StdMach** and assign **StdMach** to the machine role type called **Basic Machine**—and there are 150 machines in the **StdMach** machine role—then the **System > License Manager** shows 150 of the total number of **Basic Machine** licenses used.

---

## Users

Each user must be assigned at least one role and one scope. You can assign multiple roles and scopes to a user, but *only one role and one scope is active at any one time*. The active role and scope are selected using the **Role** and **Scope** drop-down lists in the top-right corner of the page. You can reset the user's password, enable/disable user logons and log off users if you have access to these functions.

### Master Users vs Standard Users

A master user is a VSA user that uses a **Master** user role and a **Master** scope. The **Master** user role provides user access to all functions throughout the VSA. The **Master** scope provides access to all scope data objects throughout the VSA. A **Master** user role can be used with a non-**Master** scope, but a **Master** scope cannot be used with a non-**Master** role. Kaseya Server management configuration and other specialized functions can only be performed by **Master** role users. The term *standard user* is sometimes used to indicate a user that does not use a **Master** user role and a **Master** scope.

---

## Create a New Master User

### Forgotten User Password

If you have forgotten your master user account password, the system provides a way for you to create a new master user account or reset just the password of an existing master user account. This enables you to log back in to the system and retrieve the forgotten account information. A master user is a VSA user that uses a **Master** user role and a **Master** scope.

**Note:** You must have administrator privileges on the Kaseya Server. Due to security reasons, you cannot perform the following procedure remotely.

### Creating a New Master User Account

1. Log in to the machine running the Kaseya Server.

2. Access the following web page:  
`http://localhost/LocalAuth/setAccount.aspx`
3. Enter a new account name in the **Master User Name** field.
4. Enter a password in the **Enter Password** field and confirm it by re-typing it in the **Confirm Password** field.
5. Enter an email address in the **Email Address**.
6. Click **Create**.

You can now log on to the system using the new master user account.

### Reset the Password of an Existing Master User Account

**Note:** The master user account cannot be disabled.

1. Log in to the machine running the Kaseya Server.
2. Access the following web page:  
`http://localhost/LocalAuth/setAccount.aspx`
3. Enter an existing, enabled master account user name in the **Master User Name** field.
4. Enter a password in the **Enter Password** field and confirm it by re-typing it in the **Confirm Password** field.
5. Skip the **Email Address**. You cannot reset the email address of an existing user using this web page.
6. Click **Create**.

You can now log on to the system using the existing master user account.

---

## Sharing User-Owned Objects

Each user has the ability to create user-owned objects—such as filtered views, reports, procedures, or monitor sets. Typically these objects start out as private objects. As a private object no other user can see them or use them. These user-owned objects can be shared with other *user roles* or with individual *users*. In some cases, a **Master** role user can make a user-defined object public for all users. Share options can include the right to use an object, edit, export, delete, or share an object with additional users. Share rights are set by each individual object separately. You can elect to share a user-owned object with:

- Any user roles you are a member of, whether you are currently using that user role or not.
- Any individual users that are members of your current scope.

If share rights for an object are granted by both user role and individual user, share rights are added to one another.

Typically a **Share** button displays on any page or dialog that edits a user-owned object. Individual **Share** buttons sometimes display next to each user-owned object in a list.

Examples of user-owned objects in the VSA are:

- View Definitions
- Manage Packages install packages
- Monitoring Dashlets
- Agent Procedures folders
- Service Desk Procedures folders
- Monitor Sets folders
- SNMP Sets folders
- Reports folders

- Report Sets folders
- **Service Desk** ticket named filters

**Note:** Folder trees have specialized rules about how folders are shared. See [Agent Procedures > Schedule/Create > Folder Rights](#) in online user assistance for details.

## Sharing Options

- Adding a user or user role to the **Shared Pane** allows that user to use that object. No additional rights have to be assigned to the user or user role to use that object.
- Checking any *additional rights*—such as **Edit**, **Create**, **Delete**, **Rename**, or **Share**—when you *add* the user or user role, provides that user or user role with those additional rights. You have to remove the user or user role and re-add them to make changes to their additional rights.
- **Share** means the users or user roles can assign share rights.

### Legacy Share Options

Certain functions in the VSA still set sharing rights using a legacy dialog as follows:

- Share rights are assigned *by object*. There are three sharing checkbox options. The first two checkboxes are *mutually exclusive* and determine what share rights are assigned. If neither of the first two checkboxes are checked, the shared object can only be seen by the users given share access, but the object cannot be used nor edited. The **Shared** and **Not Shared** list boxes and the third checkbox determine who can see the object.
  - **Allow other administrators to modify** - If checked, share rights to the object includes being able to use it, view its details and edit it.
  - **Other administrators may use but may not view or edit** - If checked, share rights to the object only allows using it.
  - **Make public (seen by all administrators)** - If checked, ensures that *all* current and future VSA users can see the object. If blank, only selected user roles and users can see the shared object. If blank, and new users or user roles are added later, you have to return to this dialog to enable them to see the specific object.

---

# VSA Logon Policies

Once a VSA user is defined in System > User Security, a number of functions manage when and how users can logon and the features that are available to them during logon.

VSA user logon options are specified using:

- System > Users - Optionally reset the user's password, or force the user to change his or her password, or enable/disable the user's logon or log a user off.
- System > **Preferences** (*page vii*) - The **Preferences** page sets preference options that typically apply *only to the currently logged in* user.
- System > **Change Logons** (*page ix*) - The **Change Logon** page sets your VSA logon username and password. These preference options apply *only to the currently logged on* user.
- System > **Logon Policy** (*page ix*) - The **Logon Policy** page sets logon policies that apply to all VSA users.
- System > **Logon Hours** (*page xviii*) - The **Logon Hours** page determines *when* users can logon to the VSA by specifying the weekdays and hours for each user role. Each day of the week can have different hours of operation set.
- System > Site Customization > Logon Page - Set options that display on the logon page.
- System > Site Customization > Site Header - Set options that display on the logon page.

**Note:** Additional logon options *for machine users only* are set in Agent > Portal Access.

Organizations.....	i
Scopes.....	i
User Roles.....	iii
Machine Roles.....	iii
Users.....	iv
Create a New Master User.....	iv
Sharing User-Owned Objects.....	v
VSA Logon Policies.....	vi
Preferences.....	vii
Change Logon.....	ix
Logon Policy.....	ix
Logon Hours.....	xviii
Logon Page.....	xix
System and User Logs.....	xix
Learning More.....	xxi
Index.....	23

### In This Section

Preferences	vii
Change Logon	ix
Logon Policy	ix
Logon Hours	xviii
Logon Page	xix

---



## Preferences

System > User Settings > Preferences



The **Preferences** page sets system-wide preferences that apply *only to the currently logged on user*.

**Note:** Three options on this page apply to *all users* and only display for master role users: setting the System Default Language Preference and the Download button for installing language packs, and Show shared and private folder contents from all users.

**Note:** See **VSA Logon Policies** (page vi) for a summary of functions affecting user logons.

- **Set email address to deliver messages for this administrator to** - Specifies the email address that alerts, ticket notifications and other email messages will be sent to. After entering the email address, click **Apply** to make it active. Previously set alerts retain the original email recipient addresses specified when the alerts were set.
- **Set first function after logon** - Select the name of the function you want to see when you first log on to the Kaseya Server.
- **Use Compact Navigation** - If checked, spacing is reduced between items on the navigation panel. Changes take effect after the next logon.
- **Set delay before displaying detail information when hovering over information icon**  - An  information icon displays for each ticket row in Ticketing > View Summary and Service Desk >

**Tickets** (<http://help.kaseya.com/webhelp/EN/KSD/9050000/index.asp#3646.htm>). Hovering the cursor over the icon displays a preview of the ticket. Specify the number of milliseconds to wait before the ticket preview window displays, then click the **Apply** button. Click the **Default** button to set this value back to its default.

- **Set delay before displaying detail information when hovering over agent icon**  - An agent check-in icon, for example , displays next to each machine ID account in the VSA. Hovering the cursor over the icon displays an agent Quick View window. Specify the number of milliseconds to wait before the agent Quick View window displays, then click the **Apply** button. Click the **Default** button to set this value back to its default.
- **Select time zone offset** - Select one of the following time zone offset options, then click **Apply**. See Scheduling and Daylight Savings Time.
  - **Use time zone of the browser logging into the system**
  - **Use time zone of the VSA server** - The time currently shown by your VSA browser displays next to this option.
  - **Use fixed offset from the VSA server <N> hours**

**Note:** Date format is set in System > Configure.

**Note:** Time Zone Offset applies only to time/date formatted columns or fields in the VSA user interface. It is not applied where a date/time value appears within text based content such as a log message or alert body.

- **Set up language preferences**
  - **My language preference is** - Select the language you prefer displayed when you're logged into the VSA. The languages available depend on the language packages installed.
  - **System default language preference is** - Select the default language used by the VSA user interface for all users. The languages available depend on the language packages installed. This option only displays for master role users.
  - **Download a Language Package** - Display a dialog box that enables you to download and install language packages. A language package enables the VSA user interface to be displayed in that language. This option only displays for master role users.
- **Show shared and private folder contents from all users - Master Admin Only** - If checked, a master role user has visibility of all shared and private folders. For private folders only, checking this box provides the master role user with all access rights, equivalent to an owner.
- **Select display format for long names** - The web pages are designed to display well for typical string sizes. Occasionally data fields contain long names that will not display properly on the web pages. You can specify how long names display as follows:
  - **Limit names for better page layout** - This setting limits the string size to fit well on the web page. Strings exceeding a maximum length are limited with a ... To view the entire name, hover the mouse over the string and a tool tip pops up showing the entire name.
  - **Allow long name wrapping** - Long strings are allowed to wrap within the web page. This may disturb the normal web page layout and names may wrap at any character position.
- **Clear Snooze** - Clears all outstanding task notification messages. Task notification messages are generated for tasks that are assigned to you and for tasks that are past due. Tasks are defined using the Info Center > View Dashboard page.
- **Defaults** - Resets all settings to system defaults for this user.

---

# Change Logon

System > User Settings > Change Logon

The **Change Logon** page sets your VSA logon username and password. These preference options apply *only to the currently logged on user*.

**Note:** See **VSA Logon Policies** (page vi) for a summary of functions affecting user logons.

## Changing Your VSA Logon Name and/or Password

To change your logon name and password:

1. Enter a new name in the **Username** field.

**Note:** The **Username** field cannot be edited if **Prevent anyone from changing their logon** is checked in **System > Logon Policy**.

2. Enter your old password in the **Old Password** field.
3. Enter a new password in the **New Password** field. Passwords are case-sensitive.  
If you would like the system to generate a strong password for you, click **Suggest**. A dialog box displays showing the new password; the new password is automatically entered in the **New Password** and **Confirm Password** fields. Be sure to write it down before clicking OK and closing the dialog box.
4. Confirm the password by re-typing it in the **Confirm Password** field.
5. Enter a **Security Question** and **Security Answer**. This enables you to request a new password if you forget your password.

Clicking the **Forgot Password?** link on the logon page—if activated using the System > Site Customization > Logon Page tab—emails you a link where you can change your password. To change your password, you must have already filled out a **Security Question** and **Security Answer** using System > **Change Logon** (page ix).

6. Click **Change**.

**Note:** The **Discovery** add-on module can be used to manage VSA user logons and Portal Access logons using **domain logons** (<http://help.kaseya.com/webhelp/EN/KDIS/9050000/index.asp#7293.htm>).

---

# Logon Policy

System > Server Management > Logon Policy

The **Logon Policy** page sets logon policies that apply to all VSA users. Logon policies prevent a brute force break-in to the system. By limiting the successive number of bad logon attempts and disabling rogue accounts for a set amount of time, you can prevent unauthorized access achieved by repeatedly entering random passwords.

**Note:** See **VSA Logon Policies** (page vi) for a summary of functions affecting user logons.

## Specify the bad logon attempt policy

- **Number of consecutive failed logon attempts allowed before disabling** - Specify the number of consecutive bad logons a VSA user or Portal Access user is allowed before their account is disabled in the **account** field. The count is reset to zero after a successful logon.
- **Length of time to disable account after max logon failures exceeded** - Specify the amount of time, in hours or days, that the account is disabled in the **field**.



**Note:** To activate the account manually before the lockout time elapses, another user must enable the account using the System > Users page.

- **Minutes of inactivity before a user session expires** - Specify the time period of user inactivity before the user is automatically logged out. Set the number of minutes of inactivity in the field.
- **Prevent anyone from changing their logon name** - Prevent anyone from changing their logon name.
- **Do not show domain on logon page** - Hide the **Domain** field on the logon page.

**Note:** If left blank, the domain checkbox still does not show on the logon page until at least one domain logon exists. Domain logons can be added using Discovery > **Domain Watch** (<http://help.kaseya.com/webhelp/EN/KDIS/9050000/index.asp#10750.htm>).

- **Do not show remember me checkbox on logon** - Hide the **Remember my username on this computer** checkbox on the logon page.

### Specify password strength policy

Applies to VSA-authenticated passwords only. Domain-authenticated passwords are not affected by these policies.

- Require password change every N days. Require password change cannot be more than 30 days.
- Enforce minimum password length. Enforce minimum password length cannot be less than 16 characters.
- Prohibit password reuse for N passwords. Prohibit password reuse be less than 5 passwords.
- Require upper and lower case alpha characters.
- Require both alpha and numeric characters.
- Require non-alphanumeric characters.

### IT Complete Single Sign-On Integration

Upon using the VSA for the first time after installing or patching the system, the VSA will be enabled for use with IT Complete.

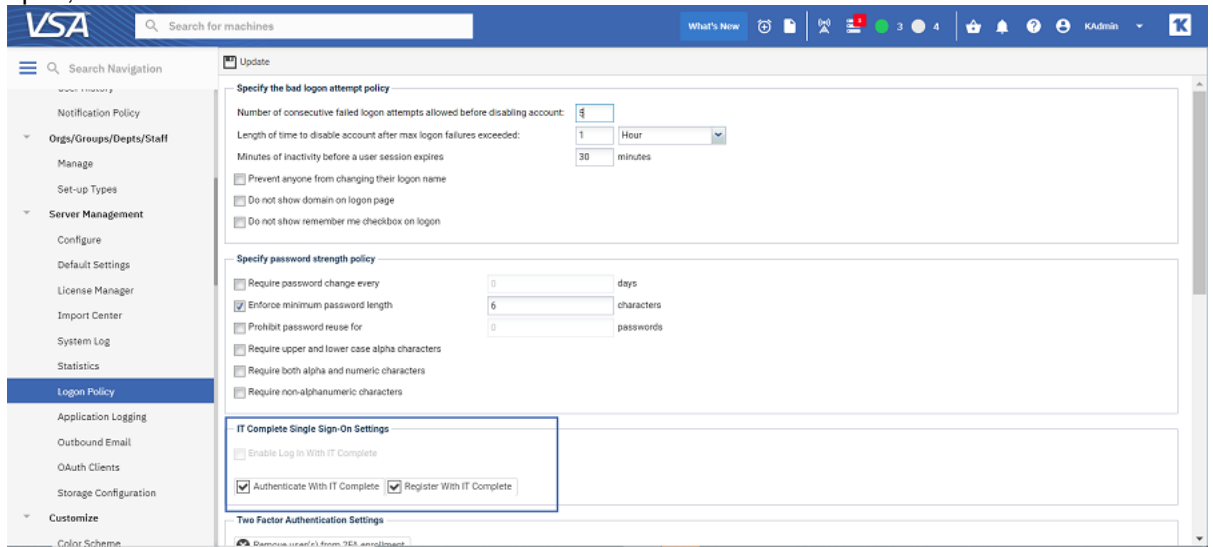
**For VSA On-Premise servers, VSA will need to be registered with IT Complete. For SaaS servers, the server registration process will be performed by Kaseya.**

**To register on On-Premise VSA per entire VSA server and within a single K1 company,** a Master Admin must authenticate to IT Complete with a prompt to complete the Kaseya One authentication process:

1. Log into the VSA as a Master Admin;



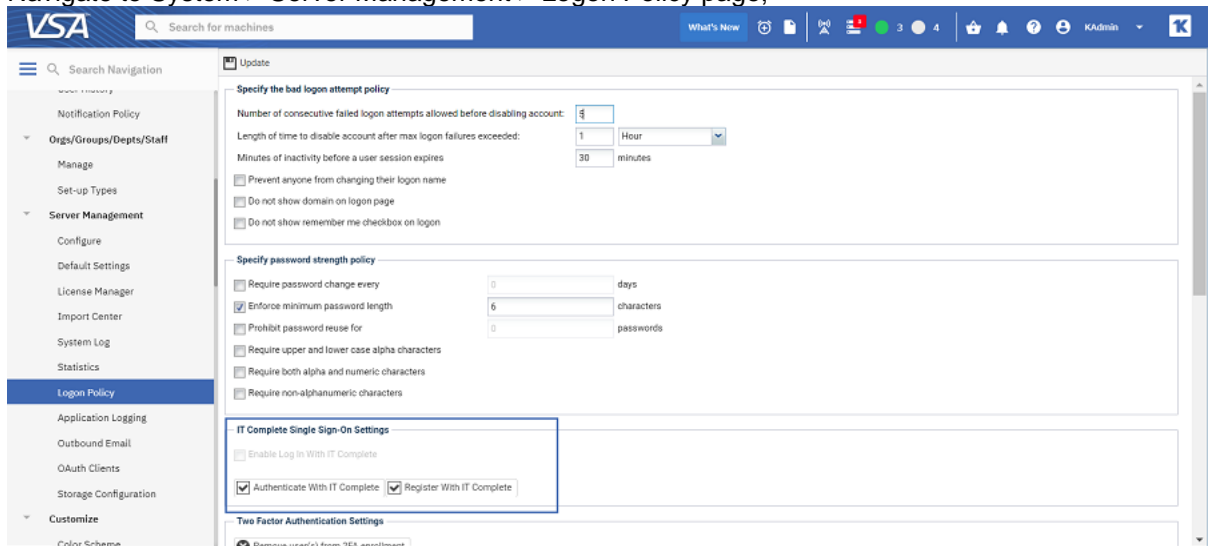
2. Navigate to System > Server Management > **Logon Policy** page;
3. Click the **Authenticate with IT Complete** button. The new window with Kaseya One login page will open;



4. Login to your Kaseya One account. Once you authenticate with Kaseya One, you can continue with the VSA registration process;
5. Click the **Register VSA with IT Complete** button;
6. Log out of your VSA account – VSA user accounts can now be associated with Kaseya One accounts.

**To register on On-Premise VSA per multiple VSA servers or with multiple K1 companies**, a tenant System user must authenticate to IT Complete with a prompt to complete the Kaseya One authentication process:

1. Log in as a System user;
2. Navigate to System > Server Management > Logon Policy page;



3. Click the **Authenticate with IT Complete** button. The new window with Kaseya One login page will open;
4. Login to your Kaseya One account. Once you authenticate with Kaseya One, you can continue with the VSA registration process;
5. Click the **Register VSA with IT Complete** button;
6. Check the **Enable Log in With IT Complete** checkbox, and click the **Update** button;

### Now your VSA account is registered with an IT Complete account.

For all VSA customers:

#### To register VSA user accounts with IT Complete (Kaseya One) accounts from the VSA Login page.

1. Select the Login with IT Complete option on the login page, to associate your VSA account with an IT Complete account;



2. Enter your IT Complete credential;



3. Enter your VSA account credential;



### Now your VSA account is registered with an IT Complete account.

To register VSA user accounts with IT Complete accounts from the VSA UI:

1. Click your VSA user logon name in the upper right-hand corner of the VSA to display your User menu;
2. Click the **Enable Log In With IT Complete** option.

**Now your VSA account and IT Complete are associated.**

To remove association of your VSA account and IT Complete account:

1. Click your VSA user logon name in the upper right-hand corner of the VSA to display your User menu;
2. Click the **Disable Log In With IT Complete** option.

**Now your VSA account and IT Complete are disassociated.**

## Two Factor Authentication Settings

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.

The screenshot shows the VSA Logon Policy configuration page. The 'All administrators are required to use 2FA' checkbox is checked. Below, a table shows 17 users with 'Enrollment Status' marked as 'X' and 'Remembered Devices' as 0.

Required	User Name	Name	Enrollment Status	Remembered Devices
<input type="checkbox"/>	auto0@test.com	user test	X	0
<input type="checkbox"/>	auto1@test.com	user test	X	0
<input type="checkbox"/>	auto10@test.com	user test	X	0
<input type="checkbox"/>	auto11@test.com	user test	X	0
<input type="checkbox"/>	auto12@test.com	user test	X	0
<input type="checkbox"/>	auto13@test.com	user test	X	0
<input type="checkbox"/>	auto14@test.com	user test	X	0
<input type="checkbox"/>	auto15@test.com	user test	X	0
<input type="checkbox"/>	auto16@test.com	user test	X	0
<input type="checkbox"/>	auto17@test.com	user test	X	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.

The screenshot shows the VSA System Management interface. The left sidebar contains a navigation menu with categories like System, User Settings, System Preferences, User Security, Orgs/Groups/Depts/Staff, and Server Management. The 'Logon Policy' option is selected under Server Management. The main content area is titled 'Update' and contains three sections:

- Specify the bad logon attempt policy:** Includes fields for 'Number of consecutive failed logon attempts allowed before disabling account' (set to 3), 'Length of time to disable account after max logon failures exceeded' (set to 1 Hour), and 'Minutes of inactivity before a user session expires' (set to 10 minutes). There are also checkboxes for 'Prevent anyone from changing their logon name', 'Do not show domain on logon page', and 'Do not show remember me checkbox on logon'.
- Specify password strength policy:** Includes checkboxes for 'Require password change every' (set to 30 days), 'Enforce minimum password length' (set to 8 characters), 'Prohibit password reuse for' (set to 0 passwords), 'Require upper and lower case alpha characters', 'Require both alpha and numeric characters', and 'Require non-alphanumeric characters'.
- Two Factor Authentication Settings:** Includes a checkbox for 'All administrators are required to use 2FA' (unchecked), a 'Remove user(s) from 2FA enrollment' button, and a dropdown for 'How long should devices be remembered?' (set to 30 Days). Below this is an 'Enrollment participation' bar showing 100% and a table of user enrollment status.

Required	User Name	Name	Enrollment Status	Remembered Devices
<input checked="" type="checkbox"/>	auto0@test.com	user test	✗	0
<input checked="" type="checkbox"/>	auto1@test.com	user test	✗	0
<input checked="" type="checkbox"/>	auto10@test.com	user test	✗	0
<input checked="" type="checkbox"/>	auto11@test.com	user test	✗	0
<input checked="" type="checkbox"/>	auto12@test.com	user test	✗	0
<input checked="" type="checkbox"/>	auto13@test.com	user test	✗	0
<input checked="" type="checkbox"/>	auto14@test.com	user test	✗	0
<input checked="" type="checkbox"/>	auto15@test.com	user test	✗	0
<input checked="" type="checkbox"/>	auto16@test.com	user test	✗	0
<input checked="" type="checkbox"/>	auto17@test.com	user test	✗	0

4. Save the changes.

**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.

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.
- ✓ - 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.

Required	User Name	Name	Enrollment Status	Remembered Devices
<input type="checkbox"/>	bd	bd user	✗	0
<input type="checkbox"/>	cecilia.osborn@kaseya.com	Cecilia Osborn	✗	0
<input type="checkbox"/>	daria.kovsharova@kaseya.coi	Daria Kovsharova	✓	0
<input type="checkbox"/>	kadmin		✓	0
<input type="checkbox"/>	kseniia	kseniia p	✓	0
<input type="checkbox"/>	sduser	sd user	✗	0
<input checked="" type="checkbox"/>	stephen.blanchard@kaseya.c	Stephen Blanchard	✓	1
<input type="checkbox"/>	Valentina.Pristavka@kaseya.c	Valentina Pristavka	✓	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:

1. By removing 2FA Remembered Devices for all users within a tenant.
2. By unenrolling a particular user or multiple users. This will also remove the user's remembered devices.

**Note:** Removing user's devices will not unenroll the User from 2FA. The user will have to enter a one-time password.

*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.

The screenshot shows the VSA System Settings interface. The left sidebar contains a navigation menu with categories like System, User Settings, System Preferences, User Security, Orgs/Groups/Depts/Staff, and Server Management. The 'Logon Policy' option is selected under System Management. The main content area is titled 'Update' and contains several sections: 'Specify the bad logon attempt policy', 'Specify password strength policy', and 'Two Factor Authentication Settings'. The 'Two Factor Authentication Settings' section shows 'All administrators are required to use 2FA' checked, 'Remove user(s) from 2FA enrollment' checked, and 'How long should devices be remembered?' set to '30 Days'. A blue button labeled 'Clear all users remembered devices' is highlighted. Below this, a table shows the enrollment status for various users.

Required	User Name	Name	Enrollment Status	Remembered Devices
<input type="checkbox"/>	auto0@test.com	user test	✗	0
<input type="checkbox"/>	auto1@test.com	user test	✗	0
<input type="checkbox"/>	auto10@test.com	user test	✗	0
<input type="checkbox"/>	auto11@test.com	user test	✗	0
<input type="checkbox"/>	auto12@test.com	user test	✗	0
<input type="checkbox"/>	auto13@test.com	user test	✗	0
<input type="checkbox"/>	auto14@test.com	user test	✗	0
<input type="checkbox"/>	auto15@test.com	user test	✗	0
<input type="checkbox"/>	auto16@test.com	user test	✗	0
<input type="checkbox"/>	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.

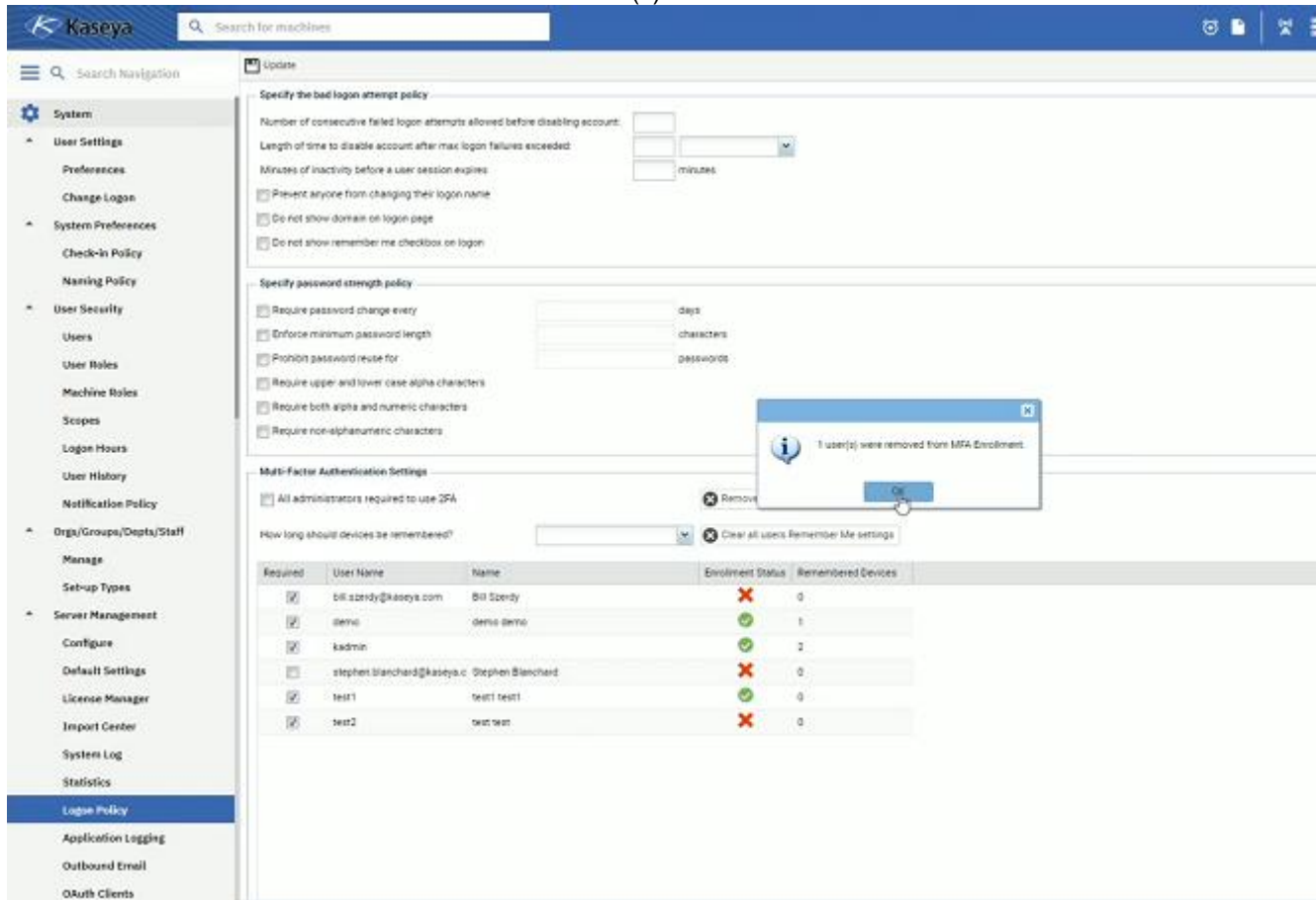
2. Navigate to System > Server Management > **Logon Policy** page.
3. Click the **Remove user(s) from 2FA Enrollment** button.

The screenshot displays the VSA (VeriSign Administrator) interface for configuring Logon Policy. The left sidebar shows the navigation menu with 'Logon Policy' selected under 'Server Management'. The main content area is divided into three sections:

- Specify the bad logon attempt policy:** Includes fields for 'Number of consecutive failed logon attempts allowed before disabling account' (set to 3), 'Length of time to disable account after max logon failures exceeded' (set to 1 hour), and 'Minutes of inactivity before a user session expires' (set to 30 minutes). There are also checkboxes for 'Prevent anyone from changing their logon name', 'Do not show domain on logon page', and 'Do not show remember me checkbox on logon'.
- Specify password strength policy:** Includes checkboxes for 'Require password change every' (0 days), 'Enforce minimum password length' (6 characters), 'Prohibit password reuse for' (1 password), 'Require upper and lower case alpha characters', 'Require both alpha and numeric characters', and 'Require non-alphanumeric characters'.
- Two Factor Authentication Settings:** Includes a checkbox for 'All administrators are required to use 2FA', a dropdown for 'How long should devices be remembered?' (set to 30 Days), and a button for 'Remove user(s) from 2FA enrollment'. Below this is a table showing enrollment participation (1.92%) and a list of users.

Required	User Name	Name	Enrollment Status	Remembered Devices
<input type="checkbox"/>	auto0@test.com	user test	✗	0
<input type="checkbox"/>	auto1@test.com	user test	✗	0
<input type="checkbox"/>	auto10@test.com	user test	✗	0
<input type="checkbox"/>	auto11@test.com	user test	✗	0
<input type="checkbox"/>	auto12@test.com	user test	✗	0
<input type="checkbox"/>	auto13@test.com	user test	✗	0
<input type="checkbox"/>	auto14@test.com	user test	✗	0
<input type="checkbox"/>	auto15@test.com	user test	✗	0
<input type="checkbox"/>	auto16@test.com	user test	✗	0
<input type="checkbox"/>	auto17@test.com	user test	✗	0

4. Select user(s) you would like to reset 2FA enrollment for.
5. Receive unenrollment confirmation for the select user(s).



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

**Note:** See Two-Factor Authentication topic to set up authenticator application.

### Update

Press **Update** to apply the settings.

## Logon Hours

System > User Security > Logon Hours

The **Logon Hours** page determines *when* users can logon to the VSA by specifying the weekdays and hours for each user role. Each day of the week can have different hours of operation set.

**Note:** See **VSA Logon Policies** (page vi) for a summary of functions affecting user logons.

### Select user role

Select a user role to display and maintain its logon hour settings.



## No Hours Restrictions

If checked, users can logon to the VSA at any time and day of the week. Uncheck to enable all other settings.

## Deny

Denies logon access for the entire weekday.

## or allow between <12:00 am> and <12:00 am>

Specify the range of time logons are allowed. All times are in the Kaseya Server's time zone. For all day access, set start and end time to the same time.

## Apply

Click to apply changes.

---

# Logon Page

The **Logon Page** tab of the **Site Customization** page sets the options displayed when a user logs on.

**Note:** See **VSA Logon Policies** (page vi) for a summary of functions affecting user logons.

1. Click the **Edit** button on the **Logon Page** tab. The **Edit Logon Page** dialog displays.
2. The following settings are all optional:
  - **Logo for Logon Page** - Browse to select a custom logon on your local machine or network. Click the **Use Default** button to reset back to the default.

**Note:** Your logo should be no larger than the recommended size.

- **Title** - Enter title text for this environment. The title displays just beneath the logo on the logon page. Click the **Use Default** button to reset back to the default.
- **Background Image** - Enter the path to a custom webpage. The path must be relative to the **Webpages** directory, or relative to the **Webpages\Access** directory, or a fully-formed URL. Click the **Use Default** button to reset back to the default.
- Standard information:
  - ✓ **Display Forgot Password on logon page** - If checked, a **Forgot Password?** hyperlink displays on the logon page. Clicking the **Forgot Password?** link on the logon page—if activated using the **System > Site Customization > Logon Page** tab—emails you a link where you can change your password. To change your password, you must have already filled out a **Security Question** and **Security Answer** using **System > Change Logon** (page ix).
  - ✓ **Display System Status on logon page** - If checked, the system status displays on the logon page.
  - ✓ **Display Customer ID on logon page** - If checked, the customer ID displays on the logon page.

---

# System and User Logs

Three logs in the **System** module track user-initiated events and system events.

- **User History** - Displays a history, in date order, of every function used by a user. The history also displays any actions captured by the System Log performed by the selected user. The system saves history data for each user for the number of days specified for the **System Log**.

- **System Log** - The **System Log** page logs events that cannot be tracked by machine ID, for a specified time period. *This log captures events not contained in any of the agent logs.*
- **Application Logging** - Controls the logging of application activity on the application server. This function is only visible to Master role users.

---

## Learning More

PDFs are available to help you quickstart your implementation of **Virtual System Administrator™**. They can be downloaded from the **first topic in the VSA online help** (<http://help.kaseya.com/webhelp/EN/VSA/9050000>).

If you're new to **Virtual System Administrator™** we recommend the following quickstart guides:

1. Getting Started
2. User Administration
3. Agent Configuration and Deployment
4. Live Connect, Kaseya Remote Control, Quick View, User Portal
5. Monitoring Configuration
6. Custom Reports

The following resources are also available.

### **Kaseya University**

---

See **Kaseya University** (<http://kuniversity.kaseya.com/>) for training options.



---

# Index

## C

Change Logon • ix  
Create a New Master User • iv

## D

Domain Logon • vii

## L

Learning More • xxi  
Logon Hours • xviii  
Logon Page • xix  
Logon Policy • ix

## M

Machine Roles • iii

## O

Organizations • i

## P

Preferences • vii

## S

Scopes • i  
Sharing User-Owned Objects • v  
System and User Logs • xix

## U

User Roles • iii  
Users • iv

## V

VSA Logon Policies • vi