Kaseya

The IT Management Cloud Company™

KASEYA CERTIFIED ADMINISTRATOR (KCA)

Enterprise Lab Guide

The Kaseya Certified Administrator Lab Guide provides hands-on exercises and a structured approach to building and administering automation and integrated systems management using the Kaseya Virtual System Administrator

Developed By Kaseya University

Table of Contents

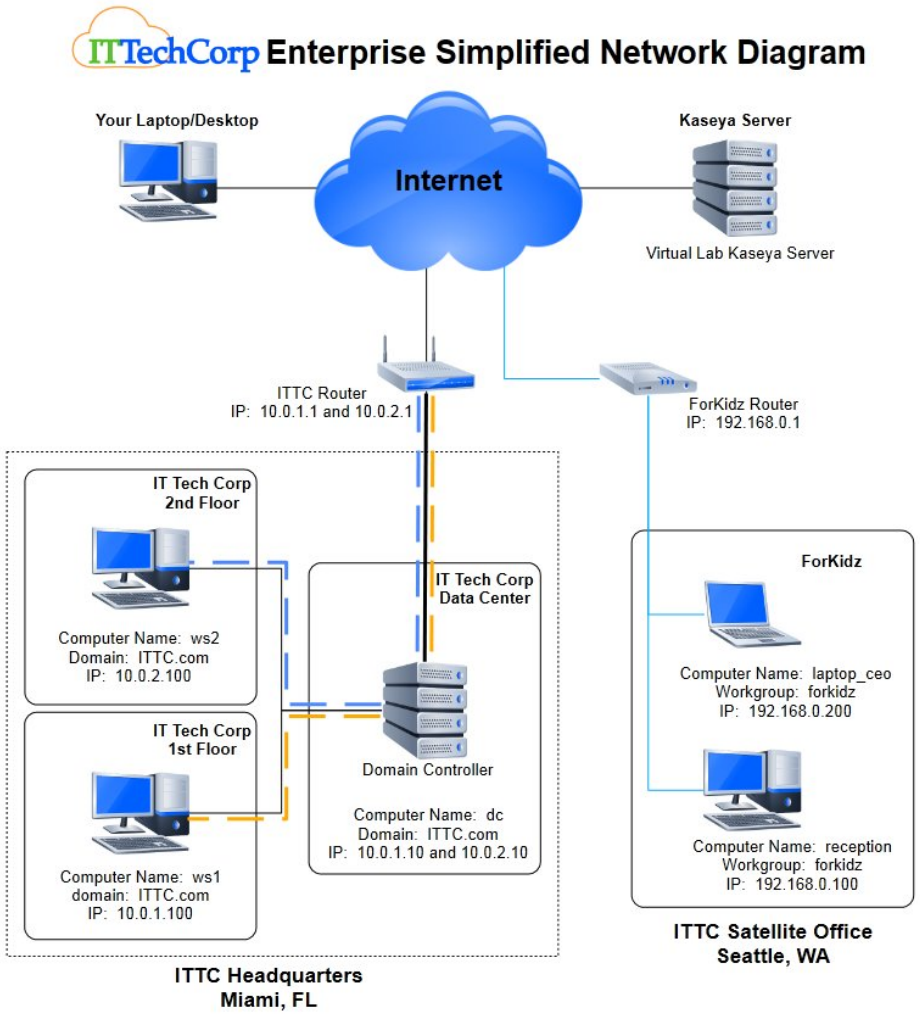
Lab Guide Overview

Welcome to the Kaseya Certified Administrator (KCA) Lab Guide. The hands-on exercises presented in this guide align directly with the courses presented in the VSA Administrator learning path and will help prepare students for the certificate exam. This lab guide uses an Enterprise-based scenario. The exercises mirror those included in the MSP scenario, but the story has been customized to mimic an Enterprise-based Kaseya deployment.

The Scenario and vLab

The exercises in this lab guide are scenario-based and tell the story of Alex, an Administrator for IT Tech Corp. IT Tech Corp is a fictitious mid-sized custom computer manufacturer which has recently purchased the Kaseya VSA to help them command centrally, manage remotely, and automate everything related to their internal IT support needs.

IT Tech Corp's main office, located in Miami, Florida, is a domain-based environment with a domain controller and several workstations. The vLab has two sample workstations and one Domain Controller representing the rest of the environment at ITTC headquarters. IT Tech Corp has a satellite office in Seattle which is responsible for the customization of kid-friendly computers for daycares and elementary schools. This office has very a basic network with one internet-connected router and several workstations. All workstations are connected via a workgroup but, due to technology limitations at the satellite office, does not have a connection to the IT Tech Corp backbone or domain. The vLab has two sample workstations representing this environment. (Network Diagram below)



Among other responsibilities, Alex was the primary admin for Active Directory at IT Tech Corp. Alex was creating GPO and VB scripts, tracking the computers in his network, and building the tools that other technicians use.

The Kaseya VSA server configuration project has been given to Alex. Alex wants to convert his current daily tasks to Kaseya and minimize the amount of individual development he has to do on a regular basis. His primary goal is to automate as many of his routine tasks as possible.

Alex is responsible for:

- getting Kaseya setup so other technicians can use the product
- adding new users, roles, scopes to define how other VSA Users will access the system
- creating the basic layout to make the Kaseya tool useful for the VSA users

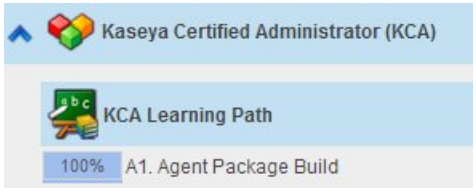
Alex is going to:

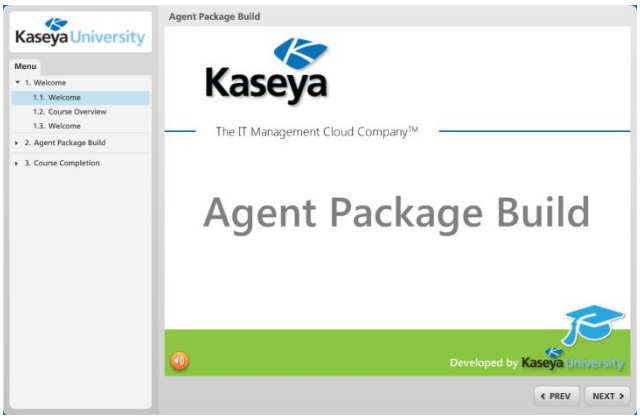
- install agents so he can remotely manage machines
- discover devices so he can install agents and remotely manage those devices
- schedule tasks to automate processes
- configure settings throughout the VSA to control how the agents behave and what info is visible, reportable, etc.
- set up a file share (LAN Cache) so machines can get files from the network to minimize internet traffic
- configure the environment so technicians can patch Microsoft updates BUT prevent any updates from installing that might be problematic or need additional testing prior to release
- keep machines updated/healthy but accommodate end user needs to limit interruption
- force compliance (Policy) and make changes on a scheduled basis (Agent Procedures)
- automatically assign settings, scripts, monitoring and other regular functions to existing machines and any new machines that are introduced into the environment.
- provide customers with regular reports on the status of devices, work accomplished, managed devices, etc.
- make the UI “look and feel” like IT Tech Corp

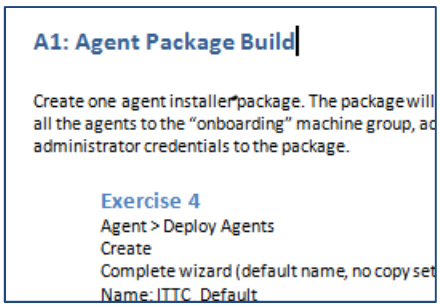
Instructions for Use

The exercises in this lab guide are designed to complement the course curriculum presented in the KCA learning path. Kaseya University recommends that you utilize this guide real-time as you work through the courses.

In order to optimize learning, in the Learning Center go to the Kaseya Certified Administrator (KCA) Learning Path, and launch and complete a course. Before moving on to the next course in sequence, open this lab guide and apply that learning using the hands-on exercises associated with specifically with the completed course before moving on to the next.







The exercises are intended to be completed IN-SEQUENCE. There is no enforcement mechanism and so the vLab does permit you to skip around. However, some of the exercises in this guide assume that prior configurations have been completed.

Finally, Kaseya University wants you to be able to do more than click through step-by-step instructions, but rather actually understand what you are doing! Thus, the exercises in this guide are written in an open-ended fashion. Should you get stuck and need help, there is an Answer Key in the back of the guide. There is often more than one way to complete the exercise. The answer key utilizes the best practice or optimal approach.

You are encouraged to do as much as you are able to without having to consult the key!

Hands-On Exercises

O1 and O2: Orientation

Alex would like to have all machines and user records belonging to IT Tech Corp grouped together and have separate groupings for each location.

Create an organization structure for IT Tech Corp. The organization needs machine groups for the endpoints and each needs an "onboarding" group for new machines. The machine groups will mirror the physical locations. IT Tech Corp has machines spread in four physical locations: a data center, on two separate floors of an office building, and the satellite ForKidz office in Seattle.

A user role, Technician, and scope are in need of creation and assignment for the VSA User, Jose Pearlman (jpearlman). Jose will be restricted to managing the machines in the ForKidz machine group and will have access to Audit and Patching configurations.

Notice about Name Clashing: Some configurations on a Cloud VSA server must be unique across the entire shared server. Where this is a requirement, we ask that you include your username as part of the configuration. When you see -<USERNAME> indicated in the lab guide, enter your VSA login name in place of the <USERNAME>. For example, if your VSA login is *awest* and you are requested to create a VSA user named jose-<USERNAME>, you would create the user jose-awest.

Exercise 1

Rename myOrg to ITTC-<USERNAME>
Create Machine Groups: "DataCenter", "FirstFloor", "SecondFloor", "onboarding", “ForKidz”

Exercise 2

Create Departments: Accounting, IT, HR, ForKidz
Create Staff record: Jose Pearlman in the IT department
Create Staff record: Samantha Jackson in the ForKidz department

Exercise 3

Create User Role: Technician with access to Audit and Patch functions
Create Scope: ForKidz. Limit the scope to machines in the ForKidz organization
Create VSA User: Create a login account for Jose Pearlman as jpearlman-<USERNAME> and assign to the Technician role and ForKidz scope

A1: Agent Package Build

In order to bring the machines under management, agents need to be installed. To get started, Alex must build an installer package.

Create one agent installer package. The package will default all the agents to the "onboarding" machine group, add the "/t" switch to the packager, and will not bind the administrator credentials to the package.

Exercise 4

The package should have the following configuration:

- Use the Computer name and associate with the ittc.onboarding machine group
- Do not copy any settings
- In addition to the default switches, add a Title of "IT Tech Corp" to the dialog box of the installer
- Do not bind credentials
- Add a package name and description and set this package as the default

A2: Agent: Manual Deploy

While automation is the ultimate goal, Alex is required to first manually deploy at least one agent into each network environment.

Install one agent into the IT Tech Corp domain network and a separate agent in the ForKidz network. Automated discovery can be used to locate additional machines once the one machine in each network has an agent. Since these vLab machines will be accessed remotely, and configure the registry to ensure the agent icon properly reflects a logged on user.

Hint: The path to the registry key is:

32 bit: HKeyLocalMachine\Software\Microsoft\Windows\CurrentVersion\Run
64 bit: HKeyLocalMachine\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

Exercise 5

Log into DC
Download and execute the agent install package

Add -remote to registry key
Verify checkin showing logged in user

Exercise 6

Log into Reception
Download and execute the agent install package

Add -remote to registry key
Verify checkin showing logged in user

A3: Agent Auto Discovery/Remote Deploy

Now that there is an agent in each environment, Alex can use Discovery to locate other computers in each environment and automatically install the agent software to all other computers found within each network.

Use the option that caters BEST for each location. (I.E. if Active Directory is predominantly used, use Discovery > Domains, if there is no Active Directory environment, use Discovery > Networks).

Configure the "Naming Policy" of the ForKidz environment to force endpoints in the ForKidz machine group to join its appropriate machine grouping based on the Default Gateway and IP Address range.

Exercise 7

Create Network using LAN Watch to scan the ForKidz network and execute the scan. LAN Watch should be configured to discover devices and install the default agent package.

Exercise 8

Configure Naming Policy to automatically move all ForKidz devices into the appropriate machine groups.

Exercise 9

Configure Domain Watch to discover devices and users in the ittc.com domain. Domain watch should automatically install the default agent package on discovered machines. Execute the scan.

A5: Agent Endpoint (to Endpoint)

With all endpoints discovered and agents installed, Alex would like to customize some of the basic settings on the agents.

Change the Working Directory to C:\ITTC and configure the Agent Menu to hide the *Exit* and *Disable Remote Control* options. Modify the Credentials used on the agent to a <USERNAME> and <PASSWORD> for the IT Tech Corp agents only (use your own lab username and password for this exercise).

Exercise 10

Configure the Working Directory to c:\ITTC for all machines

Exercise 11

Configure the Agent Menu to hide *Exit* and *Disable Remote Control* on all machines

Exercise 12

Configure the Set Credential to <USERNAME>/<PASSWORD> on the IT Tech Corp machines only

A6: Agent: Endpoint (to VSA)

Alex recognizes that the DC is not in the correct machine group. He would like to move the agent to the Data Center machine group. He also wants to ensure he's retaining log information for all machines for an appropriate period of time.

Exercise 13

Use the Agent > Change Group function to move the DC to the appropriate machine group

Exercise 14

Configure the Log History retention period to retain all agent logs for 20

A7: Agent: Agent Info

Alex knows that a user is logged into some of the endpoints, but isn't sure who. He also wants to make sure he and his technicians are aware of which machines are in which time zone. ITTC is headquartered in Miami, Florida, but their satellite office, ForKidz, is located in Seattle, Washington. The Chief Engineering Officer of Children's Technology (CEO-CT) of ForKidz, Sam Jackson, requires technicians notify her by phone prior to establishing a remote connection to her computer. Alex wants to make this information readily available to all technicians. Knowing the time zone of the endpoints will ensure technicians are conscious of contacting end users during appropriate business hours.

Exercise 15

Add the *Current* User and *Time* Zone columns to the Agent Status

BONUS ACTIVITY 1

Locate the Current User using Quick View

Exercise 16

Add the Contact for laptop-ceo
Name: Samantha Jackson
Email: sjackson@forkidz.ittc.com
Phone: 206.555.1293
Default Language: English

Exercise 17

Add an Admin note to laptop-ceo: "All techs must get verbal approval from Sam before any Remote Connection to this computer. Call only between 9am and 5pm in the user's local time zone."

Exercise 18

Add a badge to laptop-ceo: Phone Icon

T2: Tasks: Schedule and Execute

Alex knows he will be scheduling several functions throughout his work in the VSA, but he's not familiar with the scheduler utility and the variances that exist for some modules. He needs to understand the various options available and how he can best schedule tasks in ways that are healthiest for the Kaseya Server and network environments.

NO HANDS-ON LABS (scheduling will be explored in future labs)

AI1: Audit: Information Review

With Agents installed now installed, Alex would like to review some of the software and hardware information on the individual workstations.

Schedule all audits to run now. Find Disk Shares for DC and note the information shown. Find solitaire.exe (Solitaire) on endpoints using the filter grid. Navigate between both server and workstation machines and note the differences.

Create Custom Column Set that will utilize the data of Current User, Time Zone, Contact Name, Contact Email, IP Address, Connection Gateway, and Used Space.

Exercise 19

Execute a Baseline, System, and Latest Audit to run immediately

Exercise 20

Locate the disk shares configured on the Domain Controller (HINT: Use Machine Summary)
Explore available tabs

Exercise 21

Using Machine Summary and grid filters in the Audit module, find which endpoints have Solitaire installed (HINT: The Solitaire executable file is solitare.exe)

Exercise 22

Create Custom Column Set which includes:

- Current User
- Time Zone
- Contact Name
- Contact Email
- IP Address
- Connection Gateway
- Used Space

Review the data returned for the machines using the newly created Column Set

AI2: Audit: Custom Fields

Audit contains a lot of data, but there is some information that Alex needs to track on a per-machine basis which does not currently exist. Create and populate an Audit Custom Field to track a "Warranty Expiration" Custom Field on DC. Finally, edit the Custom Field to populate date one year from 'today'.

Exercise 23

Create "Warranty Expiration" Custom Field on DC
Edit Machine Data to populate date one year from 'today'

Exercise 24

Copy custom field to all machines using the Bulk Edit function
Populate the field with a date two years from ‘today’

Select machines individually and explore assigned date for each.

AI3: Audit: Manage Credentials

IT Tech Corp uses a similar credential for all of their corporate machines. However, the credential is a local administrator account for those departments in a workgroup-based environment and is a Domain Admin account for computers at headquarters. Alex would like to record the appropriate credentials for each machine based on the machine group and he would like that account configured as the Set Credential automatically.

Exercise 25

Using Audit > Manage Credentials, create a new credential for IT Tech Corp organization

- Define the credential ittcadmin with the password $uper$ecret
- Configure the credential to be the Agent Credential
- Optional: Add a descriptive note

Exercise 26

Using Audit > Manage Credentials, create a new credential for the ForKidz machine group

- Define the credential ittcadmin with the password $uper$ecret
- Configure the credential to be the Agent Credential
- Optional: Add a descriptive note

RC1: Remote Access: Theory & Architecture

Technicians at IT Tech Corp sometimes need to remote to workstations to assist end users. Periodically connecting to servers may also be required. Alex needs to ensure that any connections to corporate or client machines adhere to the business for the respective machines. NOTE: Behavior of notification polices may vary between kVNC and KRC remote connections. Refer to Remote Control Admin Guide for specific information.

Exercise 27

Configure User Role Policy for the System role with the following settings:

- If user is logged in, display alert (use the default alert or optionally customize)
- Require admin note

Exercise 28

Configure User Role Policy for the Technician role

- If the user is logged in, ask permission (use the default or optionally customize)
- Require admin note

Exercise 29

Configure Machine Role Policy for laptop-ceo

- If user is logged in, require permission
- Require admin note
- Optionally enable recording

T3: Task Views

Alex regularly needs to locate machines that have similar configurations or meet specific criteria. He wants to be able to find specific machines and then configure settings or assign tasks to all machines that meet the defined criteria. The creation of Views will help Alex to easily filter to specific agents.

Use a Machine Group Filter to filter to all machines in ForKidz. Once filtered to ForKidz, further filter to only machines containing "laptop" in the name.

Create a view to filter to All Workstation OSs, a view for All Server OSs, and finally a view to filter to machines with the Solitaire application (sol.exe) installed.

Exercise 30

Use Machine Filter toolbar to filter to all machines in ForKidz
Once filtered to ForKidz, further filter to only machines containing "laptop" in the name
Reset the filter to display all machines

Exercise 31

Create a View to filter to All Workstation-type Operating Systems
Create a View to filter to All Server-type Operating Systems
Create a View to filter to machines with the Solitaire application (solitaire.exe) installed
Explore each of the Views created

Exercise 32

Create an Advanced View to show all machines in PST time zone (HINT: Use time zone offset in hours to create this filter)

BONUS ACTIVITY 2

Edit the Solitaire View to filter to specific version of the app (HINT: Check Audit to verify the version currently installed on at least one machine)

T4: Tasks: LAN Cache

Existing configurations have saved Alex a lot of time and simplified management of his environment. He would like to create a file share on each network so he can instruct various tasks to get files from the local file share rather than each endpoint individually downloading the data from the internet. Alex knows how to create shared folders but would like an easier way to accomplish this. He would like to use the LAN Cache function to create the Share and then assign the appropriate LAN Cache to each managed machine.

Create LAN Cache on WS1 with the name of *ITTCHQ-LC*. The local folder will be named *ITTCHQ-LC* on the C: drive. Next, create a LAN Cache on the Reception machine with the Name of 4Kidz-LC. The local folder will be named '4Kidz-LC' on the C: drive.

Finally, assign the LAN Cache to the appropriate organizational endpoints.

Exercise 33

Create LAN Cache on WS1 using the following configuration:

- LAN Cache Name: ITTCHQ-LC
- Local Folder: ITTCHQ-LC
- Use the Computer Name (not IP Address) for name resolution
- The LAN Cache should be created on Drive: C:\

Exercise 34

Create LAN Cache on Reception using the following configuration

- LAN Cache Name: 4kidz-LC
- Local Folder: 4Kidz-LC
- Use the Computer Name (not IP Address) for name resolution
- The LAN Cache should be created on Drive: C:\

Exercise 35

Assign the appropriate LAN Cache to each endpoint

- Assign the ITTCHQ-LC LAN Cache to all headquarters workstations and servers
- Optionally use filters to locate the appropriate machines
- Assign the 4Kidz-LC LAN Cache to all machines in the ForKidz machine group
- Optionally use filters to locate the appropriate machines

P1: Patch: Create/Assign Policies

In order for Alex and his team to define which Microsoft Update patches will be applied to endpoints, he needs to create and assign Patch Policies. There are some patches that should be blocked for all machines across the board.

Create a "Base" policy for all workstations and servers, and name them “Base Workstations” and “Base Servers” respectively.

Alex also wants servers to have Service Packs tested before they are deployed.

Create a patch policy that blocks all service packs but allows all other patch types through.

Finally, the ForKidz department is using a web-based application that must run on IE8. These machines cannot have Internet Explorer updated beyond what they are currently running. Alex must block all IE updates from all ForKidz machines but be sure to allow all other "base" patches through, and will need a patch policy to specifically accomplish this.

Exercise 36

Create four patch policies:

- Base Workstation
- Base Server
- No Internet Explorer
- No Service Packs

Exercise 37

Assign the patch policies to the appropriate machines:

- DC: Base Servers, No Service Packs
- WS1: Base Workstations
- WS2: Base Workstation
- Laptop-ceo: Base Workstation, No Internet Explorer, No Service Packs
- Reception: Base Workstation, No Internet Explorer

P5: Patch: Scan and Status

Both the IT Tech Corp headquarters and ForKidz machines need to have Microsoft patches installed on them. In order to determine which patches are available to the machines, Alex needs to execute a patch scan.

Run a patch scan. Also schedule the patch scan to run automatically every Wednesday, during business hours, so any patches released by Microsoft that are applicable to the endpoints can be discovered.

Exercise 38

Schedule a patch scan on all machines with the following configuration:

- Every Wednesdays
- During business hours for the respective location
- Run an immediate patch scan on all machines

BONUS ACTIVITY 3

Review Patch Status to identify the installed and missing patches

P2: Patch: Patch Approval

Now that the containers for patch policies have been created, Alex wants to define which patches are actually allowed and which should be blocked. He wants Kaseya to automatically allow those patches he feels are safe, block those which need to be prevented from installation, and recognizes that sometimes he needs to handle some patches on a case-by-case basis. Alex will set the Default Approval Status to Approved for some types of patches, Denied for those he wants to block across the board, and will mark some as Pending Approval. Those in Pending he will need to process through each month or so to approve the individual patches that should be allowed and deny those individual patches that should be blocked.

For the Base Server patch policy, automatically allow all security update classifications; block Feature Packs, Tools, & Updates, and set Pending Approval for Critical, Update Rollup, and Service Packs. Verify all Products have a default approval status of Approved.

For the Base Workstations patch policy, automatically allow all security updates, service packs, critical; block Feature Pack, Tools; and set Pending Approval for Update, Update Rollup. Verify all Products have a default approval status of Approved.

For the No Service Packs patch policy, automatically allow classifications except Service Packs and block Service Packs.

Exercise 39

Set Default Approval Status on Base Server

- Approve: All security update classifications
- Manually approve all existing Security Update patches
- Deny: Feature Packs, Tools, Updates
- Manually Deny all existing Feature Packs, Tools, Updates
- Pending Approval: Critical, Update Rollup, Service Packs
    - Randomly approve some patches in these groups, deny others
- Verify all Products have a default approval status of Approved
- Check Patch > Patch Status; note the number of approved/denied patches on DC

Exercise 40

Set Default Approval Status on Base Workstation

- Approve: All security updates, service packs, critical
- Manually approve all existing patches in these classifications
- Deny: Feature Pack, Tools
- Manually deny all existing patches in these classifications
- Pending Approval: Update, Update Rollup
    - Randomly approve some patches in these groups, deny others
- Verify all Products have default approval status of Approved
- Check Patch > Patch Status; note the number of approved/denied patches on WS

Exercise 41

Set Default Approval Status on No Service Packs

- Approve: All classifications except Service Packs
- Deny: Service Packs
- Verify all Products are approved
- Manually deny all existing service packs, approve all others
- Check Patch > Patch Status; note the number of approved/denied patches on machines

Exercise 42

Set Default Approval Status on No Internet Explorer

- Approve all Classifications
- Set all Operating System-type Products to pending
- Select all patches from Pending column
- Set filter: title = *explorer*
- Deny all IE (those that match filter)
- Clear filter
- Set remaining patches to approved
- Check Patch > Patch Status; note the number of approved/denied patches on machines

Exercise 43

- Check Patch > Patch Status; note the number of approved/denied patches on machines
- Click Mixed link to show per-policy status
- Approve (or deny) one single "flavor" of a patch where multiple versions of the patch exist in the VSA
- Click Approved link to show per-policy status
- Check Patch > Patch Status; note the approved/denied number changed

BONUS ACTIVITY 4

Using Approval by Policy, find the patch approved/denied in the previous exercise. Note that the status might not match default approval status.

Exercise 44

Using Approval by Patch, identify a patch with multiple versions of same KB number
Using KB Override, deny the patch found in previous step
Using Approval by Patch, see all versions of this patch are denied

P3: Patch: Configuration - File Source and Reboot Action

Alex's technician, Jose, is ready to start deploying patches to the ForKidz computers. Before Jose starts the installs, Alex would like to make sure that the patches are not being downloaded from the internet multiple times as ForKidz has limited bandwidth. Instead of each machine getting patches directly from Microsoft, Alex would like a single LAN server to be used to retrieve the patches from Microsoft. That LAN server will then distribute the patches to the individual machines. This should prevent multiple downloads of the same file from the internet to the ForKidz network. He would like to do the same for ITTC headquarters, even though they have more bandwidth. In addition, he would like to control how the machines reboot after the patch installs execute.

Exercise 45

Configure the File Source for all machines to use LAN Cache. For the machines in the ForKidz machine group, enable the option to fail over to the internet if the LAN Cache is not available

BONUS ACTIVITY 5

Set ITTC machines to use a manually-created LAN Share

- Create share \\dc\patches at c:\patches
- Assign this UNC path and folder as the file source for ITTC headquarters machines
- Notice the notification regarding audit disk shares
- Audit > Run Audit > Run Latest Audit now
- Once Audit completes, verify the File Source notification is removed

Exercise 46

Configure the Reboot Action for all machines

- Set ITTC headquarters workstations to warn the user a reboot will occur in 10 minutes
- Set DC to reboot during the regularly scheduled maintenance window (Saturdays at 2am)
- Set ForKidz machines to ask the user if a reboot is OK but to reboot in 30 minutes if no response

P4: Patch: Pre/Post Procedures

Jose the technician has run patch cycles on several of the computers. Alex and his team are receiving alerts from Monitor when the machines reboot as part of patching. Since these reboots are expected, Alex does not want his team to have to address these alerts during a patch cycle. Instead, he would like to prevent the alerts from firing. He has also noticed that the DC behaves oddly after the reboot and would like to make sure the shutdown process complies with recommended procedures. To do so, he would like to stop the NTDS service on the DC before the reboot and start the NTDS service right after the reboot completes. Alex will need to assign pre- and post-procedures to the machines to accommodate these requests.

Exercise 47

Assign a Pre-Auto Update procedure to all ForKidz workstations(Suspend Alarms)
Assign a Post-Auto Update procedure to all ForKidz workstations(Unsuspend Alarms)

Exercise 48

Assign a pre-reboot procedure to DC to stop the NTDS service
Assign a post-reboot procedure to DC to start the NTDS service

AP1: Agent Procedures: Build and Refine

Currently, Alex must complete a number of tasks manually. He has software that needs installation, which requires sending Jose on-site. He wants to make sure the remote tag is added to the registry and doesn't want to have to remote to each computer to complete this. He wants to have the result of a net share command populated into the Agent Procedure logs, and he wants to be able to create a local user on a machine, but be able to provide the username and password at the time the procedure is scheduled to run on the machine. An email confirmation that the account was created would be nice, as well.

Exercise 49

Procedure Name: Add –remote to Registry

- add -remote to the registry value related to kausrtsk.exe. Use conditional getOS to use the appropriate registry value, depending on whether the machine is 32- or 64 bit. Write "-REMOTE ADDED" to Agent Procedure log.

Exercise 50

Procedure Name: Install 7zip

- Install 7zip using the getURL and installMSI steps. Search the web for the free 7zip installer.

Exercise 51

Create a public Managed Variable for a file share using the following configuration:
Variable Name: "FileShare"
ITTC variable value: \\dc\share
ForKidz variable value: \\reception\share

Exercise 52

Procedure Name: Install Notepad++

- Create procedure to install Notepad++ from internet using the getURL step. The procedure should download file to the appropriate managed variable, copy the file to the target machine, and silently install executable. Search the web for the free Notepad++ installer. HINT: The switch to silently install Notepad++ is /S

Exercise 53

Procedure Name: Available Network Shares

- Create a procedure to gather the results of the command shell command *net shares* to global variable; write results to Agent Procedure log.

BONUS ACTIVITY 6

- Edit the Notepad++ and 7zip procedures to create an install log. Create a procedure to execute 7zip and notepad++ installs in a single procedure without recreating the previous procedures. HINT: Use the executeProcedure step
- Parse log installer log results for "success"
- Populate a custom field with "installed" or "not installed" for each software type

Exercise 54

Procedure Name: Create Local Admin

- Create a procedure to create a local user on managed machines. At the time the procedure is scheduled, the administrator should be prompted for the username and password to create, as well as the email address to which the confirmation should be sent. These responses to these questions should be used to create the account.
- In the confirmation email, include the username and password used to create the account, as well as the machine on which the account was created.

BONUS ACTIVITY 7

Execute your procedures on managed machines

M1: Monitor: ATSE

NO HANDS-ON LABS

M2: Monitor: Monitor Sets

Note: Many of the Monitor-related labs will instruct you to use an email address as part of the alert notifications. For the purposes of these labs, please use your business email address *with ".fake"* at the end. This will prevent emails from continually flooding an inbox. For example, if Alex's email address is alex@ittc.com, he would use the email address alex@ittc.com.fake.

Alex must configure monitoring of managed endpoints within the Kaseya VSA for both ITTC headquarters machines and the ForKidz computers. He would like to avoid the need to connect to the endpoints in order to check the status of services, processes, and free space on endpoints. He has decided that he will deploy monitor sets for both Workstations and Servers within these environments. On Workstations, he must configure a monitor set to monitor available disk space (<10% free), the Windows Firewall service, and the SNMP process. On Servers, he must configure a monitor set to monitor disk space (<20% free), the windows event log service, and the SNMP process.

Exercise 55

Run Update List By Scan on DC and WS2

Exercise 56

Create Server Monitor Set

- Counter Thresholds
  - Object: Logical Disk
  - Counter: % Free Space
  - Instance: C:
  - Collection Threshold: The % Free Space data must be collected for Servers when more than 10% of the total disk space has been used. (When there is 90% free space available start collecting data)
  - Alarm Threshold: An Alarm must trigger when the alarm threshold reaches below 10% free space on the total drive of the machine. (Alarm when there is less than 10% free space available on the machine.)
- Services Check
  - Configure a Service Check for the Windows Firewall Service, which will try no attempts with a 0 minute restart interval. The re-arm for this service check must be six hours.
- Process Status
  - Create a Process Status check to alarm when the snmp.exe process is down, the re-arm period must be specified to create additional alarms every 1 hours.

Exercise 57

Create Workstation Monitor Set

- Counter Thresholds:
  - Object: Logical Disk
  - Counter: % Free Space
  - Instance: C:
  - Collection Threshold: The % Free Space data must be collected for Servers once more then 20% of disk space has been used. (When there is 80% free space available start collecting data)
  - Alarm Threshold: An Alarm must trigger when the alarm threshold reaches below 20% free space on the machine. (Alarm when there is less than 20% free space available on the machine.)
- Services Check
  - Configure a Service Check for the Event Log Service, which will try three restart attempts with a 2 minute restart interval. The re-arm for this service check must be six hours.
- Process Status
  - Create a Process Status check to alarm when the snmp.exe process is down, the re-arm period must be specified to create additional alarms every 6 hours.

Exercise 58

Assign the Server Monitor Set to DC

Exercise 59

Assign the Workstation Monitor Set to all workstations

Exercise 60

Lab 6: Individualize the Monitor Set assigned to the laptop-ceo machine. Change a setting such as the defined threshold for a counter or the number of restart attempts for a service. Commit the change and verify the monitor set appears as individualized for the machine.

M3: Monitor: Monitor Fixed Alerts

Note: Many of the Monitor-related labs will instruct you to use an email address as part of the alert notifications. For the purposes of these labs, please use your business email address *with ".fake"* at the end. This will prevent emails from continually flooding an inbox. For example, if Alex's email address is alex@ittc.com, he would use the email address alex@ittc.com.fake.

Alex needs to track some basic changes on all of his managed machines so he can be notified when configurations change, when agents fail to check in for extended periods of time, and whenever new agents are installed. He needs to make sure the router at ForKidz is active, but he does not have direct access to manage that network resource. He'll use Ping Check to ensure the IP address stays available and notify if it does not.

Exercise 61

Configure an Agent Offline alert

- Servers: Alert when offline for 1 minute with a 1 day re-arm period
- Workstations: Alert when offline for 30 days with a 7-day re-arm period
- Set all alerts to create an alarm and a ticket and send an email

Exercise 62

Configure an alert to notify when an application is installed or removed on any machine. Set the alert to create an alarm and a ticket and send an email.

Exercise 63

Configure an alert to notify when a New Agent is installed in the ForKidz organization. Configure the alert to create a ticket.

Exercise 64

Create a System Alert to run a Ping Check on the router at ForKidz site

- Use a name of your choosing
- Only alarm when service does not respond for 1 day
- Ignore additional alarms for 1 day
- Ping 192.168.0.1
- Configure the alert to create an alarm and a ticket and send an email

M4: Monitor: Monitor Event Logs

Note: Many of the Monitor-related labs will instruct you to use an email address as part of the alert notifications. For the purposes of these labs, please use your business email address *with ".fake"* at the end. This will prevent emails from continually flooding an inbox. For example, if Alex's email address is alex@ittc.com, he would use the email address alex@ittc.com.fake.

Alex has been tasked to track any error that is generated on endpoints. He does not want to scan through the logs of each machine manually to find these errors. In order to accurately and efficiently identify these errors, he will need to create an Event Log Alert to generate alarms when the errors occur. He will also need to configure a specific Event Log Alert to identify a Kaseya related error.

Exercise 65

Create Custom Event Log Alert Set with the following criteria to detect this event:

- Service Filter: *Kaseya*
- Categories: All
- Event ID: 55
- Description filter:*Kaseya Learning Error*

Exercise 66

Assign Custom Event Alert Set to all machines with the following configuration

- Enable 'Error' Log Event Log Level
- Event Log Type: Application Log
- Alert when the event occurs once
- Ignore additional alarms for 10 days
- Actions: Create an alarm, Create a ticket, Send an email

M5: Monitor: Alarms

Note: Many of the Monitor-related labs will instruct you to use an email address as part of the alert notifications. For the purposes of these labs, please use your business email address *with ".fake"* at the end. This will prevent emails from continually flooding an inbox. For example, if Alex's email address is alex@ittc.com, he would use the email address alex@ittc.com.fake.

Alex has configured and applied monitor sets to perform critical server and workstation checks. He now needs to review the alarms created based on these checks. He will also require temporary suspension of these checks to eliminate false positives during upgrades and maintenance periods.

BONUS ACTIVITY 8

Use the Alarm filter to view only some of the Alarms. If you do not have any alarms generated in your lab environment, try this task later (after alarms have had an opportunity to generate) or explore the Alarm filter in your production environment.

Exercise 67

Suspend Alarms on all machines in the ForKidz organization every weekend (HINT: You can either create two separate alarms recurring once every seven days to capture both Saturday and Sunday, or create a single recurring alarm lasting 2 full days.)

Exercise 68

Suspend Alarms on DC for 30 minutes due to emergency maintenance. Reboot DC and verify no alarms were generated during this period.

M6: Monitor: Network Monitor

Note: Many of the Monitor-related labs will instruct you to use an email address as part of the alert notifications. For the purposes of these labs, please use your business email address *with ".fake"* at the end. This will prevent emails from continually flooding an inbox. For example, if Alex's email address is alex@ittc.com, he would use the email address alex@ittc.com.fake.

Alex has been working with Jose, who is off-site at the ForKidz satellite office. Jose has informed Alex that the ForKidz would like all of their systems monitored for uptime, even ones that do not have agents installed. Alex must configure several monitors on devices in all networks to complete the monitoring setup within Kaseya. This includes CPU, Uptime, and Performance Monitoring.

NOTE: You must have completed a network discovery in the Discovery module to complete these labs

Exercise 69

Configure Monitor for non-managed assets

- Install a gateway on DC (ITTC Network Node) and Reception (ForKidz Network Node)
- Setup Credentials at the ITTC Network Node level using your Windows domain credentials and setup credentials for the ForKidz Network using non-domain credentials.
- On DC (or Gateway Machine), uncheck the 'Use WMI' option.
- Add the CPU Utilization monitor to the DC machine
- Add the SNMP monitor for the OID *System Uptime* to all workstations
- Verify and test that monitors are assigned to appropriate machines

Exercise 70

Configure an email to notify you any time any monitor triggers on any machine within the KNM Parent Level Group

BONUS ACTIVITY 9

Configure a List Reset and Create a Ticket any time any monitor within the ITTC Group triggers.

Exercise 71

Schedule Device Maintenance for DC to prevent actions from triggering during maintenance periods. Configure the schedule for 30 minutes each Saturday beginning at 10pm

Exercise 72

Create a User Notification Schedule which:

- Notifies you Monday-Friday 8am-5pm
- Notifies Jose Monday-Friday 5pm-8am

PM1: Policy Management: Policy Build

Alex has been using Kaseya for a while, and everything is working pretty well. However, he would like to minimize the amount of manual work he has to do when new machines are added to an environment. ForKidz is getting ready to replace all of their computers and ITTC is adding anew internal department. There will be a lot of work for Alex if he has to manually configure the agent settings on each of the new machines. He would like to create some Policies and let Policy Management handle the assignment of agent settings and configurations. Later, Alex will associate these policies with various machine groups and machines, but first, he needs to build them.

Exercise 73

Configure the Deployment Interval to 5 minutes
Configure Compliance Check to run daily between 6pm and 6am

Exercise 74

Create a folder called *Base Agent Settings*
Create new policy: Base Workstation
Assign the View All Workstations
Enable Policy Objects: Credential (use managed credential), log retention (15 days), agent fixed alerts (agent offline for 30 days, application removed/installed, remote control disabled), patch policies (Base Workstation), Patch Scan (weekly on Wednesdays), Auto Update (Weekly on Thursdays)
Save the policy and Apply the policy now

Create new policy called *Base Server*
Assign the View: All Servers
Enable Policy Objects: Credential (use managed credential), log retention (45 days), agent fixed alerts (agent offline for 1 minute, remote control disabled, drive space <10%), patch policies (Base Server)
Save and Apply the policy. Allow the scheduler to apply the settings.

T5: Tasks: Import/Export

Alex found some useful policies and views on http://community.kaseya.com. He's downloaded the .xml file, but he would like to import these to his server so he can use them in his own environment.

Exercise 75

- Download Learning Content Pack from http://university.kaseya.com/KaseyaUniversity/KU-ContentPack.zip
- Import the content pack using the Import Center
- Verify contents were imported (review list of views, agent procedures, monitor sets, policies, etc.)

Exercise 76

- Visit http://community.kaseya.com
- Find any procure in the community and import to your lab VSA using the Import Center
- Verify procedure imported

BONUS ACTIVITY 10

Export a procedure from lab server and import to preview or production server

PM2: Policy Management: Policy Assign

Now that Alex has built and imported several policies, he is ready to assign the policies to machines. This will allow Kaseya to be responsible for assigning the appropriate agent settings based on the agent's membership in a view, organization, machine group, etc. The DC has been behaving oddly and Alex would like to capture the logs for a longer period of time. The issue is sporadic. He would like the DC to remain "in compliance" but would like to have the logs retained for 90 days. A policy assigned directly to the DC should accomplish this exception.

Exercise 77

- Assign Base Workstation, Base Server policies at Global level
- Assign the imported *Logs and Working Directory* Policy, inside the Kaseya University\ITTC folder, to the ITTC organization
- Assign imported folder *ITTC Floor1 Custom* to ittc.firstfloor Machine Group level
- Assign imported folder *ITTC Floor2 Custom* to ittc.secondfloor Machine Group level

Exercise 78

- Reorder policies within the ITTC organization-level folder; check settings on machines
- Reorder policies within the ITTC group-level folders; check settings on machines

HINT: Use Policy > Machines to determine whether policies are re-ordered for individual machines. Optionally verify settings in the modules. If settings have not taken effect, wait a few minutes and re-check or reprocess the policies now.

Exercise 79

- Using the Agent module, set All Log Settings to 90 days for DC to create an override
- Check the policy compliance status for DC (DC should be flagged as *Manual Override*; if it is not, wait a few minutes and refresh the page or reprocess policies and refresh the page)
- Use the Compliance Status icon to view the override
- Clear Override and Reprocess Policies
- Note the DC is back in compliance (reprocess policies and/or refresh the page, if necessary)

Exercise 80

Assign the *Log History – 90 Days* from the imported content to the DC
Using the Agent module, check log retention settings on DC

SM1: Standard Solutions Package (IT Services Delivery Kit)

Alex has a pretty good thing going. He's managed to get the ITTC organization configured and the machines are being well managed. Alex has recently learned about the Standard Solution Content Pack and would like to test the use of this standard set of recommended configuration solutions on the ITTC organization.

Exercise 81

Configure the System Management utility for the ITTC organization

- Enable all options in the wizard, including severity-level emails
- Verify the download completes, which may take several minutes, in Info Center > Inbox

Exercise 82

Verify contents of pack are available

- Agent Procedures > Create/Schedule > System cabinet
- Monitor > Monitor Sets > System cabinet
- Views
- Policy Management > Policies > System cabinet
- Patch > Patch Policy > Create

Exercise 83

Verify assignment of policies

- Policy Management > Orgs/Machine Groups
- Verify policies have been assigned to ITTC
- Explore policy matrix, policy status icon pop-up
- Verify settings change on individual machines

Exercise 84

- Copy at least one of the Core policies to Private cabinet
- Edit at least one of the copied policies
- Assign the customized policy to at least one machine and ensure this policy has sufficient precedence to apply the customized settings

IC1: Info Center Build

Alex's manager has asked for some reports on the configuration of machines. ITTC will need to provide department managers with these reports. Alex will need to customize the data included in the reports so Jose can run the reports on a regular basis.

Exercise 85

Build Report Parts

- Build a Table report part to display the Agent Name and In Service Date (custom field)
  - Select the Audit > Machine Summary report part type and create a new Table
  - Define a Title and Description: In Service Date by Agent Name
  - Columns: Machine Id, CustomField00*
    - Note: Custom fields in report parts will not display the actual custom field name. Select the Custom Field
    - If you have defined multiple custom fields, you will need to determine which contains the required data. If you are unsure of which Custom Field is correct, create a table report part with all custom fields to identify the data contained in each Custom Field.
  - Order By: Custom Field (select the appropriate custom field) ascending
  - Do not use filters
  - Submit and preview the report part
- Build a Table report part to display all machines where the registry has been updated to add the –remote tag
  - Select the Logs > Agent Procedure Logs report part type and create a new Table
  - Define a Title and Description: Registry Key –Remote Status
  - Columns: Machine Id, Agent Procedure Name, Procedure Step Description, Log Time
  - Add –remote to Registry
  - Order by Log Time descending
  - Advanced Filter by Procedure Step Description equal to –REMOTE ADDED
  - Submit and preview the report
- Build a Pie Chart report part to display the number of machines running each operating system
  - Select the Audit > Machine Summary report part type and create a new Pie Chart
  - Define a Title and Description: Count of Machines by Operating System
  - Format: Select your preferred options
  - Data Properties:
    - Category: Operating System
    - Value: Machine ID; Alias: *# of each OS*; Aggregate: Count
  - Do not use filters
  - Submit and preview the report part
- Build a Bar Chart report part to display the top three machines missing with the least free space on C:\
  - Select the Audit > Disk Volumes report part and create a new Bar Chart
  - Define a Title and Description: Top Three Machines with Least Free Space on C:\
  - Format: Select your preferred options
  - Data Properties
    - Category: Machine id

        - Value: Free Space in MB
    - Order: Free Space in MB descending
    - Limit Type: Top 3
    - Advanced Filter: Drive equal to C
    - Submit and preview the report part
- Build a Bar Chart report part to display the top ten Microsoft applications deployed
    - Select the Audit > Applications report part and create a new Bar Chart
    - Define a Title and Description: Top 10 Microsoft Apps Deployed
    - Format: Horizontal Bar
    - Data Properties:
        - Category: Product Name
        - Value: Machine ID; Alias: # of Machines; Aggregate: Count
    - Order: Machine ID Count Descending
    - Limit to the top 10 Applications
    - Advanced Filter: Manufacturer Like Microsoft
    - Submit and preview the report part

Exercise 86

Build a Custom Report

- Change layout to include all parts created in the previous lab in the new report
- Change the report part "Top 10 Microsoft Apps Deployed" to return only the Top 5
- Save the change as new report part
- Save Report
- Run the Report immediately

Exercise 87

Create a New Report from a template

- Use the template Logs > Event Log Frequency Top 10
- Save the Report

Note: If Event Log logging is disabled or the right criteria has not been met in the logging, no data will not be shown.

Exercise 88

Create new report using a Legacy report

- Use the Executive Summary Legacy Report
- Save the Report

BONUS ACTIVITY 11

- Upload an image to Report Images
- Customize Cover Page, Header, Footer
- Create a new report; include any report parts as well as a report image
- Associate cover, header, footer with the new report
- Run the report

DS1: Domain Watch/AD Sync

Alex would like to leverage his existing Active Directory environment to automatically populate staff records and create new VSA users. He would like to use this information to assign Portal Access.

Exercise 89

Schedule AD Sync to run a Full Sync daily at 2am

Exercise 90

Create VSA users from existing AD records

- Select Jessie Pearlman and Tito Brown and create these AD Records as VSA Users
- Assign Technician Role and ForKidz scope to Jessie and Tito and save the changes
- Verify VSA users were created

Exercise 91

Create Staff records from existing AD records

- Select ~10 users from AD list and create these as Staff Members
- Save and Apply Changes
- Verify Staff records created in the ITTC organization

Exercise 92

Enable Portal Access for Staff Members using the Users and Portal Access function of Discovery

- Select user Jill Matthews and Assign the Portal User to WS1
- Leave the machine language and role at the defaults

B1: Branding: Agent Icon

Alex wants ITTC reflected on his corporate workstations. The blue "K" icon is ok, but he would prefer to represent IT Tech Corp.

Exercise 93

Customize the Agent icon on managed machines

- Download .zip from http://university.kaseya.com/KaseyaUniversity/KU-ContentPack.zip(includes agent icon files)
- Configure the Agent Icon to use the ITTC icons included in the downloaded .zip file

Exercise 94

Verify the Agent Icon updates on a managed machine

- Log into WS1 and check agent icon. Note the blue "K" still present.
- Force an update to the agent software and reboot (or logoff) the machine to ensure the settings apply
- Log into WS1 and note agent icon has been updated

BONUS ACTIVITY 12

Repeat Labs for *B1: Branding: Agent Icon* for all machines and verify agent icon on each.

B2: Branding: VSA

All of ITTC's end users now see the ITTC brand on the agent icon. Alex would like to reinforce the ITTC brand with his own technicians by configuring the Kaseya server to "look" like IT Tech Corp. He would also like the ITTC logo to appear on the web page from which the agent install package is downloaded.

Exercise 95

Set the color scheme of the VSA to Steel Blue

Exercise 96

- Configure the Site Header to use the ITTCLogo.png from the previously downloaded .zip file
- Configure the Site Header Title to: IT Tech Corp

Exercise 97

Edit the Deploy Header to use the ITTC Logo

C1: Customization: KLC

Alex's technicians have been using Live Connect quite a bit, and he'd like to find a way to add some easy-access utilities to the KLC page. He would like these to be available to his technicians, but not to customers accessing via Portal Access.

Exercise 98

Create Technicians home page tab for KLC

- New tab name: Technicians
- Welcome Text: IT Tech Corp Technicians
- Top Branding Frame URL: ITTC.com
- Add Agent Procedures: Computer Cleanup, Server Maintenance, 7zip and Notepad++ custom installer
- Add Custom Links: http://community.kaseya.com, http://ittc.com

Exercise 99

- Assign the Technicians tab to the Technicians user role and hide other homepages
- Modify user access rights to hide the registry editor from technicians
- Verify the technicians tab is available in KLC when logged in as a user with the Technician role

C2: Customization: Portal Access

Alex's technicians have found their customized homepage very useful. He would like to give similar access to his end users. He also recently learned that he can provide additional value by allowing his end users to remote to their work computers from any other machine in the world which will allow IT Tech Corp employees to be more productive. It won't cost Alex's IT budget anything (other than a few minutes of time) and he thinks his end users will love the extra access.

Exercise 100

Add Portal Access user Jack Lancaster with password $uper$ecret to Reception

BONUS ACTIVITY 13

Launch a separate browser on your machine to the virtual lab VSA. Log in as Jack Lancaster with the password created in the previous lab.

Exercise 101

Create a System Machine Role called *EndUserAccess*
Configure Access Rights to remove command shell, registry editor, task manager
Move reception, laptop-ceo into the new *EndUserAccess* machine role

BONUS ACTIVITY 14

Launch a separate browser on your machine to the virtual lab VSA. Log in as Jack Lancaster with the password created in the previous lab and verify Command Shell, Registry Editor, and Task Manager are not available.

Exercise 102:

Create Customer home page tab for KLC

- New tab name: EndUser
- Welcome Text: Welcome!
- Top branding frame URL: ITTC.com
- Add Agent Procedure: 7zip install
- Add Custom Links: ittc.com, helpdesk.ittc.com, kb.ittc.com

Exercise 103

- Assign the EndUser tab to the *EndUserAccess* machine role
- Modify access rights to view EndUser tab, hide other homepages

BONUS ACTIVITY 15

Launch a separate browser on your machine to the virtual lab VSA. Log in as JackLancaster with the password created in the previous lab and verify cmd shell, reg editor, task manager are not available.