



Kaseya User State Management

User Guide

June 8, 2008

About Kaseya

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

Copyright © 2000-2008 Kaseya. All rights reserved.

Names and products mentioned may be trademarks or registered trademarks of their respective owners.

Contents

User State	1
User State Tab.....	2
Configuring User State.....	3
Power Status	4
Power.....	5
Power Policy.....	8
Mapped Drives	9
Mapped Drives Policy.....	11
Printers	12
Printers Policy	13
Define Package	14
Desktop Settings Filter	15
Deploy Package	16
Backup.....	18
User Settings Filter.....	20
Restore	20
Stored Settings - Restore.....	22
Migrate.....	23
Stored Settings - Migrate.....	24
Install/Remove	25
Data Locations.....	26
Logs	27
Max Log Age.....	28
Index	31

Chapter 1

User State

In This Chapter

User State Tab	2
Power Status	4
Power.....	5
Mapped Drives	9
Printers	12
Define Package	14
Deploy Package	16
Backup.....	18
Restore	20
Migrate.....	23
Install/Remove.....	25
Data Locations.....	26
Logs	27
Max Log Age	28

User State Tab

The Kaseya User State Management (KUSM) add-on module provides backup, restore and migration of local user accounts, user settings, application settings, and system settings. This includes group-based policies for the definition and deployment of printers and mapped drives and system-wide policies for the definition and deployment of power management options.

In addition KUSM enables the definition and deployment of desktop standard packages. Desktop standard packages provide IT staff and MSPs a convenient way of maintaining consistency across an organization and enables the enforcement of corporate standards.

Staff and users invest a considerable amount of time customizing their user settings, application settings, and system settings, including browser bookmarks and custom-shortcuts on their system. Preserving customizations and settings during an OS or computer hardware upgrade is error prone and becomes unmanageable when migrating multiple machines at once. KUSM's user state migration allows automation of the entire process, saving staff and users valuable time.

Note: You can view Kaseya User State Management demos at <http://www.kaseya.com/resources/demo.php>

Functions	Description
Power (page 5)	Creates and maintains power policies and applies them to selected machine IDs.
Mapped Drives (page 9)	Creates and maintains mapped drives policies and applies them uniformly to selected machine IDs.
Printers (page 12)	Creates and maintains printer connection policies and applies them uniformly to selected machine IDs.
Define Package (page 14)	Creates a desktop standard package.
Deploy Package (page 16)	Installs a desktop standard package on selected machine IDs.
Backup (page 18)	Schedules a one-time or recurring backup of settings for all local user accounts on selected machine IDs.
Restore (page 20)	Schedules a restore of one or more local user accounts to a single target machine ID. Initially, you select the source machine you want to restore from.
Migrate (page 23)	Schedules a restore of user settings and one or more local user accounts to selected machine IDs.
Install/Remove (page 25)	Installs the User State Management client on selected machines.
Data Locations (page 26)	Specifies the directory to store managed settings files.
Logs (page 27)	Displays User State log data for a selected machine ID.

Configuring User State

The tasks [User State](#) can perform are organized into three general categories:

- [Policy](#) - Defines and applies [specialized](#) user setting policies for power management, directory mappings and printers.
- [Desktop Standard](#) - Defines and applies [standard](#) user settings.
- [User Settings](#) - Backs up each user's [individual](#) user settings and local user accounts and either restores them or migrates them.

Installation and Module Configuration

Regardless of which category of task you want to perform, the same general installation and module configuration steps apply.

1. Install [User State](#) clients on both source and target machines using [Install/Remove](#) ([page 25](#)).
2. Define a data location to store user settings. Typically this is a network directory that both source and target machines can access with their credentials. Applies only to *individual* user settings using [Backup](#) ([page 18](#)), [Restore](#) ([page 20](#)) and [Migrate](#) ([page 23](#)). Policies and desktop standard user settings are stored on the KServer.

Note: In general, use domain administrator credentials when managing machines using User State. See [Agent > Set Credential](#).

3. Optionally change the default maximum number of days to maintain User State log files using [Max Log Age](#) ([page 28](#)).

Configuring Policies

You can define and apply each of the three specialized [User State](#) policies separately.

- Power Management
 1. Before applying power policies to a machine, use the [Power Status](#) ([page 4](#)) page to compare existing power settings of machines to any of the power policies already defined. You can show this page to customers who are considering using the power management features in User State Management.
 2. Define power policies and apply them to target machines using the [Power](#) ([page 5](#)) page. A power policy is *not* defined by group ID, since the same power policies are applicable to multiple customers.
 3. Recheck the [Power Status](#) ([page 4](#)) page to display the conformance of machines to new or changed power policies. Optionally select the [Assigned Power Policy](#) item from the [Conformance](#) drop-down list to determine which machines do not conform to the power policy applied to the machine.
- Mapped Drives
 - Define mapped drive policies and apply them to target machines using the [Mapped Drives](#) ([page 9](#)) page. A mapped drive policy is defined by group ID, since mapped drives are typically unique to a customer site.
- Printers

- Define printer policies and apply them to target machines using the [Printers \(page 12\)](#) page. A printer policy is defined by group ID, since printers are typically unique to a customer site.

Configuring Desktop Standard Packages

A desktop standard package is an install file created to apply user settings uniformly across multiple machines, typically within the same company. For example, a company may want a set of company-specific desktop icons and internet bookmarks always available on each user's machine.

1. Create a desktop standard package using the [Define Package \(page 14\)](#) page. Typically desktop standard packages are specific to a group, but you can optionally create a desktop standard package for <All Groups>.
2. Apply a desktop standard package to one or more target machines using [Deploy Package \(page 16\)](#).

Configuring User Settings

User Settings backs up each user's **individual** user settings and local user accounts and either restores them or migrates them.

1. Schedule a one-time or recurring backup of settings for all local user accounts on selected machine IDs using [Backup \(page 18\)](#).
2. Optionally restore one or more local user accounts to a single target machine ID using [Restore \(page 20\)](#), or...
3. Optionally migrate user settings for one or more local user accounts from a source machine to multiple target machines using [Migrate \(page 23\)](#). Optionally rename or add local user accounts on the target machine.

Power Status

User State > Power Status

Similar information is provided by Reports > User State.

The [Power Status](#) page displays the conformance of machines to the the [power policy \(page 5\)](#) selected using the [Conformance](#) drop-down list. Machine counts are based on the machine ID/group ID filter and whether or not the User State client is installed on a machine.

Five gauges display the number of conforming, non-conforming, and non-supporting machines:

- [Turn off Monitor](#) - Machines matching the selected power policy monitor settings.
- [Turn off Hard Disk](#) - Machines matching the selected power policy hard drive settings.
- [System Standby](#) - Machines matching the selected power policy system standby settings.
- [System Hibernate](#) - Machines matching the selected power policy system hibernate settings.
- [Power Conformance](#) - This fifth top gauge represents a rollup of the four subordinate gauges. This is the total number of machines that conform to all four power settings.

These gauges are updated when:

- The User State client is installed on a machine using [Install/Remove](#) (page 25). You can compare the power settings of machines at the time of the install to any of the power policies already defined to determine which machines do not conform to the selected power policy.
- A power policy is applied to a machine.
- The latest audit is performed on a machine, typically on a daily basis.

Assigned Power Policy

Select the `Assigned Power Policy` item from the [Conformance](#) drop-down list to determine which machines that conform/do not conform/do not support their assigned power policy. This can help you determine which machines are non-conforming, regardless of the power policy applied to the machine.

<N> machines do not conform <power setting>

Click the link beneath any of the five gauges to see a list of non-conforming machine IDs.

<N> machines unassigned or unmonitored

Click the link beneath this top gauge to see a list of unassigned or unmonitored machine IDs.

<N> machines do not support <power setting>

Click the link beneath any of the four lower gauges to see a list of machine IDs that do not support this specialized power setting.

Note: Certain machines may not support one or more power policy settings. Typical examples include virtual machines and terminal servers. Power policies settings, if applied to these machines, are skipped.

Power

User State > Power

The [Power Policy](#) page creates and maintains power policies and applies them to selected machine IDs. A power policy determines how a machine's power management options are configured. Power management options can be set for:

- The display screen
- The hard drive
- Shut down, hibernate and stand by time periods
- Low battery warnings

You can provide your customers a significant savings in power consumption and extend the battery life of laptops *automatically* by applying a [Power Policy](#) to all your managed machines. The same policy is applied to each user on a

machine, whether they are logged in or not. A power policy is *not* defined by group ID, since the same power policies are applicable to multiple customers. A machine must have the KUSM client installed using User State > Install/Remove (page 25) to display on this page.

Note: Certain machines may not support one or more power policy settings. Typical examples include virtual machines and terminal servers. Power policies settings, if applied to these machines, are skipped. The Power Status (page 4) page identifies which machines do not support a specific power policy setting.

Predefined Power Policies

The following predefined power policies are provided by User State and cannot be changed. They are based on predefined power schemes in Windows XP. You can assign them just as you would any user-defined power policy. You should be aware that selecting a predefined power policy affects processor performance on XP machines.

Power Policy	Processor Performance Control Policy	
	AC power	DC power
Always On	None	None
Maximize Battery Life	Adaptive	Degrade
Home/Office Desktop	None	Adaptive
Portable/Laptop	Adaptive	Adaptive
Presentation	Adaptive	Degrade

Processor Performance Control Policies

Microprocessors employ different performance states:

- High voltage/high frequency states for use when processor utilization is high.
- Low voltage/low frequency states to conserve battery life.

To support these microprocessor performance states, Windows XP uses processor performance control policies. *The power policy determines the processor control policy on the target machine.*

Policy	Description
None	Highest performance state.
Adaptive	Performance state chosen according to demand.
Degrade	Lowest performance state + additional linear performance reduction as battery discharges.

Actions

This page provides you with the following actions:

- **Schedule** - Display a popup window of the following schedule options:
 - **Schedule Date/Time** - Select the date and time to schedule this task.

- **Recurrence** - Select whether to run this task once, hourly, daily monthly. If more than once, enter the number of times to run this task for the period selected.
- **Skip if offline** - Check to perform this task only at the scheduled time. If the machine is offline, skip and run the next scheduled period and time. Uncheck to perform this task as soon as the machine connects after the scheduled time.
- **Stagger by N minutes**. - You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the scan on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...
- **Apply / Cancel** - Apply or cancel these schedule options.
 - **Apply Now** - Apply a selected policy to selected machine IDs.
 - **Cancel** - Cancel schedule options for selected machine IDs.
 - **Edit** - Add, edit or delete an existing **power policy** (page 8). When adding or editing a policy you can rename the policy. The policies you create apply to all groups. To create a new policy select <Create New Power Policy> from the policy drop-down list and click **Edit**. You can **Share...** the power policies you create with other administrators or administrator roles. Built-in power policies cannot be modified and are already shared with all administrators.

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.

Machine.Group ID

The list of Machine ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.


Power Policy

The policy assigned to this machine ID.

Last Apply Time

The last time this policy was applied to this machine ID.

Skip if Machine Offline

If a checkmark  displays and the machine is offline, skip and run the next scheduled period and time. If no checkmark displays, perform this task as soon as the machine connects after the scheduled time.

Next Apply Time

The next time this policy is scheduled to be applied. Displays **as red text with yellow highlight** if the time is past due.

Period

If recurring, displays the interval for the scheduled task to recur.

Power Policy

The **Power Policy** dialog box specifies power management options. Managed machines are assigned power management policies using the **Power** (page 5) page.

Policy Name

Enter a name or change the name of this power policy.

Power Scheme

Enter how long the computer should wait before performing the following actions, based on whether the computer is either **Plugged In** or **Running on Batteries**:

- **Turn off monitor** - Typically, you turn off your monitor for a short period to conserve power.
- **Turn off hard disk** - Typically, you turn off your hard disk for a short period to conserve power.
- **System standby** - While on standby, your entire computer switches to a low-power state where devices, such as the monitor and hard disks, turn off and your computer uses less power. When you want to use the computer again, it comes out of standby quickly, and your desktop is restored exactly as you left it. Standby is particularly useful for conserving battery power in portable computers. Because Standby does not save your desktop state to disk, a power failure while on Standby can cause you to lose unsaved information.
- **System hibernate** - Hibernate saves everything in memory on disk, turns off your monitor and hard disk, and then turns off your computer. When you restart your computer, your desktop is restored exactly as you left it. It takes longer to bring your computer out of hibernation than out of standby.

Low Battery Alarm

Specify the following:

- **Activate low battery alarm when power level reaches <N> %** - If checked, an alarm is triggered if the power level reaches the specified percentage.
- **Sound Alarm** - If checked, a sound occurs if the alarm is triggered.

- **Display Message** - If checked, a message displays if the alarm is triggered.
- **When alarm goes off, the computer will:** Stand by, Hibernate, Shut down
- **Force action even if a program stops responding** - This ensures that a hung or crashed program doesn't prevent the system from reacting to the alarm.

Critical Battery Alarm

Specify the following:

- **Activate low battery alarm when power level reaches <N> %** - If checked, an alarm is triggered if the power level reaches the specified percentage. Typically this **Critical Battery Alarm** setting is a smaller percentage than the **Low Battery Alarm** setting.
- **Sound Alarm** - If checked, a sound occurs if the alarm is triggered.
- **Display Message** - If checked, a message displays if the alarm is triggered.
- **When alarm goes off, the computer will:** Stand by, Hibernate, Shut down
- **Force action even if a program stops responding** - This ensures that a hung or crashed program doesn't prevent the system from reacting to the alarm.

Advanced

Specify the following:

- **Prompt for password when computer resumes from standby**
- **Enable Hibernation** - If checked, enables hibernation as a power option.

Power Button Behavior (for Vista Only)

- **Closing lid of laptop computer will:** Do nothing, Stand by, Hibernate
- **Pressing power button on computer will:** Do nothing, Stand by, Hibernate, Shutdown
- **Pressing sleep button on computer will:** Do nothing, Stand by, Hibernate, Shutdown

Mapped Drives

User State > Mapped Drives

The **Mapped Drives** page creates and maintains mapped drive policies and applies them uniformly to selected machine IDs. Each managed machine can be assigned the appropriate set of mapped drives *automatically*, depending on the policy applied. The same policy is applied to each user on a machine, whether they are logged in or not. Applying a uniform set of mapped drives across an organization reduces user confusion over where resources are located and frees up their time for more productive tasks. It also reduces IT

support calls to implement these drive mappings manually.

Note: Ensure *credentialed users on target machines have access rights to the network directories being mapped to. In general, use domain administrator credentials when managing machines using User State. See Agent > Set Credential.*

A machine must have the KUSM client installed using User State > [Install/Remove](#) (page 25) to display on this page.

This page provides you with the following actions:

- **Schedule** - Display a popup window of the following schedule options:
 - **Schedule Date/Time** - Select the date and time to schedule this task.
 - **Recurrence** - Select whether to run this task once, hourly, daily monthly. If more than once, enter the number of times to run this task for the period selected.
 - **Skip if offline** - Check to perform this task only at the scheduled time. If the machine is offline, skip and run the next scheduled period and time. Uncheck to perform this task as soon as the machine connects after the scheduled time.
 - **Stagger by N minutes** - You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the scan on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...
 - **Apply / Cancel** - Apply or cancel these schedule options.
- **Apply Now** - Apply a selected policy to selected machine IDs.
- **Cancel** - Cancel schedule options for selected machined IDs.
- **Edit** - Add, edit or delete an existing [Mapped Drives Policy](#) (page 11). When adding or editing a policy you can rename the policy. You must assign the policy to a specific group. To create a new policy select <Create New Mapped Drive Policy> from the policy drop-down list and click [Edit](#).

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.

Machine.Group ID

The list of Machine ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.


Mapped Drive Policy

The policy assigned to this machine ID.

Last Apply Time

The last time this policy was applied to this machine ID.

Skip if Machine Offline

If a checkmark  displays and the machine is offline, skip and run the next scheduled period and time. If no checkmark displays, perform this task as soon as the machine connects after the scheduled time.

Next Apply Time

The next time this policy is scheduled to be applied. Displays **as red text with yellow highlight** if the time is past due.

Period

If recurring, displays the interval for the scheduled task to recur.

Mapped Drives Policy

The [Mapped Drives Policy](#) dialog box specifies a set of mapped drives. Managed machines are assigned mapped drives policies using the [Mapped Drives \(page 9\)](#) page.

Policy Name

Enter a name or change the name of this mapped drives policy.

(Group)

Enter the group ID this mapped drives policy applies to. Machine groups typically represent different customers or customer locations. Therefore mapped drives are usually unique for each machine group.

Drive Mappings

Add mapped drives to this policy.

1. [Mapped Drive Path](#) - Enter the path of a shared network folder using UNC notation.
2. [Mapped Drive](#) - Select the letter of the mapped drive.
3. [Add](#) - Click the [Add](#) button.

Repeat this sequence to add multiple mapped drives to this policy.

- [Edit](#) - Click [Edit](#) to change a mapped drive path and drive letter. Click [Update](#) to save your changes.
- [Delete](#) - Click [Delete](#) to delete a mapped drive from this policy.

[User State](#) >
[Mapped Drives](#) >
[Edit](#)

Printers

User State > Printers

The [Printers](#) page creates and maintains printer connection policies and applies them uniformly to selected machine IDs. Each managed machine can be assigned the appropriate set of printer connections *automatically*, depending on the policy applied. The same policy is applied to each user on a machine, whether they are logged in or not. Applying printer connections across an organization frees up user time for more productive tasks. It also reduces IT support calls to implement these printer connections manually. A machine must have the KUSM client installed using [User State > Install/Remove](#) (*page 25*) to display on this page.

Note: Ensure credentialed users on target machines have access rights to the printers specified. In general, use domain administrator credentials when managing machines using User State. See [Agent > Set Credential](#).

Determining the Printer Network Location

When editing a Printers policy, you must specify a UNC location for the network printer in the format `\\Server\Share`. To determine this printer network location:

1. Display [Properties](#) for a printer listed in your [Printers and Faxes](#) window.
2. Select the [Ports](#) tab.
3. The printer network location displays in the [Port](#) column with a checked checkbox next to it.

Actions

This page provides you with the following actions:

- [Schedule](#) - Display a popup window of the following schedule options:
 - [Schedule Date/Time](#) - Select the date and time to schedule this task.
 - [Recurrence](#) - Select whether to run this task once, hourly, daily, monthly. If more than once, enter the number of times to run this task for the period selected.
 - [Skip if offline](#) - Check to perform this task only at the scheduled time. If the machine is offline, skip and run the next scheduled period and time. Uncheck to perform this task as soon as the machine connects after the scheduled time.
 - [Stagger by N minutes](#) - You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the scan on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...
 - [Apply / Cancel](#) - Apply or cancel these schedule options.
- [Apply Now](#) - Apply a selected policy to selected machine IDs.
- [Cancel](#) - Cancel schedule options for selected machine IDs.
- [Edit](#) - Add, edit or delete an existing [Printers Policy](#) (*page 13*). When adding or editing a policy you can rename the policy. You must assign the

policy to a specific group. To create a new policy select <Create New Printer Policy> from the policy drop-down list and click [Edit](#).

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.

Machine.Group ID

The list of Machine ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.


Printer Policy

The policy assigned to this machine ID.

Last Apply Time

The last time this policy was applied to this machine ID.

Skip if Machine Offline

If a checkmark  displays and the machine is offline, skip and run the next scheduled period and time. If no checkmark displays, perform this task as soon as the machine connects after the scheduled time.

Next Apply Time

The next time this policy is scheduled to be applied. Displays **as red text with yellow highlight** if the time is past due.

Period

If recurring, displays the interval for the scheduled task to recur.

Printers Policy

The [Printers Policy](#) dialog box specifies a set of printer network locations. Managed machines are assigned printer policies using the [Printers](#) (page 12) page.

Policy Name

Enter a name or change the name of this printers policy.

(Group)

Enter the group ID this printers policy applies to. Machine groups typically represent different customers or customer locations. Therefore printers are usually unique for each machine group.

[User State >](#)
[Printers Policy >](#)
[Edit](#)

Printers

Add printers to this policy.

1. **Printer Network Location** - Enter a port for a network printer.

Note: Reference the [Properties > Ports tab > Port column](#) of a defined Printer definition on your user's computer for a list of candidate printer network ports.

2. **Make Default Printer** - If checked, this printer network location is set as the default printer.
3. **Add** - Click the **Add** button.

Repeat this sequence to add multiple printer network locations to this policy.

- **Edit** - Click **Edit** to change a printer network location. Click **Update** to save your changes.
- **Delete** - Click **Delete** to delete a printer network location from this policy.

Define Package

User State > Define Package

The [Define Package](#) page creates a desktop standard package. A desktop standard package is an install file created to apply user settings uniformly across multiple machines, typically within the same company. For example, a company may want a set of company-specific desktop icons and internet bookmarks always available on each user's machine. A machine must have the KUSM client installed using [User State > Install/Remove \(page 25\)](#) to display on this page.

To create a desktop standard package, perform the following steps:

1. **Desktop Standard Package** - Select an existing package or specify the creation of a new package.
2. **Package Name** - For a new package enter a package name. You can enter a different name to rename an existing package.
3. **Machine Group** - Select the machine group this package applies to. You can specify `<All Groups>` or a specific group. Since each group typically represents a different customer, packages are usually unique for each machine group. Only groups an administrator has access to are displayed.
4. **Desktop Settings Filter** - Select either `<Create New Desktop Settings Filter>` or an existing [Desktop Settings Filter \(page 15\)](#) and **Edit** to specify the system settings and applications settings to include in the package. You must also specify a local user account in this step that exists on the source machine specified in Step 5 below. Click **Delete** to delete an existing desktop settings filter. You can **Share...** the desktop settings filter you create with other administrators or administrator roles.
5. **Use Settings From** - Select the source machine to copy the details of each system setting or application setting selected from.

Note: This source machine must have a local user account that matches the local user account you specified for the selected Desktop Settings Filter (page 15) in Step 4.








6. **Create the Package** - Click this button to create the package.

Share...

Click [Share](#) to share a desktop standard package with individual administrators or administrator roles.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged in. Tool tip lists the login name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Desktop Standard Package Name

Lists available standard packages.

Master Machine.ID

Lists the source machine ID detailed settings are copied from to create this package.

Settings Filter Name

Lists the [Desktop Settings Filter](#) used to create this package.

Last Modified

Displays the the datestamp for the last time the package was modified. Displays `pending` if the package is being updated.

Desktop Settings Filter

The [Desktop Settings Filter](#) dialog box specifies a set of system settings, application settings and a local user account. The desktop settings filter is applied to a source machine to create a [desktop standard package](#) using [Define Package](#) (page 14). The same desktop settings filter can be applied to multiple

[User State](#) >
[Define Package](#) >
[Edit](#)

source machines to create multiple desktop standard packages.

Note: If a target machine doesn't use a particular setting, the setting is ignored during deployment.

Filter Name

Enter a name or change the name of this desktop settings filter.

Share...

Click [Share...](#) to share this desktop settings filter with other administrators or administrator roles.

Users

[Specify the source machine user](#) - For domain users, use the qualified DOMAIN\UserName format.

Settings are always defined by specific user on a specific machine. The [System Settings](#) and [Application Settings](#) you select in the [Desktop Settings Filter](#)—for the local user account you specify—is saved as part of the desktop standard package.

Note: The local user account you specify must exist on the source machine you specify. The source machine is selected in [Step 5 in the Define Package \(page 14\) parent window](#).

System Settings

Check each system setting you want to include in the package.

Application Settings

Check each application you want to include in the package.

Deploy Package

User State > Deploy Package

The [Deploy Package](#) page installs a desktop standard package on selected machine IDs. A desktop standard package is an install file created to apply user settings uniformly across multiple machines, typically within the same company. For example, a company may want a set of company-specific desktop icons and internet bookmarks always available on each user's machine. A machine must have the KUSM client installed using [User State > Install/Remove \(page 25\)](#) to display on this page.

This page provides you with the following actions:

- [Schedule](#) - Display a popup window of the following schedule options:
 - [Schedule Date/Time](#) - Select the date and time to schedule this task.








- **Recurrence** - Select whether to run this task once, hourly, daily monthly. If more than once, enter the number of times to run this task for the period selected.
 - **Skip if offline** - Check to perform this task only at the scheduled time. If the machine is offline, skip and run the next scheduled period and time. Uncheck to perform this task as soon as the machine connects after the scheduled time.
 - **Stagger by N minutes**. - You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the scan on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...
- **Apply / Cancel** - Apply or cancel these schedule options.
 - **Apply Now** - Apply a selected package to selected machine IDs.
 - **Cancel** - Cancel schedule options for selected machine IDs.
 - **Desktop Standard Package** - Select a desktop standard package to apply to selected machine 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.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged in. Tool tip lists the login name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of Machine ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.

Desktop Standard Package

The desktop standard package of user settings applied to this machine ID.

Last Apply Time

The last time this package was applied to this machine ID.

Skip if Machine Offline

If a checkmark ✓ displays and the machine is offline, skip and run the next scheduled period and time. If no checkmark displays, perform this task as soon as the machine connects after the scheduled time.

Next Apply Time

The next time this policy is scheduled to be applied. Displays **as red text with yellow highlight** if the time is past due.

Period

If recurring, displays the interval for the scheduled task to recur.

Backup

User State > Backup

The **Backup** page schedules a one-time or recurring backup of settings for all local user accounts on selected machine IDs. User state settings and local user accounts can be restored to the same machine using **User State > Restore** (page 20) or migrated to a different machine using **User State > Migrate** (page 23). A machine must have the KUSM client installed using **User State > Install/Remove** (page 25) to display on this page.

This page provides you with the following actions:

- **Show/Hide Scheduler** - Show or hide the following schedule options:
 - **Date/Time** - Enter the year, month, day, hour, and minute to schedule this task.
 - **Run every N periods** - Check the box to make this task a recurring task. Enter the number of times to run this task each time period.
 - **Stagger by N mins.** - You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the scan on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...
 - **Skip if the machine is offline** - Check to perform this task only at the scheduled time. If the machine is offline, skip and reschedule for the next day at the same time. Uncheck to perform this task as soon as the machine connects after the scheduled time.
 - **Save Schedule** - Apply schedule options to selected machine IDs. A user settings filter must be selected.
- **Backup Now** - Backup user settings and local user accounts of selected machine IDs immediately using the selected user settings filter.
- **Remove Schedule** - Removes the schedule from selected machine IDs.








- **Edit/Delete** - Add, edit or delete an existing **User Settings Filter** (page 20). When adding or editing a user settings filter you can rename the user settings filter. You can also share the user settings filter with individual administrators or administrator roles. To create a new user settings filter select <Create New User Settings Filter> from the drop-down list and click **Edit**. You can **Share...** the user settings filter you create with other administrators or administrator roles.

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.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged in. Tool tip lists the login name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of Machine ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.


User Settings Filter

The user settings filter assigned to this machine ID.

Last Store Time

The last time this template was applied to this machine ID.

Skip if Machine Offline

If a checkmark  displays and the machine is offline, skip and run the next scheduled period and time. If no checkmark displays, perform this task as soon as the machine connects after the scheduled time.

Next Store Time

The next time this machine ID is scheduled to have its user settings and local user accounts stored. Displays **as red text with yellow highlight** if the time is past due.

Period

If recurring, displays the interval for the scheduled task to recur.

User Settings Filter

The **User Settings Filter** dialog box specifies a set of system settings and application settings. The user settings filter is applied to a managed machine to create a backup of all selected settings for all local user accounts on that machine.

Note: When restoring you have the option selecting which local user accounts to restore and which settings to restore. If a target machine doesn't use a particular setting, the setting is ignored during restore.

Note: Local user accounts are stored as `domain\user`. When migrating local user accounts to a new machine, the local user accounts can be remapped to a new domain.

Filter Name

Enter a name or change the name of this user settings filter.

Share...

Click **Share...** to share this user settings filter with other administrators or administrator roles.

System Settings

Check each system setting you want to include in the backup.

Application Settings

Check each application setting you want to include in the backup.

Restore

User State >
Restore

The **Restore** page schedules a restore of one or more local user accounts to a single target machine ID. Initially, you select the source machine you want to restore from.

To display on this page:








- Both source and target machines must have the KUSM client installed using User State > [Install/Remove](#) (page 25)..
- A source machine must have previously stored its settings and local user account information using User State > [Backup](#) (page 18).

Once the source machine is selected, you are provided with the following actions:

- [Show/Hide Scheduler](#) - Show or hide the following schedule options:
 - [Date/Time](#) - Enter the year, month, day, hour, and minute to schedule this task.
 - [Stagger by N mins.](#) - You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the scan on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...
 - [Skip if the machine is offline](#) - Check to perform this task only at the scheduled time. If the machine is offline, skip and reschedule for the next day at the same time. Uncheck to perform this task as soon as the machine connects after the scheduled time.
- [Restore Now](#) - Restore a selected machine ID immediately.
- [Remove Schedule](#) - Remove a scheduled restore from a selected machine ID.
- [Save Schedule](#) - Apply schedule options to a selected machine ID.
- [Select a different source machine](#) - Change the machine you want to restore.
- [Edit Settings to Apply](#) - Edit the [Stored Settings](#) (page 22) for local user accounts, system settings or application settings to be restored. These changes apply only to the current restore, not to the source backup files.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged in. Tool tip lists the login name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine ID.Group ID

The target machine ID.group ID that user settings and local user accounts are being restored to. Click the [Select a different source machine](#) link to select a different machine ID.group ID to restore from.


Source Machine

The source machine this machine ID is being restored from.

Source User Settings Filter

The user settings filter being used to restore this machine ID. Click [Edit Settings to Apply](#) to change local user accounts, system settings and application settings being restored. These changes apply only to the current restore, not to the source backup files.

Skip if Machine Offline

If a checkmark  displays and the machine is offline, skip and run the next scheduled period and time. If no checkmark displays, perform this task as soon as the machine connects after the scheduled time.

Next Restore Time

The next time this template is scheduled to be applied. Displays **as red text with yellow highlight** if the time is past due.

Stored Settings - Restore

The [Stored Settings](#) dialog box for [Restore](#) (*page 20*) specifies a set of system settings, application settings and local user accounts. The stored settings are used to restore selected settings for selected local user accounts on a specified machine. By default the selected machine is the same machine used to create the stored settings, but a different machine can be selected.

Users

[Restore settings for all users that were stored](#) - All local user accounts and all selected settings for these local user accounts will be restored on the target machine.

[Restore settings for the following users](#) - Select local user accounts to restore. All *selected* local user accounts and all selected settings for these local user accounts will be restored on the target machine.

System Settings

Check each system setting you want to restore on the target machine.

Application Settings

Check each application setting you want to restore on the target machine.

Migrate

User State > Migrate

The [Migrate](#) page schedules a restore of user settings and one or more local user accounts to selected machine IDs. *For each target machine*, you select the source machine you want to restore from.

To display on this page:

- Both source and target machines must have the KUSM client installed using [User State > Install/Remove](#) (page 25)..
- A source machine must have previously stored its settings and local user account information using [User State > Backup](#) (page 18).








Once the source machine is selected, you are provided with the following actions:

- [Show/Hide Scheduler](#) - Show or hide the following schedule options:
 - [Date/Time](#) - Enter the year, month, day, hour, and minute to schedule this task.
 - [Stagger by N mins.](#) - You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the scan on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...
 - [Skip if the machine is offline](#) - Check to perform this task only at the scheduled time. If the machine is offline, skip and reschedule for the next day at the same time. Uncheck to perform this task as soon as the machine connects after the scheduled time.
 - [Save Schedule](#) - Apply schedule options to selected machine IDs.
- [Migrate Now](#) - Migrate a selected machine ID immediately.
- [Remove Schedule](#) - Remove a scheduled migration from a selected machine ID.

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.

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged in. Tool tip lists the login name.
-  Agent is currently offline
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of Machine ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.

Source Machine


Click the [Select Source Machine](#) link to select the source machine ID to migrate from.

Source Settings

The user settings filter used to backup user settings on the source machine. Click the [Source Settings](#) (*page 24*) link to change the local user accounts, system settings and application settings being migrated. These changes apply only to the current migration, not to the source backup files.

By default all local user accounts are selected for migration. You can also [Add Destination Users](#). Use this feature to rename an existing local user account as you migrate. After you've specified a new user, select the new user as a [Destination User](#) for an existing local user account.

Skip if Machine Offline

If a checkmark  displays and the machine is offline, skip and run the next scheduled period and time. If no checkmark displays, perform this task as soon as the machine connects after the scheduled time.

Next Restore Time

The next time this template is scheduled to be applied. Displays **as red text with yellow highlight** if the time is past due.

Stored Settings - Migrate

The [Stored Settings](#) dialog box specifies a set of system settings, application settings and local user accounts. The stored settings are used to restore selected settings for selected local user accounts on one or more machines. The assumption is the target machine is a different machine than the source machine, but you can use [Migrate](#) to restore settings to the same machine. You can optionally change the names of local user accounts as you migrate them. You can also add additional local user accounts. Local user accounts are stored as `domain\user`. When migrating local user accounts to a new machine, the local user accounts can be remapped to a new domain.

Users

[Source User / Destination User](#) - Check all the local user accounts you want to migrate. Optionally change the name each local user account on the target machine. All selected settings for these local user accounts will be restored on the target machine.

[User State >](#)
[Migrate >](#)
[Source Settings link](#)

[Add Destination Users](#) - Add local user accounts on the target machine. Enter a username and password and confirm the password. All selected settings for these additional local user accounts will be restored on the target machine.

System Settings

Check each system setting you want to restore on the target machine.

Application Settings

Check each application setting you want to restore on the target machine.

Install/Remove

User State > Install / Remove

The [Install / Remove](#) page installs the [User State Management](#) client on selected machines. The client and associated support files are typically installed to `C:\Program Files\Kaseya\Agent\User State Management`.

Note: [User State Management licenses are managed using System > License Manager](#).

This page provides you with the following actions:








- [Show/Hide Scheduler](#) - Shows or hides the following schedule options:
 - [Date/Time](#) - Enter the year, month, day, hour, and minute to schedule this task.
 - [Stagger by N mins.](#) - You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the scan on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...
 - [Skip if the machine is offline](#) - Check to perform this task only at the scheduled time. If the machine is offline, skip and reschedule for the next day at the same time. Uncheck to perform this task as soon as the machine connects after the scheduled time.
 - [Save Schedule](#) - Applies schedule options to selected machine IDs.
- [Install Now](#) - Installs the KUSM client on selected machine IDs.
- [Cancel Install](#) - Cancels pending installs or uninstalls on selected machine IDs.
- [Uninstall Now](#) - Uninstall the KUSM client on selected machine IDs.
- [Verify Now](#) - Verifies the KUSM client is installed properly on selected machine 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.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged in. Tool tip lists the login name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of Machine ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.

Installed

If checked, a KUSM client is installed on this machine ID.

Latest 4.0.0 / Version

The header displays the latest version number of the client software. The column displays the version of KUSM client software installed on the machine ID. Displays `Install Pending` if the client software is scheduled to be installed on the machine ID.

Verified

Displays a timestamp if the installation of the KUSM client on the machine ID has been verified.

Data Locations

User State > Data Locations

The [Data Locations](#) page specifies the directory to store managed settings files. Applies only to *individual* user settings using [Backup](#) (page 18), [Restore](#) (page 20) and [Migrate](#) (page 23). Policies and desktop standard user settings are stored on the KServer. A machine must have the KUSM client installed using [User State > Install/Remove](#) (page 25) to display on this page.

Note: In general, use domain administrator credentials when managing machines using User State. See [Agent > Set Credential](#).

Set

Click [Set](#) to specify the path where managed setting files are stored.

Clear

Click [Clear](#) to remove the path where managed setting files are stored.

Path for files

Enter the path where managed setting files are stored.

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.

Machine.Group ID

The list of Machine ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.

Managed Settings Path

Lists the managed settings path assigned to a machine ID.

Logs

User State > Logs

The [Logs](#) page displays [User State Management](#) log data for a selected machine ID. The log includes the date and time of the task, the success or failure of the task, the task name and specific log data, if applicable. Click the [Task Name](#) link to display details about the task performed. A machine must have the KUSM client installed using User State > [Install/Remove](#) (page 25) to display on this page.

Check-in status

These icons indicate the agent check-in status of each managed machine:



Agent has checked in



Agent has checked in and user is logged in. Tool tip lists the login name.



Agent has not recently checked in




Agent has never checked in



Online but waiting for first audit to complete



The agent is online but remote control is disabled

 The agent has been suspended

Max Log Age

[User State >](#)
[Max Log Age](#)

The [Max Log Age](#) page specifies the number of days to retain log data for user state management. Entries older than the specified maximum are automatically deleted.

A log is created for each machine every time a user state management operation runs. The log contains the date and time, result, and description of the task performed.

The list of machine IDs you can select depends on the Machine ID / Group ID filter.

A machine must have the KUSM client installed using [User State > Install/Remove](#) (page 25) to display on this page.

Set

Click [Set](#) to assign a maximum number of log days to selected machine IDs.

<N> Days








Enter the maximum number of log days for backups.

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.

Check-in status

These icons indicate the agent check-in status of each managed machine:

-  Agent has checked in
-  Agent has checked in and user is logged in. Tool tip lists the login name.
-  Agent has not recently checked in
-  Agent has never checked in
-  Online but waiting for first audit to complete
-  The agent is online but remote control is disabled
-  The agent has been suspended

Machine.Group ID

The list of Machine ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.

Max Age

The maximum number of log days assigned to each machine ID.

Index

B

Backup • 18

C

Configuring User State • 3

D

Data Locations • 26
Define Package • 14
Deploy Package • 16
Desktop Settings Filter • 15

I

Install/Remove • 25

L

Logs • 27

M

Mapped Drives • 9
Mapped Drives Policy • 11
Max Log Age • 28
Migrate • 23

P

Power • 5
Power Policy • 8
Power Status • 4
Printers • 12
Printers Policy • 13

R

Restore • 20

S

Stored Settings - Migrate • 24
Stored Settings - Restore • 22

U

User Settings Filter • 20
User State • 1
User State Tab • 2