Kaseya 2

User Administration

Quick Start Guide

for VSA 6.1

May 13, 2011

About Kaseya

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

Contents

User Security

System > User Security

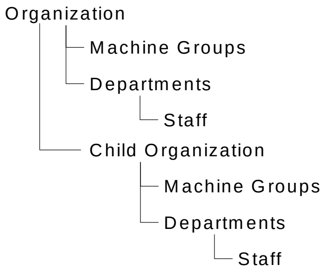
User Security determines the access users have to functions and data objects within the VSA. Understanding **User Security** configuration is easiest if you consider each of the following concepts in the order presented.

1. **Scope Data Objects** - *A* **data object** *is an object that* **you** *create and name.* An example of a data object is a machine group. Some data objects are significant enough to be managed by scopes. Scope level data objects are defined *first*, before being assigned to scopes. Scope data objects include organizations, machine groups, machines, departments and service desks.
2. **Scopes** - Sets of data objects that users have *visibility* of within the VSA.
3. **User Roles** - Sets of VSA functions that VSA users can perform. *A* **function** *acts on data objects.* Examples of functions are opening, adding, editing or deleting records.
4. **User Role Types** - Built-in classifications that determine the types of *user-role-based* licenses to apply to users in user roles.
5. **Machine Roles** - Sets of Portal Access functions that machine users can perform when displaying the VSA **Portal Access** page on their machine.
6. **Machine Role Types** - Built-in classifications that determines the type of *machine-role-based* licenses to apply to machines in a machine role.
7. **Users** - Refers to VSA users. Users of machines with agents on them are always identified as *machine users* to distinguish them from VSA users.

Scope Data Objects

For the initial release of Kaseya 2, there are five types of data objects that can be assigned to scopes. Each are defined outside of scopes before being assigned to scopes.

- **Organizations** - Organizations are a new type of record in Kaseya 2. 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. If you've worked with Kaseya 2008, then machine groups behave the same way in Kaseya 2. The only difference is that machine groups are defined by organization. Machine Groups are defined using System > Orgs/Groups/Depts > 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. You create them the same way they are created in Kaseya 2008, typically using the Agents > **Deploy Agents** function.
- **Departments** - Departments are a new type of record in Kaseya 2. A department is a division within an organization. Staff members of an organization are assigned to a department. Departments are defined using System > Orgs/Groups/Depts > Manage > Departments.

- **Service Desk** - A service desk is a new type of record in Kaseya 2. It defines all of the functionality required to process tickets using the new **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.

All in Scope

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. This is a more granular version of the **Function Access** function you used in Kaseya 2008.

> **Note:** In Kaseya 2008 a role determined both function access and machine group access. In Kaseya 2, access to functions (roles) and access to data objects (scopes) are defined independently from each other.

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. User role types include:

- **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**.

Kaseya SaaS user role types include:

- **IT Toolkit Free Admin** - Install agents, remote control and file manager with KLC, maintain users and machine groups.
- **IT Toolkit Free Admin** - Install agents, most KLC functions, maintain users and machine groups.
- **IT Workbench Admin** - Basic access to core options with no agent procedures or scripting.
- **IT Center Admin** - Similar to VSA Admin, no system tab access.

Machine Roles

The **Machine Roles** page controls access to the **Portal Access** window, which is a session of **Live Connect** provided specifically for *machine users*. The **Portal Access** window displays when a *machine user double-clicks the agent icon in the system tray of their managed machine.*

Machine Role Types

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.

- **Note:** See Master Users vs. Standard Users.

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, which 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 KServer. Due to security reasons, you cannot perform the following procedure remotely.

To create a new master user account:

1. Log in to the machine running the KServer.
2. Access the following web page:
   `http://localhost/LocalAuth/setAccount.asp`
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. Click **Create**.

You will now be logged in to the system as a new master user.

Changing the User Password

Change the user password for the original user logon using System > Users.

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
- Deploy Agent 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

Kaseya 2 Share Options

- Adding a user or user role to the **Shared Pane** allows that user to use that object. No additional rights, including **View**, have to be assigned to the user or user role to use that object.

- Checking any *additional rights*—such as **View**, **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.
- **View** *does not refer to being able to view the object.* **View** means the object's configuration can be viewed but not edited. If an export option is provided, **View** also enables the user to export the object.
- **Share** means the users or user roles can assign share rights.

Legacy Share Options

Certain functions in Kaseya 2 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.

Taking Ownership

When you first create a user-owned object, you are the owner of that object. A user-owned object can only be *owned* by one user at a time. The owner of an object always has "full rights" to that object.

Master role users have an additional right, called **Take Ownership**, that allows them to take ownership of any user-*shared* object. When a user-shared object is selected or edited by a master role user, a **Take Ownership** option displays. When ownership is taken, the new owner of that object now has "full rights" to the object.

Typically the reason you take ownership of a shared object is to maintain its contents because the original owner can't do so. For example, the owner of a shared object may have left the company and no longer be available. In most cases, master role users can work within the share rights they've been assigned by other VSA users.

> **Note:** Deleting a VSA user from the system assigns ownership of all objects belonging to that VSA user to the VSA user performing the delete.
>
> **Note:** A master role user can check the **Show shared and private folder contents from all users** in System > **Preferences** *(page 6)* to see 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.

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 6)* - The **Preferences** page sets preference options that typically apply *only to the currently logged in* user.
- System > **Change Logons** *(page 7)* - 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 9)* - The **Logon Policy** page sets logon policies that apply to all VSA users.
- System > **Logon Hours** *(page 9)* - 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.
>
> **Note:** See **Embedding the VSA Logon Form in Web Pages** *(page 11)*.

Preferences

System > Preferences

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

The **Preferences** page sets system-wide preferences that apply *only to the currently logged on* user. This includes the email address where you receive alert messages.

> **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 5)* 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 KServer.

Set delay before displaying detail information when hovering over information icon ⓘ

A ⓘ information icon displays for each ticket row in Ticketing > View Summary and Service Desk > Tickets. 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**.

- **Use time zone of the browser logging into the system**
- **Use time zone of the VSA server** - The time currently being used by the VSA displays next to this option.
- **Use fixed offset from the VSA server <N> hours**

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

Set up language preferences

- **My language preference is** - Select the language you prefer displayed when you're logged into the KServer. The languages available depend on the language packs 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 packs installed. This option only displays for master role users.
- **Download a Language Pack** - Display a dialog box that enables you to download and install language packs. A language pack 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.

> **Note:** *A master role user can get all access rights to any shared folder by taking ownership.*

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

Click **Clear Snooze** to clear 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 InfoCenter > View Dashboard page.

Defaults

Click **Defaults** to reset all settings to system defaults for this user.

Change Logon

System > Change Logon

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center, IT Workbench

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 5)* 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.

   > **Note:** 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**.

   > **Note:** 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 7)*.

6. Click **Change**.

Converting Your Existing VSA Logon to use your Domain Logon

You can convert your own VSA logon to use your domain logon as follows:

1. Open the System > **Change Logon** page in the VSA.
2. Enter your current VSA password in the **Old Password** field.
3. Enter you domain and domain logon name, formatted *all in lowercase* using the format `domain/username`, in the **Username** field.
4. Enter your domain password in the **New Password** / **Confirm Password** fields.

This enables you to logon to the VSA using your domain logon and have your VSA logon name and password managed using Active Directory. At the same time, you can continue to use all your previous VSA share rights, procedures and other user settings.

> **Note:** If a VSA user logon is based on an AD user, the VSA user's username and password cannot be changed within the VSA, only in Active Directory. Once usernames and passwords are changed in Active Directory LAN Watch must scan the AD machine again to update the VSA. Ideally LAN Watch should be run periodically on the Active Directory machine to keep VSA logons updated with the latest changes to AD logons. See Agent > View AD Users for more information.

Logon Policy

System > Logon Policy

- This page applies to the following product: On Premises

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 5)* 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 imported using Agent > View AD Users or added manually using System > **Change Logon** *(page 7)*.

- **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

Specify a password strength policy by checking the boxes beside the following:

- **Require password change every N days**
- **Enforce minimum password length**
- **Prohibit password reuse for N passwords**
- **Require upper and lower case alpha characters**
- **Require both alpha and numeric characters**
- **Require non-alphanumeric characters**

Update

Press **Update** to apply the settings.

Logon Hours

System > Logon Hours

- This page applies to the following products: On Premises, Kaseya Advanced, Kaseya Essentials, IT Center

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 5) 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 KServer's time zone. For all day access, set start and end time to the same time.

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 5) for a summary of functions affecting user logons.*

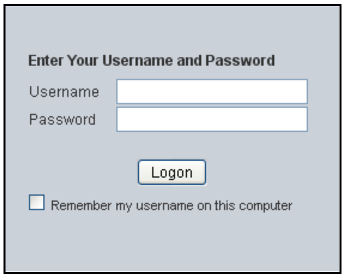
1. Click the **Edit** button on the **Logon Page** tab. The **Edit Logon Page** dialog displays.
2. The following settings are all optional:
   - **Logo for Logon Page** - Browse to select a custom logon on your local machine or network.

     > **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.
   - **Right Frame URL** - Browse to select a custom image on your local machine or network.
   - **Display System Version on logon page** - If checked, the system version displays.
   - **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 7)*.
   - **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.

Embedding the VSA Logon Form in Web Pages

You can embed the VSA logon form in web pages.


Enter Your Username and Password
Username
Password
Logon
□ Remember my username on this computer

Include the following HTML code, replacing the `server.name` text with the name of your VSA.

```
<iframe src="http://server.name/access/logon.asp?embedLogon=true"
name="getChallenge" scrolling="no" frameborder=0 width=280 height=250
marginwidth=0 marginheight=0 />
```

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 online help** (**http://help.kaseya.com/WebHelp/EN/VSA/6010000/index.htm?toc.htm?6939.htm**).

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 and Portal Access
5. Monitoring Configuration

The following resources are also available.

Training

You can view VSA training videos at the **Kaseya Portal** (**http://portal.kaseya.net**). Click the *Kaseya LMS* link under the Education folder.