System

User Guide

Version R95

English

July 19, 2019

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

System Overview

System

The **System** module enables users to maintain policies for the entire system:

- **Preferences**
- **User Security**
- **Organizations, Groups, Departments and Staff**
- **Server Management**
- **Customization**
- **Database Views**

Functions	Description
Preferences *(page iii)*	Sets system-wide preferences that apply only to the currently logged in user.
Change Logon *(page iv)*	Changes the username, password and security question of the currently logged on user.
Check-in Policy *(page v)*	Set limits on a variety of agent check-in parameters.
Naming Policy *(page vii)*	Automatically enforces naming policies based on each machines IP address, network, and computer name
Users *(page ix)*	Creates, edits and deletes users.
User Roles *(page xiv)*	Creates and deletes user roles. User roles determine the access rights for VSA users. Assign roles types to user roles.
Machine Roles *(page xvi)*	Creates and deletes machine roles. Machine roles determine the access rights for machine users. Assign role types to machine roles.
Scopes *(page xviii)*	Assigns organization, machine groups, machines, departments and service desks to scopes.
Logon Hours *(page xxi)*	Specifies when users can logon to the VSA.
User History *(page xxi)*	Displays the functions visited in the last 30 days for each user.
Manage *(page xxii)*	Defines organizations, groups, departments and staff members of departments.
Set-up Types *(page xxvii)*	Defines types of organizations.
Request Support *(page xxvii)*	Accesses Kaseya support.
Configure *(page xxviii)*	Displays Kaseya Server information, license code and subscription information, obtains latest server updates, and server IP information.
Default Settings *(page xxxiv)*	Specifies default settings for server management. Applies to all tenant partitions.
License Manager *(page xxxvi)*	Allocates available agent and user licenses.
Import Center *(page xxxviii)*	Imports and exports user-defined automation solutions into and out of the VSA.
System Log *(page xxxix)*	Logs events that can not be tracked by machine ID.

VSA Logon Policies

Once a VSA user is defined in System > **User Security** *(page viii)*, 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** *(page ix)* - 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 iii)* - The **Preferences** page sets preference options that typically apply *only to the currently logged in* user.
- System > **Change Logons** *(page iv)* - 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 xli)* - The **Logon Policy** page sets logon policies that apply to all VSA users.
- System > **Logon Hours** *(page xxi)* - 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** *(page xlv)* - Set options that display on the logon page.
- System > Site Customization > **Site Header** *(page xlvi)* - Set options that display on the logon page.

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

User Settings

User Settings pages set options that typically apply *only to the currently logged on* user.

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 ii)* 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** *(page iv)*.
  - **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** *(page xxviii)*.
- **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.

Scheduling and Daylight Savings Time

The VSA does not automatically adjust scheduled events for changes between standard time (ST) and Daylight Savings Time (DST). When a task is scheduled, the time zone used to schedule that task is converted into the time used by the Kaseya Server. Regardless of the time zone preferences set by the user in System > Preferences or whether agent time scheduling is used or not, once scheduled the task only "knows" the Kaseya Server time it is suppose to run.

The following workarounds are available.

- **Use the System Clock Used by the Kaseya Server** – *On Premises only* - If the system clock used by system hosting the Kaseya Server is configured to adjust for DST, then scheduled VSA tasks will adjust as well. This option is not available with SaaS because the same instance hosts multiple tenants in different countries and time zones. DST adjustments differ for each country. SaaS instances are set to Greenwich Mean Time (GMT) and never change.
- **Schedule Once** – *On Premises and SaaS* - The easiest method of managing ST/DST changes is to set the schedules once and plan to run them one hour earlier or later, depending on whether ST or DST was used. For example, in the United States, DST runs for the majority of the year, 238 days out of 365. So for the U.S., scheduling using the DST version of your timezone is recommended.

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 ii)* 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** *(page xlv)* 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 iv)*.
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)*.

System Preferences

Check-in Policy

System > System Preferences > Check-in Policy

The **Check-in Policy** page defines group ID policies controlling the minimum, maximum and fixed values allowed for a variety of options. These policies prevent users from selecting settings that place undue stress on Windows servers running the Kaseya Server.

Changing One Field at a Time

If you need to make a change to only one setting in a group:

1. Enter a new value in the field you want to change.
2. Leave all other fields empty. This indicates that these fields will remain unchanged.
3. Click **Update**.

Min/Max Age for Log Entries

These values determine the minimum and maximum values that can be entered in the **Set Max Age for Log Entries** options in Agent > Log History. To remove a value, enter `0` (zero).

Check-In Period

These values determine the minimum and maximum settings that can be entered in the **Check-In Period** setting of Agent > Check-In Control. To remove a value, enter `0` (zero).

KServer Address (0 for editable) - Primary/Second

Two KServer address fields can be specified. The agent checks into the primary server but not the secondary server unless the primary server goes offline.

If `0` is entered in the **Primary** or **Secondary** fields and **Update** clicked, then the **KServer (1st) (2nd)** column of selected group IDs displays `Editable`. Users can enter any domain name server (DNS) name or IP address they like in the **Primary KServer** and **Secondary KServer** fields in Agent > **Check-in Control**.

If these checkboxes are checked and *DNS names or IP addresses are entered* in these fields and **Update** clicked, the **KServer** column of selected group IDs display fixed DNS names or IP addresses. Users are required to use these fixed IP addresses in the **Primary KServer** and **Secondary KServer** fields in Agent > **Check-in Control**.

> **Best Practices:** Although a public IP address may be used, Kaseya recommends using a **domain name server (DNS)** name for the Kaseya Server. This practice is recommended as a precaution should the IP address need to change. It is easier to modify the DNS entry than redirecting orphaned agents.

Allow automatic account creation for selected Group ID

If enabled, new machine ID accounts are created automatically for selected group IDs as soon as the machine's agent checks into the Kaseya Server the first time using a new machine ID name and selected group ID.

For example, an agent is installed on a new machine. The group ID `acme` already exists, but the machine ID `ksmith` does not. With this option enabled for the `acme` group ID, the `ksmith.acme` machineID.group ID account is created as soon as the agent checks in the first time.

> **Note: Allow automatic account creation for selected Group ID** is enabled by default.

To enable automatic account creation for selected group IDs:

1. Check **Allow automatic account creation for selected Group ID**.
2. Select group IDs in the paging area.
3. Click **Update**.

   `Auto Enabled` displays in the **Group IDs/Auto Acct** column of selected group IDs.

Allow automatic account creation for groups without a policy

This option only displays for master role users. If enabled, new machine ID accounts are created automatically for group IDs that do not have any **Check-in Policy** defined, or for agents with a group ID that does not yet exist, as soon as the machine's agent checks into the Kaseya Server the first time using a new machine ID name.

> **Note: Allow automatic account creation for groups without a policy** is enabled by default.

Update

Click **Update** to apply policy parameters to selected group IDs.

Remove

Click **Remove** to remove policy parameters from selected group IDs.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Groups IDs

Lists machine groups. All machine IDs are associated with a group ID and optionally a subgroup ID.

Auto Acct

`Auto Enabled` indicates automatic account creation is enabled for this group ID.

Log Age (Min) / Log Age (Max)

Lists the settings entered in the **Set Max Age For Log Entries** fields in the header, for each group ID.

KServer (1st) (2nd)

Lists the IP addresses/host names of the primary (1st) and secondary (2nd) servers allowed for group IDs.

Check-in (Min) / Check-in (Max)

Lists the settings entered in the **Check-In Period** fields in the header, for each group ID.

Naming Policy

System > System Preferences > Naming Policy

The **Naming Policy** page defines the IP address criteria used to automatically re-assign machines to a different machine group. Each machine group can be assigned multiple naming policies.

Naming policies can also force the renaming of a machine ID, if the machine ID name doesn't match the computer name, reducing confusion when administering managed machines.

Assigning machines to machine groups by IP addresses has the following benefits:

- Typically an organization represents a single customer enterprise and group IDs and subgroups represent locations within that enterprise. When an employee transfers to a new location, the managed machine can be automatically re-assigned to the appropriate machine group or sub-group for that location as soon as the managed machine's agent checks in from the new location's network.
- Using managed variables, managed machines can run procedures that access *locally available resources* based on the group ID or subgroup ID. Using **Naming Policy** this benefit can be applied automatically by IP address even to a highly mobile workforce that travels between different enterprise locations.
- 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** *(page vii)* 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.

Connection Gateway

Optionally check the **Connection Gateway** checkbox and enter the connection gateway IP address. The connection gateway is typically the WAN address of the managed machine. This rule can be applied independently to a group ID. The managed machine must have this IP address as its connection gateway to be automatically assigned to the group ID.

IP Range

Optionally check the **IP Range** checkbox and enter an IP address range, such as `192.168.1.2` – `192.168.1.254`. This rule can be applied independently to a group ID. The IP address of the managed machine must fall within this range to be automatically assigned to the group ID.

Force machine ID to always be computer name

Optionally check the **Force machine ID to always be computer name** checkbox to force each machine ID name to match its corresponding computer name. This rule can be applied independently to a group ID.

> **Note:** Machines are renamed to the new group ID at their next full check-in. The quick check-in cycle does not trigger a rename. To rename a group of machines quickly using **Naming Policy**, schedule the `Force Check-in` sample agent procedure located in Agent Procedures > Schedule / Create.

Update

Click **Update** to apply the naming policy to the selected machine group. The system immediately begins enforcing the group ID's new rule as machines check into the Kaseya Server.

Add

Click **Add** to add a new naming policy to existing naming policies for a selected machine group.

> **Note:** Each machine group can be assigned multiple naming policies. Use this capability to automatically assign machines with different IP address ranges to the same machine group.

Clear

Click **Clear** to remove the naming policy from a machine group. The system immediately stops applying the rule for the machine group.

Machine Group

This column lists the machine groups defined for the system. Select the radio button beside a **Machine Group** before updating, adding or clearing a naming policy.

Connection Gateway

Displays the connection gateway assigned to the machine group.

IP Range

Displays the IP ranges assigned to the the machine groups.

Force Machine ID

Displays a check mark if **Force machine ID to always be computer name** is enabled for a machine group.

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** (page xxii) - A **data object** is an object that you create and name. **Scope data objects** are important enough to warrant being secured system-wide. Scope data objects include organizations, machine groups, machines, departments and service desks. Scope data objects are defined *first*, before being assigned to scopes.
2. **Scopes** (page xviii) - Sets of data objects that users have *visibility* of within the VSA.
3. **User Roles** (page xiv) - 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** (page xvi) - Built-in classifications that determine the types of *user-role-based* licenses to apply to users in user roles.
5. **Machine Roles** (page xvi) - Sets of Portal Access functions that machine users can perform when displaying the VSA **Portal Access** page on their machine.
6. **Machine Role Types** (page xvii) - Built-in classifications that determines the type of *machine-role-based* licenses to apply to machines in a machine role.
7. **Users** (page ix) - Refers to VSA users. Users of machines with agents on them are always identified as *machine users* to distinguish them from VSA users.

Users

System > User Security > Users

The **Users** page creates and deletes user accounts. This page can also assign users to **User Roles** *(page xiv)* and **Scopes** *(page xviii)* when the user account is created.

- 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.
- Each user can change their own logon name, password and email address using System > **Preferences** *(page iii)*.
- To simplify management and auditing of your VSA, provide each user with their own unique logon name. Avoid using generic logons like `User` or `Admin`. Generic logons make it difficult to audit the administrative actions taken by each user.
- Logons can also be managed using **AuthAnvil** *(http://help.kaseya.com/webhelp/EN/aapsfk/9050000/index.asp#home.htm)* or **AuthAnvil On Demand** *(http://help.kaseya.com/webhelp/EN/AAPSFK/9050000/index.asp#38197.htm)*.

Creating a New User

1. Click **New**. The **Add User** dialog box displays.
2. Enter **User Information**:
   - Enter a **Email Address** for the new user.
   - Select an **Initial Role** for new user.
   - Select an **Initial Scope** for the new user.
   - Enter a **First Name** and **Last Name**.
3. Enter **Related Org Staff Member** information:
   - Select a **Staff Org**.
   - Select a **Staff Dept**.
   - Enter or select a **Staff Member** or create a new staff member record.
4. Define **User Credentials**:
   - Enter a **User Name**.
   - Enter a password in the **Password** and **Confirm Password** fields. Passwords are case-sensitive.
   - Check the **Require password change at next logon** checkbox to force the user to enter a new password when they first logon.
5. Click **Save**. The new user displays in the middle pane.

Changing an Existing User Record

1. Click a **User** displayed in the middle pane.
2. Optional **Edit** the following attributes of the User record:
   - **First Name**
   - **Last Name**
   - **Email Address**
   - **Staff Org**
   - **Staff Dept**
   - **Staff Member**
3. Optionally add or remove roles using the **Roles** tab.
4. Optionally add or remove scopes using the **Scopes** tab.

5. Optionally specify access to machines or other assets using the Personal Scope tab.
6. Optionally change the password by clicking the **Set Password** button.
7. Optionally force a user to change their password by clicking the **Force Password** button.
8. Optionally enable / disable user logons by clicking the **Enable** or **Disable** buttons.

Set Password

Select a user in the middle pane and click **Set Password** to change the password for the selected user. Passwords are case-sensitive.

Force Password

Forces a selected user in the middle pane to change their logon the next time they logon.

Enable / Disable

Select a user in the middle pane and click **Enable** or **Disable** to enable or disable a selected user's ability to logon to the VSA. This does not affect users already logged onto the VSA. A **Disabled** column in the middle pane indicates whether a user is prevented from logging on to the VSA.

Log Off

A column in the middle pane indicates whether a user is currently logged on. Select a logged on user, other than yourself, in the middle pane and click **Log Off** to log off that user. *Users are still logged on if they close their browser without logging off.* The **Minutes of inactivity before a user session expires** setting in System > **Logon Policy** *(page xli)* determines when the inactive user sessions are automatically logged off.

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

Master User 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** *(page xiv)* 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.

Master Users

- Any user can be assigned a `Master` user role and `Master` scope, if sufficient roletype licenses exist.
- `Master` *role* users can view and operate all navigation and control options provided by the user interface. `Master` *scope* users can view, add, edit or delete all scope data objects: organizations, machine groups, machines, departments, and service desks.
- Masters can add or delete any user, including other master users. Since even a master user can't delete their own account while logged on, the system requires at least one master user be defined at all times.
- `Master` and `System` roles cannot be modified. A `System` user has access to all user data and functions in a tenant partition.
- A `Master` role and scope user can upload any file type, including `.html`, `.exe`, `.zip`, `.php`, etc.

Standard Users

- A standard role user cannot see roles they have not been granted permission to see.

- A standard scope user cannot see data objects or users they have not been granted permission to see.
- Standard users can create other users, scopes and roles, if given access to these functions.
- A standard user can *not* grant access privileges beyond the ones the standard user has.
- Standard users, if permitted function access, can only create other standard users, not master users.
- By default, a new standard user inherits the scopes and roles of the standard user that created him.
- If a master user creates a new standard user, the standard user inherits *no* scopes or roles. Using this method the master user has to manually assign the scopes and roles of the new standard user.

Machine Users

- Machine users use machines with VSA agents installed on them. They should not be confused with VSA users who can logon to the VSA.
- Machine users can click the agent icon on the machine's system tray to see a Kaseya User Portal or Portal Access (Classic) window of functions and data related to that single machine.
- Access to **Kaseya User Portal** or **Portal Access** functions are determined by the machine role the machine is assigned to. Managed machines are assigned to the `Default` machine role by default and have access to all machine user **Kaseya User Portal** or **Portal Access** functions, unless limited by a VSA user.
- Both the service desk and the organization or machine must be a member of the `Anonymous` scope to display **Service Desk** tickets in **Live Connect** and **Kaseya User Portal** and **Live Connect (Classic)** and **Portal Access (Classic)**.

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.

If Your Account Is Disabled

If your VSA account is disabled because you entered the wrong password too many times, then you can choose to wait for a set period of time for the account to be automatically re-enabled. By default this time period is 1 hour, but the waiting period may have been adjusted by your VSA system administrator.

If your account has been disabled for another reason, you will have to contact your VSA system administrator to re-enable your account. A disabled user account cannot be re-enabled by resetting the password.

To create a new master account on the Kaseya Server see: **Create a New Master User** *(page xi)*.

Changing Passwords Used by External Applications

External Applications and Authentication Using the Web Service API

External applications can be integrated to the VSA via the Web Service API. These external applications can be provided by independent software vendors (ISVs) such as Autotask, ConnectWise, or Tigerpaw. External applications can also be developed by consulting firms, or any organization with technical expertise. To use the Web Service API, external applications must be programmed to authenticate using a valid VSA user name and password.

V6.2 Password Changes that Impact External Applications

VSA v6.1 and prior versions used a SHA-1 algorithm to hash passwords. Therefore, external applications that were compatible with v6.1 used an authentication method based on SHA-1. Beginning with v6.2, a SHA-256 algorithm is used to hash any password that is created under v6.2. Passwords created in prior versions of the VSA remain hashed with SHA-1 until such time as the password is changed or the user is renamed at which point the password is hashed using SHA-256. External applications that were used with v6.1 must be updated, via a programming change, to support SHA-256 passwords in v6.2.

Updating External Applications and Passwords

If you used v6.1 or a prior version of the VSA with an external application, ensure the compatibility of the credential being using. Kaseya recommends arranging to get an updated version of the external application that is compatible with VSA v6.2. Until then, following the procedure for **Creating a New SHA-1 Credential for a Legacy External Application** described below can be used to maintain compatibility with third party applications.

> **Warning:** Changing a password used by a legacy external application will **disable the integration** until either the external application is updated to use the required SHA-256 hashing algorithm or a new SHA-1 credential is created and implemented. Ensure passwords used by external applications are not changed before the update is implemented.

If you used v6.1 or a prior version of the VSA with an external application provided by an ISV or other party:

1. Contact the ISV or party who developed the external application.
2. Request an updated version of the external application.
3. Implement the updated version of the external application.
4. At this point, you can change the password or rename the account used by the external application.

For ISVs or parties responsible for the development of external applications

1. Refer to the **Hashing Algorithm** section of the Authenticate topic in online help. This section provides instructions on how to update the external application to be compatible with VSA v6.2, while also retaining compatibility with prior versions of the VSA.
2. Implement the required programming change to the external application.

Creating a New SHA-1 Credential for a Legacy External Application

If you are running VSA v6.2 or later, and need to create an SHA-1 username and password that is compatible with a legacy external application, and that has not yet been updated to be compatible with v6.2 passwords, use one of the following procedures. You can either create a new master user and password, or reset just the password of an existing master user.

> **Note:** You must have administrator privileges on the Kaseya Server. For 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/setAccountV61.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. Enter an email address in the **Email Address**.
6. Click **Create**.

The external application can now be updated to use the new user account and SHA-1 password to connect to the VSA.

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/setAccountV61.asp`
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**.

The external application can now be updated to use the new SHA-1 password to connect to the VSA.

User Roles

System > User Security > User Roles

The **User Roles** (page xiv) page creates and deletes user roles. Within an user role you can select:

- **Members** *(page xiv)* - Assign or remove members for a user role.
- **Access Rights** *(page xiv)* - Select the access rights for a user role. Access rights determine the functions a *user* can access.
- **Role Types** *(page xvi)* - Assign or remove role types for a user role. Access rights are restricted by the set of licensed role types assigned that user role.

VSA users can belong to one or more VSA user roles. Each user role must be assigned to at least one user role type.

- A VSA user logs on with both a user role (functions they can perform) and a scope (scope data objects they can see). Membership in a user role and a scope is independent of each other.
- VSA users can also be assigned to user roles using the System > **Users** *(page ix)* > Roles tab.
- See System > **Users** *(page ix)* for a discussion of the `Master` user role.
- Restrict access to **User Roles** and **Roles** for all roles except roles responsible for administrating function access.

Middle Pane

You can perform the following actions in the middle pane of **Roles**:

- **New** - Create a new role.
- **Copy Permissions** - Copy the permissions from any other role. By default, all objects in the access tree are enabled, so copying permissions only has a visible effect if some of the objects in the role being copied are disabled.
- **Rename** - Rename the role. Role names can only be all lower case.
- **Delete** - Delete the selected role. All VSA users must be removed from a role before you can delete it.

Related Pages

The following policies are assigned by user role:

- Access to the entire VSA by weekday and hour using System > **Logon Hours** *(page xxi)*
- Remote control user notification using Remote Control > User Role Policy
- Field permissions for editing tickets in Ticketing > Edit Fields and Service Desk > Role Preferences
- **Sharable objects** *(page xix)*—such as procedures, reports, monitor sets and agent installation packages—can be shared by user role.

User Roles - Member tab

The **Members** tab displays which VSA users are assigned to the role selected in the middle pane.

- Click the **Assign** and **Remove** buttons to change the role VSA users are assigned to.
- Sort and filter the VSA users listed in the **Members** page.

User Roles - Access Rights tab

The **Access Rights** tab in the System > **User Roles** page determines what functions VSA users belonging to a selected role can perform. For example, access rights can include whether or not a user can open, add, edit or delete a particular record.

Note: Scopes determine whether a user can *see* certain user-created data structures displayed in the VSA. **Roles** determine access rights to the functions that act on those data structures.

A navigation tree provides access to each module, folder, item, and control in the VSA.

- Click the ⊞ or ⊟ icons next to any item in the tree to display or hide child branches of that item.
  - A checked item means a role provides access to that item.
  - A unchecked item means a role does *not* have access to that item.
  - Click **Expand All** to expand the entire tree.
  - Click **Collapse All** to collapse the entire tree.
- Click **Set Role Access Rights** to change access rights for a role.
  - Checking or clearing any checkbox sets the same state for any child items.
  - Click **Enable All** to enable all items.
  - Click **Disable All** to disable all items.

Specialized Access Rights

- Info Center > Dashboard > **Admin Notes**
- Info Center > Dashboard > **Status**
- Info Center > Dashboard > **Online Help**

Quick View - Hovering the cursor over a check-in icon displays an agent **Quick View** window immediately. You can use **Quick View** to:

- View agent properties
- Start a shared or private Kaseya Remote Control session
- Launch an agent procedure
- Launch Live Connect
  - **Quick Launch Functions** - Shows or hides the action buttons that display along the top of the Quick View popup window.
  - **Run Procedure Now**
    - ✓ **Execute Procedures** - Shows or hides all agent procedure in the Quick View > Quick Launch Procedure list.
    - ✓ **Edit Procedure List** - Shows or hides the add and delete buttons in the Quick View > Quick Launch Procedure list.
    - ✓ **Change Settings** - Shows or hides the configuration gear icon  in the Quick View title bar. The configuration settings let the user show, hide or re-order the list of options displayed in the Quick View popup window, according to user's own preferences.
  - **Quick View Data** - Applies only to functions displayed using Quick View (Classic).
- System > System Preferences > **Functional Access** - *(Deprecated)*
- System > System Preferences > **Enable Scheduling** - Applies to the **Schedule** button for the following functions only. For more information see the **Kaseya knowledge base** *(https://helpdesk.kaseya.com/entries/33901207)*.
  - Patch Management > Manage Machines > Scan Machine
  - Patch Management > Manage Machines > Initial Update
  - Patch Management > Manage Machines > Automatic Update
  - info center > Reporting > Reports
  - Info Center > Reporting > Report Sets
- System > System Preferences > Enable Wake on LAN - Applies to Patch Management > Scan Machine > Schedule button only

User Roles - Role Type tab

Click the **Assign** and **Remove** buttons to change the role types a user role is assigned to.

Roles 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** *(page xiv)* tab and Machine Roles > **Access Rights** *(page xvii)* tab. The number of role type licenses purchased displays in the System > **License Manager** *(page xxxvi)* > 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

System > User Security > Machine Roles

The **Machine Roles** (page xiv) page creates and deletes machine roles. Machine roles determine what *machine users* see when they use Kaseya User Portal or Portal Access (Classic) from a machine with an agent. The user access window displays when a *machine user double-clicks the agent icon in the system tray of their managed machine.*

> **Note:** The **User Roles** page determines what *VSA users* see when they use Live Connect or Live Connect (Classic) from within the VSA.

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

- **Members** *(page xvii)* - Assign or remove machines for a machine role.
- **Access Rights** *(page xvii)* - Select the access rights for a machine role. Access rights determine the functions a *machine user* can access.
- **Role Types** *(page xvii)* - Assign or remove role types for a machine role. Currently there is only one machine role type provided and no access rights are restricted.

> **Note:** The **Home** page seen by machine users when they first display the **Portal Access** window can be customized using System > Customize > **Live Connect** *(page l)*.
>
> **Note:** See Enabling Ticketing for Portal Access Users on Unsupported Browsers.
>
> **Note:** See the PDF quick start guide, **Live Connect** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/EN_LiveConnect_R95.pdf#zoom=70&navpanes=0)*.

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.

Middle Pane

You can perform the following actions in the middle pane of **Machines Roles**:

- **New** - Create a new machine role.
- **Copy Permissions** - Copy the access rights to the selected machine role from any other machine role.
- **Rename** - Rename the machine role.
- **Delete** - Delete the selected machine role. All machines must be removed from a machine role before you can delete it.

Machine Roles - Members tab

The **Members** tab displays which machines belong to the machine role selected in the middle pane.

- Click the **Change Machine Role** button to change the machine role a machine is assigned to.
- Sort and filter the machines listed in the **Members** page.

Machine Roles - Access Rights tab

The **Access Rights** tab in the System > **Machine Roles** page determines what functions *machine users* can perform on machines belonging to a selected machine role. For example, access rights can include whether or not a machine user has access to their own machine remotely from another machine.

A navigation tree provides access to each item and control on the **Live Connect** page.

- Click the ⊞ or ⊟ icons next to any item in the tree to display or hide child branches of that item.
  - A checked item means a machine role provides access to that item.
  - A unchecked item means a machine role does *not* have access to that item.
  - Click **Expand All** to expand the entire tree.
  - Click **Collapse All** to collapse the entire tree.
- Click **Set Role Access Rights** to change access rights for a machine role.
  - Checking or clearing any checkbox sets the same state for any child items.
  - Click **Enable All** to enable all items.
  - Click **Disable All** to disable all items.

Machine Roles - Role Types tab

Note: There is only one machine role type, so all machines must use the **Basic Machine** role type.

- **Basic Machine** - Provides access to all **Portal Access** functions available to machine users.

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** *(page xiv)* tab and Machine Roles > **Access Rights** *(page xvii)* tab. The number of role type licenses purchased displays in the System > **License Manager** *(page xxxvi)*

> Role Type tab. Each role type license specifies the number of *named users* and *concurrent users* allowed.

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** *(page xxxvi)* shows 150 of the total number of `Basic Machine` licenses used.

Scopes

System > User Security > Scopes

The **Scopes** (page xviii) 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.

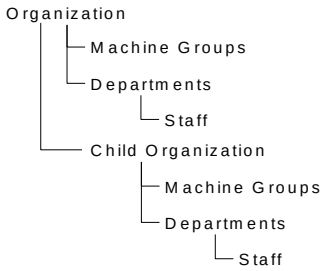
Note: A user logs on with both an assigned role (the functions they can perform) and an assigned scope (the data they can see). Membership in a role and membership in a scope are independent of each other.

Users can also be assigned to scopes using the System > **Users** *(page ix)* > Scopes tab.

Scope Data Objects

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** - 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** *(page xxii)*.



- **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.

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.

Master Scope

See System > **Users** *(page ix)* for a discussion of the `Master` scope.

Middle Panel

You can perform the following actions in the middle pane of **Roles**:

- **New** - Create a new scope.
- **Rename** - Rename the scope.
- **Delete** - Delete the selected scope. All VSA users must be removed from a scope before you can delete it.

Scope Details

Each tab provides the following actions:

- **Assign** - Assigns access for a data structure to a scope.
- **Remove** - Removes access for a data structure from a scope.
- **All in Scope** - Displays only on the **Organizations**, **Machine Groups**, **Machines** and **Departments** tabs. Clicking the **All in Scope** button on a tab displays a new window listing all data structures of that tab type in the scope, whether defined explicitly or implicitly.

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.

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 ii)* 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.

User History

System > User Security > User History

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

Click **a user name** to display the log for that user.

> **Note:** This log data does not appear in any reports.

Notification Policy

System > User Security > Notification policy

The **Notification policy** permits Master/System users to configure Admin Security Notifications.

Update

Press **Update** to apply the settings.

Security Notification Configuration

- **Notify when an admin is created-as or promoted-to Master/System** - the option is set to send Admin Security Notifications when an administrator is created-as or promoted-to Master/System.
- **Notify when an admin is Enabled/Disabled** - the option is set to send Admin Security Notifications when an administrator is Enabled/Disabled.
- **Notify when an admin is Modified** - the option is set to send Admin Security Notifications when an administrator is Modified.

- **Notify when an admin is Locked-Out** - the option is set to send Admin Security Notifications when an administrator is Locked-Out.
- **All Admins** - all administrators are set to receive Admin Security Notifications.
- **Email Address(s)** - specify the email address(s) of administrators that will receive Admin Security Notifications. This option is *only available* if **All Admins** is not selected.

Orgs/Groups/Depts/Staff

- **Manage** *(page xxii)* - Create organizations, machine groups, departments and staff.
- **Set-up Types** *(page xxvii)* - Create organization types used to classify organizations.

Manage

System > Orgs/Groups/Depts/Staff > Manage

The **Manage** page defines the organizations you do business with. Typically an organization is a customer, but an organization could also be a business partner. Organizations are associated with **Scopes** *(page xviii)*, tickets and with desk definitions. Every managed machine, managed device and VSA user belongs to an organization.

Within an organization you can define:

- **General** *(page xxii)* - General settings for the organization.
- **Machine Groups** *(page xxiii)* - Machine groups associated with this organization.
- **Departments** *(page xxiv)* - A unit of administrative responsibility within an organization.
- **Staff** *(page xxv)* - Personnel assigned to a department.
- **Custom Fields** *(page xxvi)* - Assigns values to custom fields used to classify organizations.
- **Systems Management** *(page xxvi)* - Configures **Policy Management** policies for an organization using a setup wizard.

Manage - General tab

System > Orgs/Groups/Depts/Staff > Manage > General tab

Click **New** to display the **Add Organization** window, or click a row in the middle panel, then click **Edit** to display the **Change Organization** window. Enter the following attributes:

- **New/Convert** - Select **New Organization** if no other data source exists to convert from. If **Service Billing** is installed you can create a organization by converting an existing customer record or vendor record.
- **ID** - The record identifier. Can only be changed using the **Rename** button.
- **Org Name** - The display name for the identifier.
- **Deploy Agent URL** - Click this link to create an agent install package specific to the default machine group in this organization on the Agent > Packages > **Manage Packages** page.
  1. You must click a **Deploy Agent URL** link *at least once* to create the agent package
  2. Optionally edit **Deploy Agent URL** agent packages just as you would any other agent package.
  3. Email a **Deploy Agent URL** link to the machine users of that machine-group or organization to prompt them to install an agent.
  4. When a user clicks the **Deploy Agent URL** sent to them, a download page prompts them to download the package. The agent automatically installs. This download page is different from the legacy download page shown on the **Manage Packages** page. You can customize this

new download page using the **Deploy Header** *(page xlix)* tab on the System > Customize > **Site Customization** page.

- **Org Type** - The type of organization. See **Organization Types** *(page xxvii)*.
- **Default Dept. Name** - The default department for the organization.
- **Default MachGroup Name** - The default machine group for the organization.
- **Org Web Site** - The organization's web site.
- **Number of Employees** - The number of employees in the organization.
- **Annual Revenue** - The annual revenue of the organization.
- **Preferred Method of Contact** - The organization's preferred method of contact: `Phone, Email, Mail, Fax`.
- **Parent Organization** - The parent organization of this organization. The parent organization must be previously defined to display in this drop-down list.
- **Primary Phone** - The primary phone of the organization.
- **Primary Email** - The primary email of the organization.
- **Primary Contact** - The primary contact for the organization. A contact is a **staff** *(page xxv)* member of a department.
- The address of the organization:
  - **Country**
  - **Street**
  - **City**
  - **US State**
  - **Zip Code**
- **Map** - Clicking this hyperlink displays the location of the address in Google maps.

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** *(page vii)* 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.

Manage - Machine Groups tab

System > Orgs/Groups/Depts/Staff > Manage > Machine Groups tab

Define the machine groups associated with this organization. Machines are always defined by machine group and machine groups are always defined by organization. You can define multi-level hierarchies of machine groups by identifying a parent machine group for a machine group.

Deploy Agent URLs

Click the **Deploy Agent URL** link in any row to create an agent install package specific to that machine group on the Agent > Packages > **Manage Packages** page.

1. You must click a **Deploy Agent URL** link *at least once* to create the agent package
2. Optionally edit **Deploy Agent URL** agent packages just as you would any other agent package.
3. Email a **Deploy Agent URL** link to the machine users of that machine-group or organization to prompt them to install an agent.
4. When a user clicks the **Deploy Agent URL** sent to them, a download page prompts them to download the package. The agent automatically installs. This download page is different from the legacy download page shown on the **Manage Packages** page. You can customize this new download page using the **Deploy Header** *(page xlix)* tab on the System > Customize > **Site Customization** page.

Actions

- **New** - Adds a new machine group.
  - **Name** - The name of the machine group.
  - **Parent Group** - Parent machine group. Optional.
- **Change Machine Group ID** - Renames a selected machine group ID.
- **Move** - Moves all machines and sub-machine groups from a source machine group to a target machine group. The move can be to a target machine group in the same organization or a different organization. *The source machine group is deleted after the move.* Cannot be used on the last machine group in a source organization.

  > **Note:** If you want to re-create the same machine group with the same contents at the target location, create the machine group at the new location *before* the move, then select it when you perform the move.

- **Delete** - Deletes a selected machine group. A machine group must be empty of member machines to delete it. Machines can be moved to a different machine group using Agent > Manage Agents > Change Group.
- **Agents** - Lists the member machines of a selected machine group.
- **Set Default** - Sets a selected machine group as the default machine group for an organization.

Manage - Departments tab

System > Orgs/Groups/Depts/Staff > Manage > Departments tab

Departments can be defined within an organization, customer record or vendor record. Example: `IT`, `Sales` or `Accounting`. All staff members are defined by the department they belong to. You can define multi-level hierarchies of departments by identifying a parent department for a department. You can reassign a staff member to any other department within the same organization, customer record, or vendor record.

Actions

- **New / Edit** - Adds a new department.
  - **Department Name** - The name of the department.
  - **Parent Department** - Parent department. Optional.
  - **Manager** - The manager of the department. Optional. The staff member record must be previously defined.
- **Move** - Moves all staff and sub-departments from a source department to a target department. The move can be to a target department in the same organization or a different organization. *The*

source department is deleted after the move. Cannot be used on the last department in a source organization.

> **Note:** If you want to re-create the same department with the same contents at the target location, create the new department at the new location *before* the move, then select it when you perform the move.

- **Change Department ID** - Renames the department ID of a selected department.
- **Delete** - Deletes a selected department. A department must be empty of staff members to delete it. Staff members can be moved using the **Staff** *(page xxv)* tab.
- **Set Default** - Sets a selected department as the default department for an organization.
- **Delete** - Deletes a selected department. A department must be empty of staff members to delete it. Staff members can be moved using the **Staff** *(page xxv)* tab.

Manage - Staff tab

System > Orgs/Groups/Depts/Staff > Manage > Staff tab

Create staff members within departments and maintain contact information for each staff member. Contacts and their phone numbers can be associated with tickets and with desk definitions. Staff member information can also be updated by Active Directory domain using Discovery > Domains > **Domain Watch** *(http://help.kaseya.com/webhelp/EN/KDIS/9050000/index.asp#10750.htm)*.

Adding / Editing a Staff Record

- **Full Name** - The full name of a person within the organization.
- **Department** - The department the person is associated with. The department must be previously defined to display in this drop-down list.
- **Supervisor** - The person this staff member reports to. The Supervisor must be previously defined as a staff member in the same department.
- **Title** - The person's title in the organization.
- **Function** - The function the person performs in the organization.
- **User Name** - VSA user ID associated with this staff member. Required to **View All Tickets** and for Time Tracking.
- **View All Tickets** - If checked, the VSA user associated with this staff member can view all **Service Desk** tickets in his or her scope as well as tickets associated with this specific staff member record. If blank, this VSA user can only view **Service Desk** tickets associated with this specific staff member record.

Contact Information

- **Preferred Contact Method** - `Email`, `NotSet`, `Phone`, `TextMsg`
- **Phone Number** - The person's direct phone number.
- **Email Address** - The person's email address.
- **Text Message Phone** - The person's text message phone number.

Time Sheet Approval

A staff member record must be associated with a VSA user to approve timesheets and have visibility of timers.

- **Approve All Timesheets** - If checked, this staff member can approve any timesheet. This ensures all timesheets can be approved in a timely manner, if other approvers are temporarily unavailable.
- **Approval Pattern** - Specifies the approval pattern required to approve this staff member's timesheets. Approval patterns determine whether the staff member's supervisor, or the supervisor's supervisor, or both, are required to approve the staff member's timesheet.

Note: See Time Tracking configuration options.

Visibility of Service Desk Tickets by a Staff Member

If a VSA user name is associated with the staff member record of an organization, then that VSA user has visibility of tickets associated with that staff member record *even if the VSA user's scope does not allow it*. Any tickets created by that VSA user are automatically associated with their staff member record and organization. This method primarily supports machine users using Portal Access to create and manage their own tickets. Machine users expect to have access to all the tickets they create and to any tickets created on their behalf, but may have no scope privileges defined for them. If a scope does exist for a VSA user associated with a staff member, checking the checkbox called **View all tickets** in the **staff member** *(page xxv)* record provides visibility of those additional tickets by scope.

Example: Dale is the main customer contact for the XYZ organization. He is provided a scope that allows him to see all tickets related to his organization, even tickets not created by him, so the **View all tickets** checkbox is enabled. Brandon from the XYZ organization contacts the service desk to submit a ticket as well. Initially it's unclear whether Brandon should have access to any other tickets beyond the tickets he himself creates, so the **View all tickets** is left unchecked. Later, if Dale okays greater access for Brandon, the service desk provider can assign a scope to Brandon and check the **View all tickets** checkbox.

Manage - Custom Fields tab

System > Orgs/Groups/Depts/Staff > Manage > Custom Fields tab

Assign values to the custom fields displayed on this tab. The values you assign are used to classify organizations. The titles of the custom fields displayed on this tab can be customized using Site Customization > **Org Custom Field Title** *(page xlviii)*.

Manage - Systems Management tab

System > Orgs/Groups/Depts/Staff > Manage > Systems Management tab

The **Systems Management** tab provides a setup wizard. The **Systems Management Configuration** setup wizard enables you to quickly *configure and apply machine management policies for a specific organization*. Once configured, these polices are assigned to each machine you manage on behalf of that organization. Policies govern many different aspects of machine management:

- Audit scheduling
- Monitoring
- Alerts
- Patch Management
- Routine machine maintenance using agent procedures

With policies you no longer have to manage each machine individually. You only have to assign or change the policy. A policy assignment or a change within an assigned policy is propagated within 30 minutes to all member machines without you having to schedule anything. Once applied, you can quickly determine whether managed machines are in compliance or out of compliance with their assigned policies. Compliance tracking by individual policy provides you with the information you need to deliver IT services consistently throughout the organizations you manage.

Note: See the **Standard Solution Package** for a detailed explanation of each option in the **setup wizard** *(http://help.kaseya.com/webhelp/EN/SSP/9050000/index.asp#11220.htm)*.

Set-up Types

System > Orgs/Groups/Depts/Staff > Set-up Types

The **Set-up Types** page defines records that classify your organizations. For example, you might define an organization as a `division` within your enterprise, or classify organizations regionally or by revenue. Alternatively, you might classify organizations as a `prospect`, `preferred customer`, or `business partner`. It depends on your business requirements.

Service Desk

Set-up Types can be optionally used to automatically **associate a ticket with a policy** *(http://help.kaseya.com/webhelp/EN/KSD/9050000/index.asp#6210.htm)* in the **Service Desk** module.

General tab

Click **New** to display the **Add Organization Types** window, or click a row in the *middle* panel, then click **Edit** to display the **Change Organization Types** window. Enter the following attributes:

- **ID** - The record identifier. Can't be changed once you save it.
- **Description** - A brief description of this ID.

Server Management

Request Support

System > Server Management > Request Support

The **Request Support** page provides multiple ways of contacting Kaseya support.

- **Support Web Site -** Find answers to common questions using the Kaseya Support website at **https://**www.kaseya.com**/customer-success/support**. This website provides links to the **Kaseya Forum** and to the **Kaseya Knowledge Base**.
  - **Kaseya Forum** - Hosts an interactive community of Kaseya users that discuss a wide variety of issues and solutions on a daily basis. Subscribe to the forum to get new posts of interest directly emailed to you as new information appears. You can access the forum at **http://community.kaseya.com/xsp/default.aspx**.
  - **Kaseya Knowledge Base** - Provides technical information about installation and usage of the Kaseya IT Automation Framework. You can access the knowledge base at **https://helpdesk.kaseya.com/hc/en-gb**.
- **Manage your support request** - The **Kaseya Help Desk** *(https://helpdesk.kaseya.com/hc/en-gb/articles/360000333152)* provides a single point of contact for managing your Kaseya support tickets, accessing the knowledge base, and participating in the user forum.

Your Information

Typically Kaseya support needs some basic information about your system to begin providing support. Your user name, email address, Customer ID, and system URL are provided for your convenience.

Configure

System > Server Management > Configure

The **Configure** page manages the configuration of your Kaseya Server and related services. Related topics include:

- **Change Reporting Configuration** *(page xxxii)*
- **Indexing the Audit Results Table** *(page xxxiv)*
- **Default Settings** *(page xxxiv)*
- **Kaseya Server Setup** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/Install)*

Version, Patch Level, and Licensing

- **Version Number** - Shows the version number of the system.
- **Installed Patch Level** – Shows the installed patch level of the system.
- **Available Patch Level** – Shows the highest patch level available to install.
- **Check for Latest Patches** – Click this link to see the **latest patch release notes** *(http://help.kaseya.com/webhelp/EN/RN/index.asp#PatchReleaseNotes.htm)* and instructions on how to update your system with the latest patches.
- **Warn if the server cannot get data from http://vsaupdate.kaseya.net** - Check this box to display a warning if your VSA cannot connect to `http://vsaupdate.kaseya.net` to fetch the latest PCI ID list used by audit. Your VSA attempts to automatically fetch this information from `http://vsaupdate.kaseya.net`. Verify that the server can connect outbound to port 80 on `http://vsaupdate.kaseya.net` and that its responses are not blocked by your firewall.
- **Warn when the license reaches the maximum number of seats** - Check this box to display a warning when the number of machine ID accounts reaches the maximum for your VSA.

Reapply Schema / Defrag Database

Warning: Do not use the Microsoft SQL tuning advisor against the schema. It adds keys that conflict with the smooth operation of the system.

- Click **Reapply Schema** to re-install and validate the last database schema that was downloaded using **Check for Update**. Reapply schema is a safe operation that users can run in an attempt to resolve a variety of problems. Reapply schema:
  - Sets default values and runs basic consistency checks on the database.
  - Rebuilds all pre-defined Kaseya procedures.
  - Rebuilds all pre-defined Kaseya procedure samples.
  - Reschedules default backend processing procedures for the Kaseya Server.
  - Only runs automatically when the Kaseya Server is updated or an add-on is installed.

  This is all completed without the risk of losing any agent data. This is a good self healing routine to run if you observe:
  - Procedures failing in the **IF** condition or in specific steps.
  - Pending alerts not being processed within a two minute interval. You can monitor this using the System > **Statistics** *(page xxxix)* page. This might indicate a problem with backend processing procedures.
- Click **Defrag Database** to defragment the physical files on your disk arrays. Fragmented SQL Server data files can slow I/O access.

Sample Data

- **Reload sample scripts with every update and database maintenance cycle** - Check to reload sample agent procedures.

- **Reload sample event sets with every update and database maintenance cycle** - Check to reload sample event sets.
- **Reload sample monitor sets with every update and database maintenance cycle** - Check to reload sample monitor sets.

HTTPS

- **Automatically redirect to https at logon page (except when accessing via localhost)** - If checked, ensures all users logging into the VSA remotely use the secure HTTPS protocol.

> **Note:** You can redirect *all* HTTP requests to HTTPS, not just specified ports, by adding the `--redirectHttpToHttps` option to the `Arguments` value in the `<KaseyaInstallationDirectory>\Services\KaseyaEdgeServices.config` file. For example: `"Arguments": "--listenPort 80,443,5721 --redirectHttpToHttps"`

API

- **Enable VSA API Web Service** - Check to enable the VSA API Web Service.

Patch Management

- **Enable Invalid Patch Location Notifications** - Microsoft sometimes prepares patches that do not allow the File Source function to download patches successfully. If checked, this option notifies Kaseya that an "invalid patch location" exists for a patch required by any of the managed machines on your system. Notification alerts Kaseya to prepare a valid patch location manually and send it out as an updated patch location override for all customers to use. If blank, no notification is sent to Kaseya. You will still receive updated patch location overrides prepared in response to notifications reported by *other* customers, regardless of this setting.

> **Note:** Notification sends no customer-specific or machine-specific information to Kaseya.

Ticketing

- **Allow non-authenticated users to download attachments from ticket notifications** - If checked, links to attachments embedded in the notes of tickets can be opened in outbound emails without requiring the user to authentic themselves to the VSA. For security reasons, enabling this option is not recommended.

Database Backups

- **Run database backup / maintenance every <N> Days @ <Time>** - The Kaseya Server automatically backs up and maintains the MS-SQL database and transaction log for you. Click **Set Period** to set the frequency and time selected. If your Kaseya Server is shut down at the scheduled backup time, the backup will occur the next time the Kaseya Server goes online. You can enter zero to disable recurring backups.
- **Backup folder on KServer** - Set the directory path to store database backups in. The default directory path is typically `C:\Kaseya\UserProfiles\@dbBackup`. Click **Change** to confirm changes to the directory path. Click **Default** to reset the directory path to its default.
  - Database backups older than three times the backup and maintenance period are discarded automatically to prevent your disk drive from filling up. For example, if the backup occurs every 7 days, any backup older than 21 days is deleted.
  - If the backup folder is on a different drive to where SQL Server is installed, the `NETWORK SERVICE` account should be added to the folder access list with Modify permissions.
- **Change DB** - Connect your Kaseya Server to a database on a different machine.
  1. Backup your existing `ksubscribers` database by clicking **Backup Now** in the System > **Configure** page.
  2. Copy the database backup file to the database server you wish to connect to.

3. Use SQL Server Management Studio (SSMS) on the new database server to restore the `ksubscribers` database. Right click Databases > Restore Databases...
4. Verify the restored `ksubscribers` database is set to **mixed mode authentication**.
   - ✓ In SQL Server Management Studio (SSMS) right click the restored `ksubscribers` database and select **Properties**.
   - ✓ Click the **Security** tab.
   - ✓ Under authentication, select **SQL Server and Windows**.
   - ✓ Click **OK**.
5. **Verify CLR is enabled in the new database server** *(https://helpdesk.kaseya.com/entries/33743166)*.
6. Verify your Kaseya Server is on the same LAN as your new database server and **port 1433** is open on the database server.
7. Click the **Change DB** button.
8. Enter the database location using one of the following formats:
   - ✓ computer name
   - ✓ computer name\instance name
   - ✓ IP address
9. Enter a database logon name. The default logon name is `sa`.

   Note: This logon is only used to configure the database. The system creates its own database logon to use going forward.
10. Enter the password associated with this logon name.
11. Click **Apply**. The system then connects to the remote database and configures it.
12. At the end of the process IIS will be reset. Wait about 1 minute for it to complete.
13. Refresh the VSA, and re-log in.
14. Return to the **Configure** page and click the **Reapply Schema** link near the top of the page. Wait for it to complete.

- **Backup Now** - Initiate a full database backup now. Use this function *before* you shut down or move your Kaseya Server, to ensure you have the latest Kaseya Server data saved to a backup. The backup will be scheduled to run within the next 2 minutes.
- **Restore** - Click to restore the Kaseya Server's database from a backup file. A file browser displays a list of Kaseya Server database backup files you can restore from.

Note: After a restore of a 5.1 database, the SSRS URL will be invalid and need to be reset. After a restore of a 6.x database the SSRS URL may be invalid and need to be reset.

Archive

Archiving of agent logs are enabled, by log and machine ID, using Agent > Log History.

- **Archive and purge logs every day at <time>** - Specifies the time of day log files are archived and purged.
- **Set Period** - Click to confirm changing the time log files are purged and archived.
- **Log file archive path** - The file location where the archive files are stored.

Note: Monitoring data log archives—identified on the Agent > Log History page—are stored in the `<KaseyaRoot>\UserProfiles\@dbBackup` directory. This is to improve performance on systems where the database is on a different server. All other agent log archives are stored in the directory specified by the System > **Configure** *(page xxviii)* > **Log file archive path** field.

- **Change** - Click to the confirm changing the archive file location. A procedure runs to move any existing archive files in the old file location to the new file location.
- **Default** - Resets the log file archive path to the default location on the Kaseya Server. A procedure runs to move any existing archive files in the old file location to the new file location.

Server Status

- **KServer Log** - Displays the last 300 kbytes of the Kaseya Server's log file. The entire log file is up to 5 Mbytes in size and is located at `xx\KServer\KServer.log` where `xx` is the parent directory of the VSA web directory.
- **Live Connect KServer** - An agent is automatically installed on the Kaseya Server. You can click the check-in icon for this agent to initiate a Live Connect session with the Kaseya Server.
- **Stop KServer** - Shows the current status of the Kaseya Server: **running** or **stopped**. The Kaseya Server can be stopped by clicking **Stop Service**.
- **Enable alarm generation** - Uncheck to prevent generating unnecessary alarms. This can occur if you stop the Kaseya Server, disconnect from the internet, or maintain the system. Otherwise leave this box checked.
- **Restart MsgSys** - Restarts the MessageSys service. This service is the application server that manages requests from VSA application users.
- **Enable logging of procedure errors marked "Continue procedure if step fail"** - If checked, failed steps in procedures are logged. If blank, failed steps in procedures are *not* logged.
- **Enable logging of successful child script execution in agent procedure log** - If unchecked, child script success entries are not included in the agent procedure log. This can reduce the size of the agent procedure log tremendously. It takes up to 5 minutes for the KServer to read this setting change.
- **Enable auto close of alarms and tickets** - If checked, open alarms and tickets for monitor sets and offline alerts are automatically close when the alert condition no longer exists. Offline alerts are configured using Agent Status alerts. Checking this checkbox requires the **Enable alarm generation** checkbox be checked to auto close alarms and tickets.

Server Settings

- **Select time format** - Click the appropriate radio button to select how time data is displayed. The default is AM/PM format. Both these display formats are compatible with Microsoft Excel.
  - AM/PM format - 9:55:50 pm 9-Apr-07
  - 24-hour format - 21:55:50 9-Apr-07

> **Note:** Time offset is set in System > **Preferences** *(page iii)*. The date format is set in System > **Local Settings** *(page xlix)*.

- **Change external name / IP address of Server** - Shows the current external name or IP address of the Kaseya Server. This is the address the agents of managed machines access for check-in purposes. The address can be changed by entering a new address or host name in the field and pressing **Change Name/IP**.

> **Note:** Do *not* use a computer name for your Kaseya Server. The agent uses standard WinSock calls to resolve a IP address from a **fully qualified host name**. Resolving an IP address from a computer name requires NETBIOS, which may or may not be enabled on each computer. NETBIOS is an optional last choice that the Windows will attempt to use to resolve a name. Therefore, only fully qualified names or IP addresses are supported.

- **Set URL to MS-SQL Reporting Services Engine** - Click the **Change Reporting Config...** *(page xxxii)* button to specify the URL used by the VSA to connect to Reporting Services. You can also specify the credential used to access Reporting Services and customize the URL displayed in the header of all VSA reports.

- **Specify port Agents check into Server with** - Entering a different port and clicking **Change Port** switches the port the Kaseya Server uses *immediately*.

  > **Warning:** Before you change the Kaseya Server port ensure that all agents are set to use the new port with their primary or secondary Kaseya Server. Agent check-ins are configured using Agent > Check-in Control.

- **KServer ID** - ID used to bind agents to the Kaseya Server - The unique identifier for this Kaseya Server. Bound agents cannot check-in successfully unless the unique Kaseya Server ID they are bound to using the Agent > Check-in Control page matches the unique ID assigned to the Kaseya Server using the System > **Configure** *(page xxviii)* > **Change ID** option. Prevents IP address spoofing from redirecting agent check-ins. Only change the Kaseya Server ID if you are installing a fresh VSA and wish to duplicate the ID of an existing Kaseya Server with agents already bound to it.

Version Information

Displays the following information about your VSA configuration.

- OS Version
- IIS Version
- Kaseya Server Version
- SQL Version
- Database Location
- Agent On Kaseya Server

References

- **Release Notes** - Click **Release Notes** to display a list of all changes and enhancements made to the VSA, for all versions of the software.
- **Show License** - Click **Show License** to display the current license agreement to use the VSA.

Change Reporting Configuration

System > Server Management > Configure *(page xxviii)* > Change Reporting Config...

The **Change Reporting Configuration** dialog selects the type of reporting server used to run reports.

- A built-in, proprietary report server is provided that requires no additional configuration.
- If instead, a SQL Server Reporting Services (SSRS) is preferred, you can configure the VSA connection to the SSRS instance used to generate VSA reports. The SSRS may be installed locally or remotely from the Kaseya Server and locally or remotely from the SQL Server instance hosting the `ksubscribers` database.

Actions

- **Edit** - Edits the reporting server configuration.
- **Test** - Tests that reporting server configuration is working.
- **Run Registration** - This button is used by developers to register newly created data sets for customizable reports, instead of running **Reapply Schema** for the entire VSA.

Options

- **Use Kaseya Reporting** - If checked, a built-in, proprietary report server is used to run reports. Intended for smaller implementations of the VSA. This report server is used by default for new installs of the VSA. If blank, an SSRS report service is used to run reports. SSRS is intended for larger implementations. If blank, you must provide a **Host Name** URL to a SQL Server Reporting Services instance to run reports.
- **Reporting Timeout (Min)** - Sets the time to wait for a report to complete publishing.

- **Host Name** - The URL used by the VSA to connect to a SQL Server Reporting Services instance. Mandatory to run reports. The VSA typically uses one of the following URL patterns to connect to a SQL Server Reporting Services instance. Specifying the appropriate URL is mandatory to run reports.

  > **Note:** - See the **SSRS Configuration** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/install/index.asp#10436.htm)* in the *Kaseya Server Setup* user guide for a visual walkthrough of the steps required to configure an SSRS reporting server.

  SQL on the same box as VSA

  `http://localhost/ReportServer` *(most common)*
  `http://localhost/ReportServer$SQLExpress`
  `http://localhost/ReportServer_<SQLINSTANCENAME>`
  `http://localhost:<PORTNUMBER>/ReportServer_<SQLINSTANCENAME>`

  SQL box separate from VSA

  `http(s)://<SQLSERVERNAME>/ReportServer` *(most common)*
  `http(s)://<SQLSERVERNAME>/ReportServer$SQLExpress`
  `http(s)://<SQLSERVERNAME>/ReportServer_<SQLINSTANCENAME>`
  `http(s)://<SQLSERVERNAME>:<PORTNUMBER>/ReportServer_<SQLINSTANCENAME>`
- **User Name** - The user name used to access the Reporting Services instance when running reports. Applies to some configurations. See **Adding Custom Credentials to a Remote Report Server** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/install/index.asp#6601.htm)* in the *Kaseya Server Setup* user guide for a visual walkthrough of this configuration.
- **Logo** - The URL of the image displayed in the header of reports. Applies to some configurations. By default, VSA report headers display the image specified by the System > Site Customization > **Site Header** *(page xlvi)*. Changing the value in the System > Configure > **Change Reporting Config...** *(page xxxii)* > **Logo** field overrides this default, changing the URL *for report headers only*. Changing the URL in the Change Reporting Config... > **Logo** field does not affect the display of the **Site Header** image. If a logo does not display in SSRS reports it may be due to either of the following conditions:
  - The SSRS is installed on the same machine as the Kaseya Server. SSRS is unable to retrieve the logo because of firewall issues. Change the URL to `localhost` from the externally available URL/IP address.
  - The VSA has been configured using a self-signed security certificate. Change the protocol from `https` to `http`.
- **Report URL Base** - Overrides the URL used for CURL reports. For most reports the *external* VSA URL is used to generate reports but, an issue called "router loopback" can occur with CURL reports. Enter a different URL from the external VSA URL to avoid this issue. Defaults to `http://localhost:80/`
- **Concurrent Reports** - Sets the number of reports that can be published simultaneously. Concurrent reports greater than this number are queued.
- **Keep All Reports** - If `No`, **Number of Days** determines how long reports are kept. If `Yes`, all reports are kept and **Number of Days** setting is not applicable.
- **Keep Number of Days** - Sets the number of days to keep a report after its creation date. Must be at least 30 days.

  > **Note:** Only deletes reports *created after* the **Number of Days** value is enabled. Reports can be manually deleted from the `<Kaseya_Installation_Directory>\WebPages\DataReports` directory.

Indexing the Audit Results Table

Note: The following "one time" configuration task applies only if a dialog recommends indexing of the Audit Results table. The dialog only displays, if applicable, when a master user logs on to the VSA.

The response time of the Kaseya Server database can be improved by indexing the audit results table. **Depending on the number of records in this table, this process could take 1 to 4 hours to complete. The Kaseya Server should be shut down during this process to prevent the possibility of losing audit data.**

1. Click the **Stop Kserver** button on the System > **Configure** *(page xxviii)* page.
2. In SQL Server Management Studio:
   a. Open a new query window and ensure `ksubscribers` is the selected database.
   b. Run the following stored procedure: `Exec spCreateAuditRsltAppsPK`

   This procedure might run 1 to 4 hours or longer, depending on the number of records in the table and the speed of the SQL Server.
3. Click the **Start Kserver** button on the System > **Configure** *(page xxviii)* page.

Note: Creating indexes manually or through the SQL tuning advisor on the `ksubscribers` database can cause errors during Reapply-Schema and when upgrading to new versions of Kaseya and is strongly discouraged.

Default Settings

System > Server Management > Default Settings

The **Default Settings** page specifies default settings for server management and a file upload whitelist.

Default Settings tab

- **Default value for Time on Schedule** - Sets the default time to use for scheduling, using either agent time scheduling or server time scheduling. Applies only to schedulers that support agent time scheduling.
- **Discovery - Domain Watch policies "Include new Computers/Contacts" include moved objects** - If a policy is applied to an OU/Container that has "Include New Computers" or Include new Contacts" checked, and:
  - This option is Y, then the policy is applied to computers or contacts moved into the OU/Container.
  - This option is N, then the policy is not applied to computers or contacts moved into the OU/Container.
- **Discovery - Staff record "View All Tickets" enabled** - If checked, the **View All Tickets** *(page xxv)* checkbox is checked when the staff member record is created.
- **Discovery - Staff record Department name assignment scheme**
  - `Assign based on Active Directory OU Name` - A department is created for the new staff record based on the OU/Container name.
  - `Assign based on Active Directory Department property` - A department is created for the new staff record based on the department name specified for the user in Active Directory.
- **Discovery - Staff record Staff name assignment scheme**
  - `Assign based on Active Directory Display name. If empty, use First name plus Last name`
  - `Assign based on Active Directory User logon name`

- Assign based on Active Directory First name plus Last name

- **Enable Agent Procedure Signing** - If yes, user saved agent procedures are signed and require approval.
- **LAN Cache - Use auto-generated administrator credentials** - If yes, then credentials are automatically created for you when you create a LAN Cache using the Agent > Configure Agent > LAN Cache > Add LAN Cache dialog. If no, this same dialog provides the option of manually specifying existing credentials for the LAN Cache you create.
- **Require email address at logon** - If yes and a user does not already have an email address specified, requires the user to enter an email address as soon as the user logs on. If no, an email address is optional.
- **Require email address for user name** - If yes, a user name record must have an email address. If no, an email address is optional. Applies only to new or renamed user names.
- **Show organizations in views with one machine group** - Controls the display of the **Machine Group** dropdown filter list at the top of every agent page. If Yes, the **Machine Group** drop-down displays every organization and every machine group as separate items. If No, organizations are not shown as separate items in the list *for organizations with one machine group only.*

  Note: If you are using the **Ticketing** module and associating tickets by organization, then this option should be set to No.

- **Use domain short name in the construction of user passwords** - If legacy AD logons were created using the **View AD Users** page in VSA 6.2 or earlier and these legacy AD logons continue to be used, then set to Yes. This enables user passwords for existing legacy AD logons to continue to be recognized. Whenever a password for an existing AD logon is reset, a newer hashing algorithm is used, based on fully qualified domain names. If legacy AD logons using the **View AD Users** page were never implemented prior to 6.3, then set this option to No.
- **Use Fast Transfer option** - If Yes, provides a faster method of transferring files from the VSA to agent machines. Requires the VSA use IIS ports 80 and 443, which must remain open on the firewall. If No, fast transfer downloads are prevented. Defaults to Yes. Applies to:
  - Patch Management for both on premises and SaaS
  - Software Deployment and Recovery for on premises only.
- **Use new Live Connect when clicking the Live Connect button in Quickview** - If Yes, Live Connect displays. If No, Quick View (Classic) displays.
- **Replace KRC with RC in KLC to allow you to enforce all screen sessions getting recorded** - Yes by default. If Yes, clicking an agent status icon runs an updated version of Kaseya Remote Control, which includes the option of recording a session. If No, clicking the agent status icon runs legacy Kaseya Remote Control, which does not include the option of recording a session.

Attachment Upload Whitelist tab

The **Attachment Upload Whitelist** tab controls the types of attachments that can be uploaded to the various rich text editors used throughout the VSA framework. A default set of file types is specified. Default file types can be deleted but not modified. Users can set the list back to only the default list of file types. Only master role users have access to this new tab.

Service Desk and **Ticketing** tickets created by inbound email only accept attachments with extensions allowed by this tab. If an attachment is not accepted during inbound email processing, a message is inserted into the description of the ticket to notify the user that the attachment was excluded and lists the supported file extensions.

License Manager

System > Server Management > License Manager

The **License Manager** page allocates machine licenses by org ID or group ID. This page also displays the number of user licenses purchased for each role type. If necessary, you can kill user sessions from the page to enable other users to logon.

Types of licenses managed include:

- Agent licenses - applies to machines by organization, group or group ID
- Role type licenses - applies to VSA users or machines by role type

Add-on module licenses only display if you have purchased and installed those add-on modules.

Agent License Counts

The following events affect agent license counts:

- An "unused" agent license is changed to "used" if a machine ID account is created and the agent installed.
- If the agent is deleted but not the account, the agent license is still considered "used".
- If the account is deleted, regardless of what happens to the agent, the agent license goes back to "unused".
- If an account is created, but the agent is not yet installed the first time, the account is called a machine ID template. Machine ID template accounts are not counted as "used" until you install the agent.

General tab

The **General** tab displays the products you have purchased.

Update Code...

Click the **Update Code...** to enter a new license code or reapply your existing license code.

Show License

Click **Show License** to display the current license agreement to use the VSA.

(Header Information)

Displays the following information about your VSA configuration.

- **Kaseya Managed Services Edition** - The version number of the Kaseya Server.
- **License Code** - The current license code for this Kaseya Server.
- **Expiration Date** - The current expiration date for running the system "as is" with the current license code.
- **Maintenance Expiration Date** - The current expiration date of maintenance services, including upgrades and access to tech support.

Product Name Table

Displays the following information about your add-on modules.

- **Product Name** - The version number of the Kaseya Server.
- **Version** - The version number of the product.
- **Status** - The status of the product: `Installed`.
- **Latest Hotfix Level** - The latest hotfix level for the add-on module.
- **Usage Type** - The level of functionality enabled for the product. Applies across all role types. See Service Desk Licensing.

Licenses tab

The **Licenses** tab displays the number of agent-based licenses for each product you have purchased. You can allocate portions of the total number of agent licenses you have purchased for a product to specific organization and machine groups.

(License Type Table)

The license type table displays the following:

- **License Type** - Lists each product you have purchased that requires an agent-based license. This can include:
  - Agents - VSA agents
  - KBU - Workstation clients
  - KBU - Servers clients
  - KES - Endpoint Security clients.
  - KDPM - Desktop Management clients.
- **Used** - The current number of managed machines that have this product installed.
- **Max** - The maximum number of managed machines that can install this product

Change License Allocations

The total number of licenses available can be allocated to a specific organization, group or sub-group ID. Select any organization, group or sub-group in the allocation table, then click the **Change License Allocations** button.

(Allocation Table)

The allocation table displays the following:

- **Organization/Machine Group** - Lists both organizations and groups within organization in a single column. You select any row to allocate agent licenses to that row.
- **Type** - `Org` or `Group`. Machine groups can include machine sub-groups.
- **Agents Used** - The current number of managed machines that have this product installed in this organization or machine group.
- **Agents Max** - The maximum number of managed machines that can install this product in this organization or machine group.

Role Types tab

The **Role Types** tab displays the license counts you've purchased for each role type in your VSA. 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** *(page xiv)* tab and Machine Roles > **Access Rights** *(page xvii)* tab. The number of role type licenses purchased displays in the System > **License Manager** *(page xxxvi)* > Role Type tab. Each role type license specifies the number of *named users* and *concurrent users* allowed.

- **RoleType** - The name of the roletype.
- **Description** - The description of the roletype.
- **Max Named Licenses** - The maximum number of users licensed for this roletype.
- **Max Concurrent Licenses** - The maximum number of current users licensed for this roletype.

View Sessions

Click a role type, then click **View Sessions** to display a list of current VSA user sessions using that role type. You can select one or more sessions and click **Log Off Selected Sessions** to end those sessions. Use this feature to log off unnecessary sessions if a user is unable to logon because a roletype maximum of *concurrent* sessions has been reached.

Import Center

System > Server Management > Import Center

The **Import Center** page imports and exports automation solutions—user-defined data structures that can be applied to multiple agents—into and out of the VSA. This enables you to migrate automation solutions between VSAs, or import automation solutions from other solution providers. Objects may need to be shared with your scope before they display in export object drop-down lists.

Import/export types of automation solutions include:

- Packages
- Agent Procedures - Includes the option of exporting and importing folders of agent procedures. Check the **Show Only Folders** checkbox at the top of the **New Export** dialog to select a *folder* of agent procedures to export.
- Agent Templates
- Event Sets
- Service Desk Holiday
- Monitor Sets
- Monitor SNMP Sets
- Patch Policies
- Policy
- Reports
- Report Data Part
- Report Template
- Service Desk Tickets
- Service Desk Definitions
- Service Desk Message Templates
- Views

You can import or export multiple items of multiple types using a single XML. For example, you may want to import a set of agent procedures and monitor sets that are both used together for form a single automation solution.

Imports tab

Use this tab to import an automation solution XML into your VSA.

- **New Import** - Select an XML file to import, then click the **Process** button.
- **View Import Details** - Displays a history of the import.

The paging displays a log of the files you have imported.

Exports tab

Use this tab to export an automation solution XML into your VSA.

- **New Export**
  1. Select the type of automation solution to export.
  2. Select one or more items of that type to export.
  3. **Click the Continue button to add another type of automation solution.**
  4. Click the **Export** button to export. A single XML file is created that is still stored on the Kaseya Server.
  5. Click the **Download** hyperlink for the newly exported file that displays in the table grid of the Exports page.
  6. Confirm saving the file to your local machine.

- **View Export Details** - Displays a history of the export.

System Log

System > Server Management > 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.* Examples include:

- Deleting machine IDs
- Failed and successful logon attempts
- Successful Kaseya Remote Control sessions
- Starting/stopping of the Kaseya Server
- Deleting trouble tickets assigned to a group (not a machine)
- Scheduling reports

Save History to N Days

Click **Apply** to save system log events for the specified number of days.

Select Page

When more rows of data are selected than can be displayed on a single page, click the << and >> buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data.

Search

The search function acts as a filter on the **Description** field. Enter a set of words to search for and click the **Search** button. Only rows matching the search criteria are listed. Use % or * as a wild card. Use the underscore character (_) as a single character placeholder. Text is case insensitive.

> **Note:** This log data does not appear in any reports.

Statistics

System > Server Management > Statistics

- Related information is provided using Reports > Network Statistics.

The **Statistics** page displays various statistics to provide an indication that the Kaseya Server is running optimally. The statistics shown are not affected by the machine ID/group ID filter setting.

Agents currently online

Number of agents currently checking into the system.

Total Licenses Used

Number of agent licenses used.

Total Template Accounts

Number of machine ID templates defined.

Total Machine IDs

Number of machine IDs defined on the Kaseya Server, whether their agents have ever checked in or not. *Total Licenses Used + Total Template Accounts = Total Machine IDs.*

KServer CPU usage

the last 5 minutes: x%
long term average: x%

Total System CPU usage

the last 5 minutes: x%
long term average: x%

Remote Control Sessions

The number of remote control sessions relayed through the Kaseya Server that are currently active.

Pending Alerts

Alerts are processed by the background task every two minutes. This number shows how many alerts are backed up waiting to be processed by your system. If more than 0 alerts are pending, a button appears labeled **Clear Alerts** appears. Click this button to clear out all pending alerts.

Pending Patch Scan Results

The number of machines that currently have patch scan results that have been completed but not yet processed. If a Kaseya Server has a lot of patch scans that happen in a short period of time, the actual results of those scans might not appear for some time. The count is a measure of that backlog of processing.

Database Location

Displays the location of the database.

Database Size

Total size of your database. Typical systems consume about 1 to 2 MB of database size per machine ID.

Database File Path

Full path to the database on the database server machine.

Kaseya File Path

Full path on the Kaseya Server to the location of its system files.

Statistics Collected

Clicking the **statistics collected at** link displays charts of VSA server statistics.

- **Active connections** - Number of managed machines that currently have active connections to the Kaseya Server.
- **New connections in last 10 seconds** - Number of new TCP/IP connections accepted by the Kaseya Server. Agents using a connection established during a prior check-in do not contribute to this count.
- **Checkin message queue length** - Number of check-in messages waiting for processing by the Kaseya Server.
- **Command message queue length** - Number of messages, other than check-in, waiting for processing by the Kaseya Server.
- **Bandwidth - received bytes/sec** - Bytes per second input into the Kaseya Server agent port.
- **Bandwidth - sent bytes/sec** - Bytes per second output from the Kaseya Server agent port.
- **Database CPU utilization -** This number indicates the percentage of CPU utilization by the database server at the time specified. Excessively high values for prolonged periods may be an indication that this server is underpowered or could benefit from additional RAM.
- **Total connections processed since KServer start -** This number indicates the total agent connections processed by the Kaseya Server since the service last started.

- **Event log entries received in last minute** - The number of event log entries received in the last minute for the entire system.
- **Event log entries received in last five minutes** - The number of event log entries received in the last five minutes for the entire system.
- **Event log entries received in last hour** - The number of event log entries received in the last hour for the entire system.

Top scripts run in the last hour

This table lists the procedures that have run and completed execution on all online machines in the last hour, with the greatest frequency listed first. Clicking the **scripts** links displays a details page.

Top scripts pending (online machines only)

This table lists the procedures waiting to execute on all online machines, with the greatest frequency listed first. Clicking the **scripts** link displays a details page.

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 ii)* 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 ix)* 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**

- 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.

Application Logging

System > Server Management > Application Logging

The **Application Logging** page controls the logging of application activity on the application server. *This function is only visible to master role users and is used primarily by Kaseya support.*

- It is possible to set the level of logging in the log files, from `None` to `Maximum`. The amount of information in these logs depends on how much logging is in each application and the level of detail specified by the **Application Logging** configuration.
- There are also checkboxes to record the request and response. An XML file is created in `\Kaseya>Xml>Log` for each request and each response. In addition, there is an option to log transactions. When this is checked, another XML file is created in this same directory for each database update.
- There are options to filter by queue. This is to help narrow down the amount of information that goes into the log.
- The **Log** tab displays log records. This table supports selectable columns, column sorting, column filtering and flexible columns widths.

Outbound Email

System > Server Management > Outbound Email

The **Outbound Email** page maintains settings for routing outbound email generated by the Kaseya Server to a host email server. The host email server accepts outbound email and delivers it to recipients on your behalf. If the email server host requires authentication you can include a username and password.

> **Note:** These settings are typically set during the install process. You can modify them after the install using this page.

Enable/Disable Automatic Delivery

Automatic delivery of outbound email is disabled by default. You must enable automatic delivery of outbound email to send emails automatically throughout the VSA as soon as they are created.

Manual Delivery

If you disable automatic delivery, you can still send outbound email manually:

1. Click the System > Outbound Email > **Log** tab
2. Select one or more outbound emails with a status set to `Queued`.
3. Click the **Send Now** button.

Configuration

Click **Edit**. Complete the fields in the **Edit** dialog box.

- **Host Name** - The name of the host email server. Example: `smtp.mycompany.com`. If no authentication or special port number is required, then only specify values for the **Default Days to Keep Logs** and **Default Sender Email** fields.

  > **Note:** Entering `localhost` in the **Host Name** field means you are using the Kaseya Server's **IIS Default SMTP Virtual Server** to route outbound email. The **Default SMTP Virtual Server** service must be installed and running in order to send email. The service must also be able to resolve DNS addresses to route email to other SMTP servers.

- **Port** - Typically 25, but the host email server may require a different port number. Ports 465 and 587 are typically used for connecting to an SMTP email server over SSL/TLS.
- **User Name** - If required for authentication, enter the username of an account authorized to use the host email server.
- **Password** - If required for authentication, enter the password of the account.
- **Default Days to Keep Logs** - Enter the number of days to keep log outbound email entries.
- **Default Sender Email** - Enter the default From address displayed by outbound email. The From address displayed by outbound email uses the following order of precedence:
  1. If there is a From address in the **sendEmail()** step of a procedure, then that address is used.
  2. Else the sendEmail() step uses the From address provided by a linked Service Desk > **Message Template**, if the link exists and a From address is specified.
  3. Else the sendEmail() step uses the **Reply Email Address** of the Service Desk > **Incoming Email and Alarm Settings** > email reader linked to the service desk. This link between the email reader and the service desk is set using the Service Desk > Desk Definition > Properties > General > Standard Field Defaults > Email field.
  4. Else the **Default Sender Email** address set in System > **Outbound Email** is used.

Testing

If you suspect that you are not receiving emails from the Kaseya Server, click the **Test** button on this page to send test emails to various recipient addresses.

> **Note:** If `localhost` is entered in the **Host Name** field, the **Log** tab could show a sent email as successful, but still not be relayed successfully because of configuration problems with the **Default SMTP Virtual Server**.

Click **Test**. Complete the fields in the **Test** dialog box.

- **To** - The email address to send the test email.
- **Subject** - The subject line of the test email.

Logging

The **Log** tab displays a log of all outbound emails sent by the Kaseya Server. This table supports selectable columns, column sorting, column filtering and flexible columns widths.

- **Send Now** - Send or resend selected emails
- **Forward** - Forward a selected email to a different address than originally specified.
- **View** - View a selected email.
- **Delete** - Delete selected emails.

OAuth Clients

System > Server Management > OAuth Clients

The **OAuth Client** page registers clients to access your specific VSA. Registering an OAuth client ensures a customized app is authorized to provide users with extended access to VSA functionality and user data, *without having any knowledge of the user's VSA credentials.*

A registered OAuth client delegates a user's initial logon to the VSA. The VSA then returns client-specific tokens back to the app server. The app server uses these tokens to authenticate the client app. Because of OAuth delegation, neither the app server nor the client app ever has access to the VSA user's actual credentials.

After the initial logon. the client app shows the VSA user a customized view of VSA functionality and user data, based on the developer's use of VSA APIs. Typically the client app does not need to re-authenticate unless the client-specific token elapses without being refreshed by repeated use. The default is 60 days.

Note: For guidance on how to build an OAuth client that communicates with the VSA see **Using OAuth 2.0 to Access VSA APIs** *(http://help.kaseya.com/webhelp/EN/RESTAPI/9050000/UsingOAuth2.0toAccessVSAAPIs.pdf#zoom=70&navpanes=0)* .

Registration

Registering an app generates an email message that includes codes for two items:

- A `client_ID`
- A `client_secret`

An app developer uses these codes to uniquely identify their app as a trusted client with your VSA using OAuth authentication.

Actions

- **Register Client** - Registers a client app with your specific VSA. Enter the following:
  - **Client Name** - The client identifier.
  - **Redirect URL** - A URL provided by the app developer. This URL is displayed to the user when their initial logon authentication has been completed.
  - **Email** - The recipient sent an email containing the `client_ID` and `client_secret`.
- **Re-send client Credentials**
- **Delete**
- **Refresh**

Columns

- **Name** - The client name.
- **Type** - Always `confidential`. The only type of OAuth client supported at this time.
- **Redirect Url -** A URL provided by the app developer. This URL is displayed to the user when their initial logon authentication has been completed.
- **Registered By** - The VSA user who registered the OAuth Client.
- **Client Email** - The recipient sent an email containing the `client_ID` and `client_secret`.
- **Registered On** - The date of the registration.

Storage Configuration

System > Server Management > Storage Configuration

- This option only displays for master role users.

The **Storage Configuration** page sets storage log settings for all partitions. Stored log files can be viewed using the Agent > Agents > Screen Recordings page.

Header Fields

- **Location to store files** - The network location for all stored log files.
- **Length of time to keep logs** - The length of time to store log files.
- **Set tenant storage size** - The storage space allocated to each tenant.
- **Set notification threshold** - Administrators are notified when used storage exceeds this threshold.

Tenant Storage Information

- **Tenant Name**
- **Storage Used (MB)**

Customize

Color Scheme

System > Customize > Color Scheme

The **Color Scheme** page determines the set of colors displayed by the VSA environment. **Color Scheme** selection applies to all users within the same partition.

To change color schemes:

1. Select a color scheme in the middle pane.
2. Click the **Set Scheme** button.

Site Customization

System > Customize > Site Customization

The **Site Customization** page provides the following tabs for customizing the user interface *for all users*.

- **Logon Page** *(page xlv)*
- **Site Header** *(page xlvi)*
- **Agent Icons** *(page xlvi)*
- **Deploy Header** *(page xlvii)*
- **Org Custom Field Title** *(page xlviii)*

Each tab is edited separately.

Logon Page

System > Customize > Site Customization > 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 ii)* 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.
   - **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.
   - **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** *(page xlv)* 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 iv)*.
   - **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.

Site Header

System > Customize > Site Customization > Site Header

1. Click the **Edit** button on the **Site Header** tab. The **Edit Site Header** dialog displays.
2. The following settings can be customized:
   - **Logo** - Browse to select a custom logo on your local machine or network. Click the **Default** button to reset back to the default.

     Note: By default, VSA report headers display the image specified by the System > Site Customization > **Site Header** *(page xlvi)*. Changing the value in the System > Configure > **Change Reporting Config...** *(page xxxii)* > **Logo** field overrides this default, changing the URL *for report headers only*. Changing the URL in the Change Reporting Config... > **Logo** field does not affect the display of the **Site Header** image.
   - **Title** - Enter a custom title that displays next to the logo. Click the **Default** button to reset back to the default.
   - **Header Height** - The header height in pixels. Defaults to 50.
   - **Favorites Icon** - When your VSA website is bookmarked in a browser, this "favicon" image displays next to the text of the bookmark. Customize this image using a 16x16 pixel ico file.

     Note: The **Favorites Icon** is not supported in a SaaS-based VSA.

Agent Icons

System > Customize > Site Customization > Agent Icons

1. Click the **Edit** button on the **Agent Icons** tab. The **Edit Agent Icons** dialog displays.
2. Upload customized Windows icons to the Kaseya Server. Windows icons must be in .ico format, the color depth must not exceed 256 colors. The maximum size of 32x32 pixels is recommended.
   - **Agent online** - The agent is checking in successfully.
   - **Agent offline** - The agent is not checking in.
   - **Agent blinking** - A message is waiting to be read by the machine user.

- **Remote control is disabled** - Remote control of the managed machine has been disabled by the machine user.

3. Upload customized Mac icons to the Kaseya Server. Mac icons must be in .tif format, the color depth must not exceed 32 bit color. The maximum size of 48x48 pixels is recommended.
   - **Agent online** - The agent is checking in successfully.
   - **Agent offline** - The agent is not checking in.
   - **Agent blinking** - A message is waiting to be read by the machine user.
   - **Remote control is disabled** - Remote control of the managed machine has been disabled by the machine user.

   > **Note:** Custom Mac icon images do not display in the **Site Customization** page, but display correctly when an agent install package is subsequently created and installed on a Mac machine.

4. Upload customized Linux icons to the Kaseya Server. Linux icons must be in .png format, the color depth must not exceed 256 colors. A size of 24x24 pixels is recommended.
   - **Agent online** - The agent is checking in successfully.
   - **Agent offline** - The agent is not checking in.
   - **Agent blinking** - A message is waiting to be read by the machine user.
   - **Remote control is disabled** - Remote control of the managed machine has been disabled by the machine user.

> **Note:** See **Creating Custom Agent Icons** *(page xlviii)* for more information.

Deploy Header (Classic)

System > Customize > Site Customization > Deploy Header (Classic)

Customize the logo and text displayed when Agent > Manage Packages displays a web page to the user, instructing them to install the agent.

Use the edit toolbar to add images and special formatting to the text. *Images must be uploaded rather than copied and pasted in.*

- - Hyperlink selected text. You may need to reset links copied and pasted from another source.
- - Insert a table.
- - Insert a horizontal line as a percentage of the width, or set a fixed width in pixels.
- - Indent text.
- - Outdent text.
- - Remove formatting.
- - Insert a symbol.
- - Insert an emoticon.
- - Preview the display of text and images.
- - Upload a file or image.
- - Set selected text to subscript.
- - Set selected text to superscript.
- - Toggle full screen mode for editing and viewing.

Org Custom Field Title

System > Customize > Site Customization > Org Custom Field Titles

Customize the titles of custom fields that are used to classify organizations. Assign values to custom fields using System > Manage > Org/Groups/Depts/Staff > **Custom Fields** *(page xxvi)*.

Creating Custom Agent Icons

Four Agent Icons

To incorporate custom agent icons in the system tray (Windows) or menu bar (Mac OS X) of each managed machine, create *four icons*. These icons must be named:

For Windows Agents

- `online.ico` – By default, this is the blue K icon displayed when agent is connected to the Kaseya Server.
- `offline.ico` – By default, this is the gray K icon displayed when agent is not connected to the Kaseya Server.
- `blink.ico` – By default, this is the white K icon displayed when agent requires the user to click the icon to see a message.
- `noremote.ico` – By default, this is the red K icon displayed when the user has selected the **Disable remote control** menu item from the agent popup menu.

For Mac Agents

- `macOnline.tif` - By default, this is the blue K icon displayed when agent is connected to the Kaseya Server.
- `macOffline.tif` - By default, this is the gray K icon displayed when agent is not connected to the Kaseya Server.
- `macNoremote.tif` - By default, this is the white K icon displayed when agent requires the user to click the icon to display a message.
- `macBlink.tif` - By default, this is the red K icon displayed when the user has selected the **Disable remote control** menu item from the agent popup menu.

For Linux Agents

- `linuxOnline.png` - By default, this is the blue K icon displayed when agent is connected to the Kaseya Server.
- `linuxOffline.png` - By default, this is the gray K icon displayed when agent is not connected to the Kaseya Server.
- `linuxNoremote.png` - By default, this is the white K icon displayed when agent requires the user to click the icon to display a message.
- `linuxBlink.png` - By default, this is the red K icon displayed when the user has selected the **Disable remote control** menu item from the agent popup menu.

Formatting Custom Agent Icons

For **Windows** custom agent icons:

- The format must use the Windows icon format. A simple bitmap file cannot simply be renamed using the .ico extension.
- The maximum size of 32x32 pixels is recommended.
- The color depth cannot exceed 8 bit color (256 colors).

For **Apple** custom agent icons:

- The format must be .tif.
- The maximum size of 48x48 pixels is recommended.
- The color depth should be RGB 32 bit color.

For **Linux** custom agent icons:

- The format must be .png.
- A size of 24x24 pixels is recommended.
- The color depth cannot exceed 8 bit color (256 colors).

Installing Custom Icons

1. Navigate to the System > Site Customization > **Agent Icons** *(page xlvi)* tab.
2. Click the **Agent Icons** tab.
3. Click the **Edit** button. The **Edit Agent Icons** dialog displays.
4. Click the browse button for any agent icon to select a custom agent icon on your local machine.
5. Optionally click the **Use Default** buttons to reset agent icons to their default images.

Updating Existing Agents with Custom Agent Icons

The customized agent icons are automatically deployed when updating Agents using the Agent tab > Manage Agents. You will need to check the **Force update** check box to update agents that are already at the current version.

Creating Agent Install Packages with Custom Agent Icons

Updated agent icons are included in any newly downloaded `KcsSetup` files created by Manage Package. If you have placed an agent installer `KcsSetup` file in a domain logon script, then you must re-download the `KcsSetup` file to include the updated icons and replace the file on the domain server.

Deploy Header

System > Customize > Site Customization > Deploy Header

Customize the logo, title and body text displayed when a **Deploy Agent URL** link is clicked. See the System > **Manage - General tab** *(page xxii)* for more information.

- **Logo**
- **Title**
- **Content**

Local Settings

System > Customize > Local Settings

The following settings will be applied system wide going forward from this release. These settings currently affect the **Time Tracking** and **Service Billing** modules.

Date Format

- **Format** - Selects the date format used by dates the VSA.
  - mm/dd/yyyy
  - dd/mm/yyyy
  - yy/mm/dd
- **Delimiter used** - Selects the date format delimiter used by dates in the VSA.
  - / (slash)

- - (dash)
- . (dot)

> **Note:** The time format is set in System > **Configure** *(page xxviii)*.

Number Format

- **Decimal Places** - Selects the number of decimal places used to display currency in the VSA. Accepts up to 3 decimal places.
- **Decimal Format** - Selects the decimal format used to display currency in the VSA.
  - xx,xxx.xx
  - xx.xxx,xx

Time Zone

- **Time Zone Offset (in Hours)** - Sets the *tenant time zone offset*, in hours, for reports in tenant partitions.The default timezone for all tenants is VSA server time.

Customize: Live Connect (Classic)

System > Customize > Live Connect

The **Customize: Live Connect (Classic)** page customizes **Home** tabs that display in the Live Connect (Classic) and Portal Access (Classic) windows. You can create multiple, customized **Home** tabs and save them by name.

These **Home** tabs are enabled for a particular role by checking the checkbox underneath Live Connect > Home in:

- System > User Roles > **Access Rights** *(page xiv)*
- System > Machine Roles > **Access Rights** *(page xvii)*

You can customize three sections on the default **Home** page.

- **Portal Header** - Customize the text and image displayed at the top of the **Home** tab.
- **Agent Procedures** - Provide a customized list of agent procedures that the user can run immediately from this tab.
- **Custom Links** - Provide a customized list of URLs that the user can click using this tab. For example, you could provide a URL to a website page providing technical information used to troubleshoot problems on managed machines.

Make available to All Tenants

If checked, this Home page can be added to user roles and machines roles on all tenant partitions. This option only displays for master role users.

IT Glue

System > Customize > IT Glue

VSA supports integrating with IT Glue which can be used within Live Connect. More information can be found in our **Integration guide** *(http://help.kaseya.com/webhelp/EN/ITG/9050000/#40494.htm)*. Use this page as verification that the integration is enabled.

IT Glue Configuration Settings

- **Enable integration with IT Glue** - Check mark this to enable API support for syncing with IT Glue. This gets check marked automatically when authenticating the integration from IT Glue's portal. Unchecking it will prevent syncing.
- **URL of IT Glue Server, including https://:** - This is a special URL provided by IT Glue. This gets filled in automatically when authenticating the integration from IT Glue's portal. It is not typical to edit this unless instructed by Support.

BMS Integration

Sync Configuration

VSA > System > BMS Integration > Sync Configuration

In the VSA the **Sync Configuration** page configures VSA access to data in BMS. Once the configuration is activated, BMS creates tickets for the VSA, based on ticket creation events detected in the VSA.

Prerequisites

- The *RMM Integration - Kaseya v2* record for the corresponding BMS company you wish to integrate must already be configured and enabled for your VSA.
- The **Activate Service Desk** checkbox in the VSA > **Service Desk** module—if installed—must be deactivated.

Actions

- **Edit** - Configures the BMS company account that creates tickets for this VSA.
- **Test** - Tests the connection with the BMS server and company account.
- **Resume / Enable Sync Processing**
  - Resumes creating tickets in BMS.
  - Any ticket creation events in the VSA that have occurred since sync processing was paused are forwarded to BMS.
- **Pause Sync Processing**
  - Halts ticket creation in BMS.
  - Ticket creation events continue to be queued, ready to create tickets when you resume sync processing.
- **Activate Integration Module**
  - The VSA > **Service Desk** and **Ticketing** modules will no longer create tickets for any ticket creation events in the VSA. This includes tickets created for alerts and for inbound emails.
  - The email readers for **Service Desk** and **Ticketing** will no longer be polled.

  Note: Existing tickets are not processed in this initial release of *RMM Integration - Kaseya v2*.
- **Deactivate Integration Module**
  - Ticket creation events in the VSA begin creating tickets in the **Ticketing** module.

Procedure

1. In the VSA, select the System > BMS Integration > **Sync Configuration** page.
2. Click **Edit**.
3. Enter the following in the **Edit Settings** dialog.
   - **URL of BMS Server** - Enter the URL of your BMS server.

- **Company** - Enter your BMS company name.
- **Username** - Enter a BMS login username. The BMS "root" user account is recommended. See the prerequisites in Integrating Servers v2.
- **Password** - Enter the password for your BMS login username.
- **Select Asset Push Rule**
  - `Agent Assets Only` - Only computers with agents installed on them are pushed to BMS.
  - `All Assets` - Devices without agents can be promoted to assets. Both computers and devices promoted to assets are pushed to BMS.
  - `None` - No assets are pushed to BMS.
- **Ticket Processing Rules**
  - `Deduplicate matching tickets updated within <N> hours` – Matching tickets can be sent to BMS as a single ticket with a duplicate count of X within the designated time frame.
  - `Reopen closed duplicate tickets` – Closed duplicate tickets can be reopened after synchronization to BMS.

4. Click **Test** to verify your VSA can access the BMS server.
5. Click the **Activate Integration Module**.
6. Click the **Resume/Enable Sync Processing** button.
   - Both buttons must have a green checkmark to trigger the creation of tickets in BMS.
7. Configure ticket creation events in the VSA.
8. Optionally review log entries created by the VSA for ticket requests sent to BMS
   - System > BMS Integration > **Sync Transaction Log** - Displays a log of sync transactions between the VSA and BMS.
   - System > BMS Integration > **BMS API Log** - Displays a log of REST API requests related to the integration between the VSA and BMS.

Sync Transaction Log

`VSA > System > BMS Integration > Sync Transaction Log`

In the VSA the **Sync Transaction Log** page displays a log of sync transactions between the VSA and BMS. **Sync Configuration** *(page li)* must be configured and activated to see data displayed in this page.

- A `Success - bmsTicketNumber = <ticket number>` log entry in the **Status** column displays the BMS ticket number created.
- The value displayed in the **Record Reference** column displays an additional number for the ticket in BMS. Navigate to the BMS > Service Desk > Tickets > (selected ticket) > Edit > RMM Integration > **Ticket Reference** field to see the same number displayed.

BMS API Log

`VSA > System > BMS Integration > BMS API Log`

In the VSA the **BMS API Log** page displays a log of REST API requests related to the integration between the VSA and BMS. **Sync Configuration** *(page li)* must be configured and activated to see data displayed in this page.

Index