Echo Administrator Guide Documentation

Release 4.7.0

Devon IT

May 22, 2017

Contents

Note: A NOTE indicates important information that helps to make better use of the product.

Caution: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

Warning: A WARNING indicates a potential for property damage, personal injury, or death.

Information in this publication is subject to change without notice.

THIN CLIENT
HARDWARE | SOFTWARE
EXPERTS

Rev. 2017-05

CHAPTER 1

Virtual Appliance Installation and Setup

This administration guide outlines how to install, setup, and run the Echo™ Management Platform. Required components include:

1. A 64-bit host running VMware® Workstation Player™, VMware® ESXi™, Citrix® XenServer®, or Microsoft® Hyper-V®.
2. Access to DNS and DHCP server configuration.

The instructions below are for users who wish to use an alternate method to the OVF deployment that is available.

1.1 Download and Install VMware vSphere or VMware Player

Download and install the VMware vSphere® Client or VMware® Workstation Player™ on a dedicated system. If assistance is needed to install this software correctly, please visit *http://vmware.com*.

1.2 Install Virtual Machine Setup on VMware

1.2.1 VMware ESX v5.0+

To start a virtual machine of the Management Appliance on VMware® ESX® versions 5.0 and up:

1. Launch **VMware® vCenter™ Converter™**. Have the Management Appliance files extracted so they are ready for installation. Click on **Convert Machine** to begin the installation process.
2. In **Source System**, select **VMware Workstation Player** or **other VMware virtual machine**.
3. Click **Browse** and locate the extracted Management Appliance files and select the appropriate **.vmx** file and click **Next**.
4. In **Destination System**, select the **VMware Infrastructure virtual machine** option and enter the VMware Infrastructure server credentials for an account that has administrator access to the ESX or vSphere server on which the Management Appliance is to be installed and click **Next**.
5. In **Destination Virtual Machine**, enter a name for the new Virtual Machine and select a destination for the Management Appliance on the ESX or vSphere server, then click **Next**.

6. In **Destination Location**, select an appropriate datastore where the Management Appliance will be stored. The appliance will consume approximately 11GB of hard disk space.
7. In **Options**, configurations may either be adjusted or left at default settings. When finished, click **Next**.
8. In **Summary**, verify that all the settings are correct and click **Finish**.

Note: Make sure that this is a newly downloaded appliance and not one that has been opened and run within VMware Workstation Player.

1.2.2 Installing without VMware vCenter Converter

To start a virtual machine without the use of vCenter Converter:

1. Extract the Management Appliance files. Open the VMware Infrastructure Client and connect to the ESX or vSphere server.
2. Browse the datastore where the Management Appliance will be hosted in. Once in the Datastore Browser, select the option to **Upload Folder**.
3. Browse to the location of the extracted Management Appliance folder and select it for upload. When the Management Appliance has finished uploading, return to the VMware Infrastructure landing page.
4. Create a new Virtual Machine and select the hosting server that will run the Management Appliance.
5. At the **Configuration** screen, select the Custom option to allow for a customized setup process and click **Next**. In **Name and Location**, enter a name for the new Virtual Machine and select a destination for the Management Appliance on the ESX or vSphere server, then click **Next**.
6. In **Storage**, select the datastore where the Management Appliance will be stored. This should be the same datastore that was chosen in Step 2. For the **Virtual Machine Version**, select the version best suited for the server.
7. In the **Guest Operating System** screen, select the OS type that will be used. In most cases, the Guest OS for the Management Appliance will be Linux, with the Ubuntu Linux (64-bit) version.
8. For the **CPU**, **Memory**, and **Network** screens, the default options will be acceptable in most cases. However, these can all be adjusted based on what is desired or specified. In **SCSI Controller**, select the LSI Logic Parallel option.
9. In the **Select a Disk** screen, use the "Use an existing virtual disk" option. Choosing this option will create a new **Select Existing Disk** screen. From there, locate the folder that as uploaded from the Datastore Browser in Step 2.
10. In **Advanced Options**, select a virtual device node and make any necessary adjustments. In most cases, these options can be left to their default settings.
11. Review all settings in the **Ready to Complete** screen before finalizing the virtual machine. If everything looks acceptable, click **Finish**. The appliance can now be booted up to complete the installation process.

1.2.3 VMware Workstation Player

To start a virtual machine on VMware Workstation Player:

1. Launch **VMware Workstation Player** and click **Open**.
2. Open the correct **.vmx** file located in the Echo folder.
3. The virtual appliance will immediately begin booting.

1.3 Installing on XenServer®

If the **.xva** file for the Management Appliance is available, follow these steps to set up on XenServer®:

1. Open the XenCenter® Client.
2. The server should already be listed from the initial installation of XenCenter. Select the desired server from the inventory on the left hand side.
3. In XenCenter, access **File**, then **Import** and browse to the location of the XVA file for Echo. Click **Next**.
4. Select the server where the Management Appliance will be placed on. Click **Next**.
5. Select which storage repository to use from the list and click **Import**.
6. Choose the desired networking option and click **Next**.
7. Click **Finish** to complete the process.

1.4 Installing on a Hyper-V® Server

If the **.vhd** file for the Management Appliance is available, follow these steps to set up on Hyper-V® server:

1. Open the Hyper-V® Manager.
2. If necessary, right click on Hyper-V® Manager in the left hand column and select **Connect to Server...**, then click **Ok**.
3. Click on **Action**, then **New**, followed by **Virtual Machine** on the right hand side. Click **Next**.
4. Name the management server. Click on **Browse** and navigate to the location where the files will be stored. Click **Next.**
5. If applicable, select the generation of the virtual machine. Select **Generation 1** and click **Next** to continue.
6. Designate the amount of RAM (1024MB minimum) that will be allocated to the Hyper-V® server. Click on **Next**.
7. Select the connection to use from the dropdown menu and click **Next.**
8. Click on **Use an existing virtual hard disk** and then click **Browse**. Navigate to the **.vhd** file and click **Next**.

9. Confirm that the information presented is accurate. Click **Previous** to make any adjustments, or **Finish** if everything is correct.

1.5 First Run Configuration

1.5.1 Password and Time Zone Configurations

1. Turn on the Virtual Machine.
2. After the boot up process is complete, the **Setting Password** page is displayed.
3. Enter a password for the default **bwadmin** account. This password is required to initially log in to management platform.

Note: There is no minimum character limit required when entering a new password and the password is case sensitive. It is recommended that the administrator create a password of at least six characters, using a combination of upper and lowercase alphanumeric characters.

---

4. Once a password has been entered, use the arrow keys to navigate to the **OK** button and press to continue. A prompt will appear, asking for the password to be entered a second time. Press the **OK** button again.
5. A list of locations is displayed in the **Change Time Zone** page. Select the appropriate time zone and press .

1.6 Network Configuration

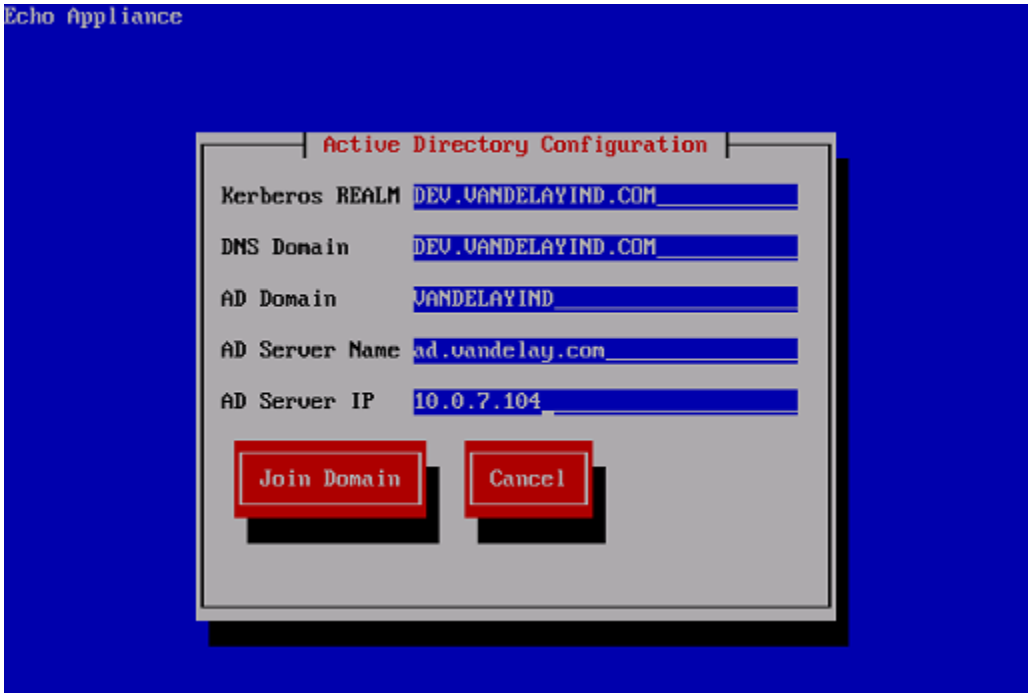
After the password and time zone have been configured, the next step of the initial setup wizard is to determine the IP configuration.

1. Enter a static IP address for this instance of the management platform, and press **OK**.
2. On the next page will be a prompt to enter the subnet mask. Typically, this will be a class C subnet mask (`255.255.255.0`). Once the subnet mask has been filled in, press **OK**.
3. On the **Configure Gateway** page, enter the gateway IP address and press **OK**.
4. On the **Configure DNS Nameservers** page, enter the IP addresses of the nameservers, using a space in between each address. This will allow the appliance to resolve domain names. Once the IP addresses have been entered, press **OK**.
5. In the **Configure DNS Search Domains** page, enter the DNS search path for the domain. If there are multiple domains, separate the entries with a space. Once all domains have been entered, press **OK**.
6. After selecting **OK**, the network interface will restart and the **Main Menu** will display.

1.7 Active Directory

Echo supports Active Directory Integration, which will allow Active Directory accounts to be used instead of the default `bwadmin` credentials.

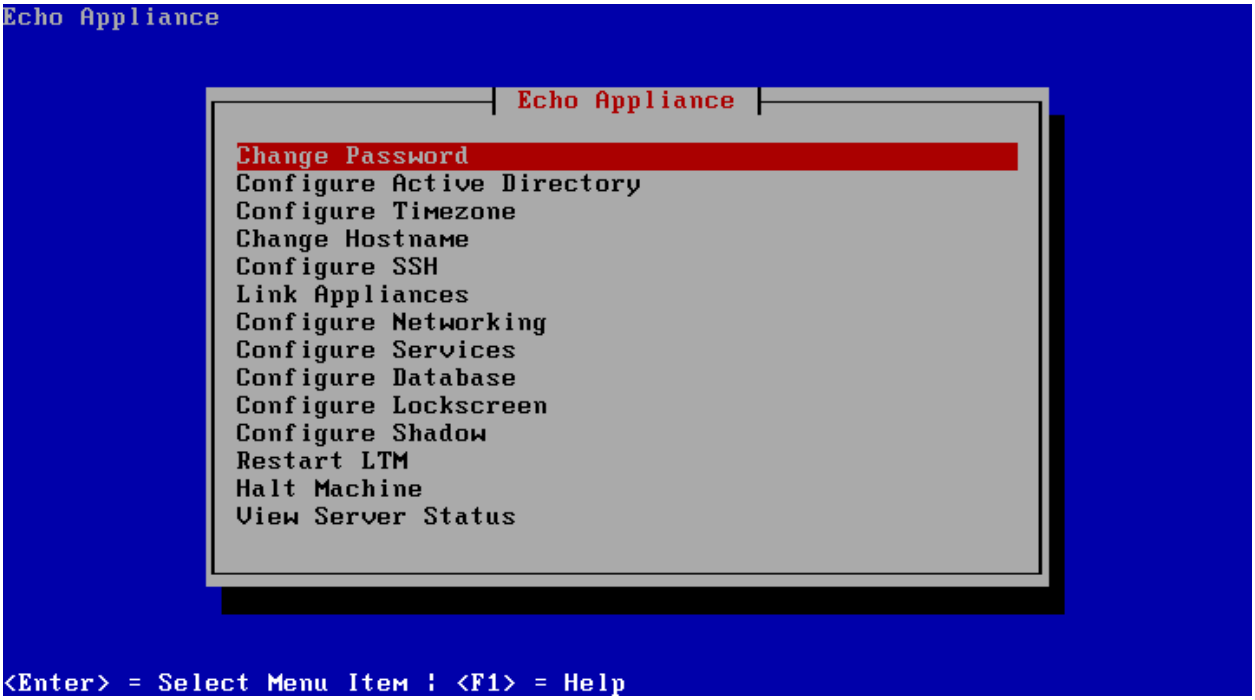
Note: Before continuing, verify that both Active Directory is currently running, and that there is a currently working installation of the Echo Appliance.



1. Access the Echo Administrator Console and select "*Configure Active Directory*". After that, the following fields will need to be completed:
   - **KERBEROS Realm** - Enter the domain name. (ex: `DOMAIN.COM`).
   - **DNS Domain** - Enter the DNS domain name. (ex: `DOMAIN.COM`)
   - **AD Domain** - Enter the Active Directory domain name. (ex: `DOMAIN`)
   - **AD Server Name** - Enter the hostname of the domain controller. (ex: `dc.domain.com`)
   - **AD Server IP** - Enter the IP Address of the domain controller. (ex: `192.168.1.100`)
2. Select *Join Domain* and authenticate with an Active Directory Administrator account. Once this is complete, Echo will state that it has successfully joined the domain and then restart the Appliance. To begin using Active Directory accounts to login to the Web Application, refer to the *Permissions* section.
3. If necessary, create a new Security Group in Active Directory. Otherwise, existing Active Directory groups will be suitable. If this group will require specific permissions when accessing Echo, these will be set in the **Permissions** section of the Web Application.

1.8 The Main Menu

Once initial setup process is complete, the **Main Menu** screen becomes the starting point for all future appliance configurations.



1.8.1 Main Menu Options

Change Password This options will change the password for the default administrator account. The default password is set upon starting the appliance for the first time and can be changed at any time. There is no character limit, so it is recommended to set a password that is memorable, but secure.

Configure Active Directory Used to configure integration with Active Directory for user credentials. Integrating with Active Directory will allow credentials from the Active Directory to be used, in addition to the default *bwadmin* account. For more on Active Directory, refer to the activedirectory-reference section or the *Permissions* section.

Configure Timezone The time zone can be configured based on the current location of the server. By default, this is set to the **America/New York** time zone.

Change Hostname Select this to change the hostname of the Echo server. This may be done for cases where it is desirable to assign a hostname that is more relevant to the server. The default hostname is ws-broker.

Link Appliances This option allows two Management Appliances to link together, if they share a database. A database will need to be configured beforehand. This option may also be ideal for administrators who wish to use the AMQP protocol with their setup.

Configure SSH Select this to configure the built-in SSH server. Enabling **SSH** will allow remote access to the command line of the management server.

Configure Networking The network options of the Management Appliance can be configured. The following settings can be adjusted:

Configure Network Interfaces This option modifies the static network settings.

Configure Routes This option modifies the local routing table.

Configure Database The management server can be configured to use external PostgreSQL, MSSQL, and MySQL databases. By default, it uses it's own internal MySQL Database. This database can be configured at any time. This is required for linking appliances together.

Configure Lockscreen The timeout period for the lockscreen can be adjusted, as well as disabled. Disabled lockscreens can be re-enabled at any time.

Configure Shadow This configures the way the Management Server handles Shadow sessions. By default, the Management Server will allow ten Shadow sessions running at one time among all active users and sessions. Any other attempts to Shadow a device will be rejected until one of the other ten sessions has concluded. The number of allowed Shadow sessions can be adjusted to accommodate for current network speed. There are also fields to tell the Management Appliance what ports are open for Shadow to use. For more information on using Shadow, see *Shadow*.

Restart Echo This will restart the Echo server. This option is necessary for cases where the Management Server has had settings adjusted.

Halt Machine This will power off the Management Appliance. This option is necessary for cases where the Management Server may be replaced.

View Server Status This will display the current status of the server. Here, Administrators will be able to view the status of all connected servers, as well as the database connectivity status. This status screen will also inform the Administrator if the Management Appliance is currently joined to an Active Directory, and if there has been a link created with another appliance. Miscellaneous information about the current appliance version is also displayed for support purposes.

1.9 Final Configuration Steps

1.9.1 DNS Configuration

By default, devices running DeTOS™ will attempt to resolve two types of DNS records:

- A top-level, Host(A) Record named `ws-broker`.
- An SRV record named `_mgr._tcp`.

It is recommended for simple deployments that the administrator use the first approach, and create a single DNS entry for **ws-broker**, assigned to the static IP configured for the Management Appliance. For example:

- `ws-broker.myXyzConsulting.com`
- `ws-broker.HiTechSolutions.net`
- `ws-broker.development.org`

In more complicated deployments where high availability is required it is recommended that an SRV record be used instead. Assigning a number of IP addresses for multiple instances of the Management Appliance allows for management reliability in failover scenarios.

1.10 Firewall Ports

1.10.1 What Ports need to be Open for Functionality?

- **Port 80:** Used by the Management Server. HTTP – Standard web port for the appliance Web UI.
- **Port 443:** Used by the Management Server. HTTPS – Secure (SSL) communication over http protocol
- **Port 50000:** Used by the Management Server, Hosts, and Devices. Used by SOAP. This port needs to be open on ALL devices within the management environment
- **Port 5671:** Used by the Management Server, Hosts, and Devices. Used by AMQP. This port needs to be open on ALL devices within the management environment

1.11 Enable AMQP Support

It is possible to switch to the AMQP protocol on supported devices. This is an option for users who wish to use NAT transversal. To enable AMQP support:

1. If there is a firewall on the network, ensure that the following ports are open:
   - **Port 80:** HTTP - This is a standard web port for the Management Appliance WebUI.
   - **Port 443:** HTTPS - This is a secure (SSL) communication over an HTTP protocol.
   - **Port 50000:** This is used by SOAP. This port needs to be open on the Management Server environment (Bidirectional Connection Required) and all devices need to be able to reach it.
   - **Port 5671:** This is used by AMQP. This port also needs to be open on the Management Server environment.
2. Create an `ftp://` or `http://` server that can be accessed by the relevant thin clients. This server will be used to host the script that will enable AMQP support on devices. The script can be accessed from here (http://downloads.devonit.com/SalesEng/amqp/enable-amqp) for devices running DeTOS, and here (http://downloads.devonit.com/SalesEng/amqp/enable-amqp.cmd) for devices running Windows Embedded operating systems. If it is not possible to create a host server, then the links provided may also be used as a host.
3. Open the Management Appliance WebUI by browsing to the IP address or hostname of the appliance within any web browser. Log in using Administrator credentials, then open the **Devices** inventory.
4. Select one or more of the devices that will use the AMQP protocol. Click on the **Device Actions** button (the **Gear** icon) and select the **Execute a File** option. Insert the `ftp://` or `http://` location that is hosting the AMQP script and click on the **check** button to apply the script to the device(s).

To verify that a device is set to use the AMQP protocol, click on the device's information icon (the **i** button located next to the device in the device inventory). The **Protocol** of the device will be listed.

Note: Once AMQP support is enabled, port 50000 is no longer required to be open.

1.12 Check Connectivity

Using a web browser, enter the server address into the web browser address bar. A security warning may need to be bypassed to access the login page. The server can be added as a "Safe Site" to avoid security warnings in the future. If the installation and setup was performed successfully, the **Login** screen will display.

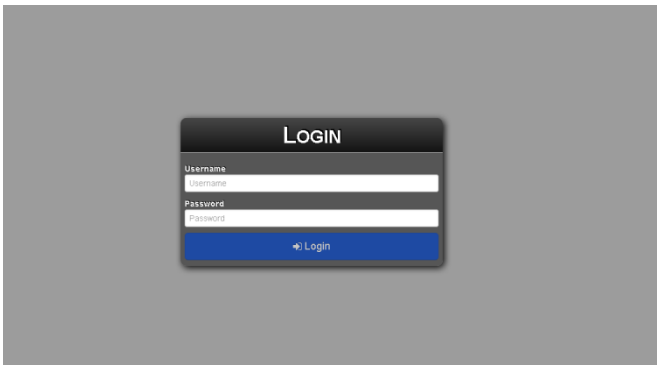
1.12.1 Troubleshooting a Bad Connection

Make sure that the appliance has network connectivity and that data packets can flow to and from the appliance. To access different virtual terminals, press and the right arrow key. Once at the terminal prompt, the following will be visible:

```
ws-broker login:
```

Log in using the username **bwadmin** and the password, which was set during the initial configuration of the appliance. Test network connectivity by pinging remote machines to ensure the appliance can see machines on the network. Also ping the appliance from a thin client to make sure the device can see the server.

If the server is not responding to any pings that are sent out or received, double-check the network settings and make sure that port 50000 is open on the network.



1.13 Additional Installation

1.13.1 Steps for Advanced Configurations

Please read the next sections only if more than one Virtual Appliance is being deployed in the same environment. If this does not apply, skip to basics-reference.

1.13.2 Configure Appliance to Use an External Database

The appliance may be connected to an external database, if desired. To configure the appliance to use an external database:

1. Select **Configure Database** from the **Main Menu**.
2. Choose the **Select and Configure a Different Database** option.
3. Choose the desired database type.
4. Enter the appropriate values for the **IP address**, **port**, **username**, **password**, and **database** fields that correlate to the external database. When finished, select **Save**.
5. Select **Restart Echo** from the **Main Menu** to activate the database connection.

CHAPTER 2

Learning Basics

2.1 Basic Terminology

The following terms are used throughout this document.

- **Device** - This is the physical thin client to which the monitor, keyboard and mouse are attached.
- **Session** - This is a network connection between a thin client and a host, with the display and USB components connected.
- **Cloning** - This is a process of copying the profiles, settings, or images from one device in order to make them available for application to other devices.

2.2 Accessing the Graphical Interface

1. Using a web browser, type the server address that was assigned to the Management Appliance into the address bar.

   Note: An untrusted connection warning may appear within the browser. This will need to be bypassed, and the Management server will need to be added as an exception.

2. Enter a username and password. This login can be the Administrator credentials that were set up during installation, or another set of credentials based on Active Directory accounts, if established. Click on the **Login** button. If properly configured, and DNS settings are correct, the **Administration Page** will display.

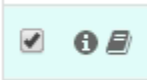
2.3 The Administration Page

The **Administration Page** is divided into two main sections. The left-hand side displays the navigation bar with the various pages the administrator can navigate to. The central area of the page is dedicated to the inventory or configuration table depending on which tab is selected. The different administration pages are briefly described below. For further instruction on each page, see the devices-reference chapter.

2.4 Devices Page

The **Devices** page is where users may view an inventory of all devices being managed by the platform. Information such as the **Name**, **IP Address**, **OS**, and other details for each device can be viewed here.

Next to each device is a **View Device** button, a **Logs** button, and a checkbox, used to select any number of devices at once. A group of devices can be selected by clicking on a device's checkbox, followed by pressing `Shift` and clicking on the last device to be selected for that group. The **View Device** button lists all available details pertaining to the device not displayed by default in the inventory, such as the Serial Number or UUID. The **Logs** button displays any logged events from the selected device(s).



2.5 Connections Page

Devices have the ability to connect to remote services utilizing a number of connection types. The **Connections** page is where users can go to create, manage, and edit any desktop connections that are available.

2.6 Profiles Page

A key function of the management platform is the creation and application of **Profiles**, in order to effectively manage the settings applied to remote devices. A profile can contain a variety of options such as connections, settings, certificates, disk images, and software packages, which can then be applied to devices according to defined rules. The **Profiles** page is where the administrator can create, manage, and edit these profiles.

2.7 Disk Images Page

A **Disk Image** is a file that can be included in order to combine different settings and profiles into one complete package. While creating **Profiles** and editing **Device Settings** provide ways to customize devices, uploading a **Disk Image** allows the administrator to combine multiple profiles and settings, as well as an operating system, into a single resource. Utilizing disk images can simplify the management process.

2.8 Device Settings Page

Device Settings are the various settings, including display, sound, keyboard, mouse, and password configurations, for a particular device. Administrators can use the management platform to clone these settings from one device, store them within the database, and then apply them to other devices.

Note: For more information on how to configure device settings, please refer to the OS guide. Details on how to alter these settings, install MUI packs, and select languages can be found there.

2.9 Certificates Page

Certificates can be added into the management platform and seen in the **Certificates** page. These certificates can then be pushed down to devices through the main inventory page.

2.10 Software Page

Software packages allow administrators to incrementally patch existing devices with updates or new versions of existing software. New packages may be released periodically for general use, or custom packages can be created as required by users. This table inventories the currently available packages that have been included by an administrator.

2.11 Tasks Page

The **Tasks** page can be used to monitor the progression status of **Device Actions** that were scheduled for deferred execution. Tasks that are currently active can also have their schedules revised here.

2.12 Logs Page

The **Logs** page can be used to monitor and view activity on the management platform, as well as changes made to devices themselves.

2.13 Searches

The **Search** bar, located on the upper right-hand side of each inventory table, allows users to easily search that table for specific information. A search scans all possible fields in each table, so it is possible to narrow the visible items based on specified criteria. Finding devices that share a common IP address, have the same model type, or use the same OS are a few of the many uses of this feature.

For example, if an administrator has to perform an update on all devices running DeTOS, typing "DeTOS" into the search field displays only those devices in the inventory table. The administrator can then perform updates with a more focused view of the devices being managed.

A new feature of the Management Appliance, **Groups**, supports usage as a search term. Click on the group tag of a device, or enter "group:", and all devices that have been assigned to that group will display in the inventory table. As information is entered into the Search field, the inventory table will automatically update and display the items that match the search criteria.

CHAPTER 3

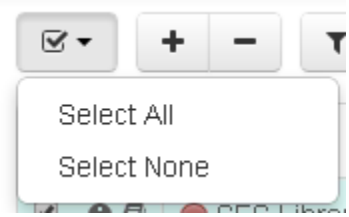
Device Management

3.1 Action Bars

At the top of each inventory table are a series of icons that allow administrators to perform various tasks. The available options differ from table to table.

3.2 Selection Tool

The first icon is the selection tool. This icon can be used to select all of the items listed in the inventory, or to ensure that none of them are selected. To use the selection tool, left click on the icon and click on **Select All** or **Select None** from the dropdown menu.



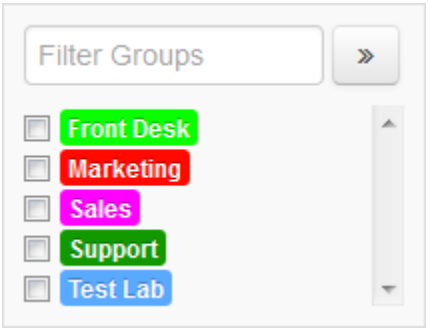
3.3 Add or Remove

The **Add** and **Remove** icons perform different tasks depending on which page is open. When used on the **Devices** tab, for instance, these icons will allow the administrator to either add a new device to the managed devices list by entering an IP address, or to remove selected devices from the list. On the other pages, these icons are used to either create new entries (like profiles or disk images), or to remove entries.

3.4 Filter

Only available in the **Devices** table, the **Filter** button offers two unique features. The **Connected** setting will organize devices based on connectivity, starting with devices that the network can reach. Selecting **Connected** again will instead filter unreachable devices to the top of the list.

The **Show/Hide Group Tray** will display or hide the Group Filter interface. This displays all of the groups that devices can be sorted into. The checkbox next to each group will filter the Device Inventory to display all devices associated with all of the selected groups. The *Filter Groups* field is available for cases where a large number of groups are present. This filter will display all applicable groups based on what has been typed into the text field, and will automatically update the group list as text is entered.



3.5 Groups

Administrators may create **Groups** in order to organize the devices displayed in the **Devices** page. By selecting a device and clicking on this button, administrators may assign a device to one or multiple groups by typing in the name of the group they have previously created. Groups can also be automatically applied to devices that meet the criteria that the Group is set to apply for.

If necessary, clicking on the group tag, located next to the name of a device, will have the management server search through the device inventory based on Groups. This will display all devices that fall into that group. Devices that do not apply to a group are *Unassigned*.

3.5.1 Applying or Removing a Group

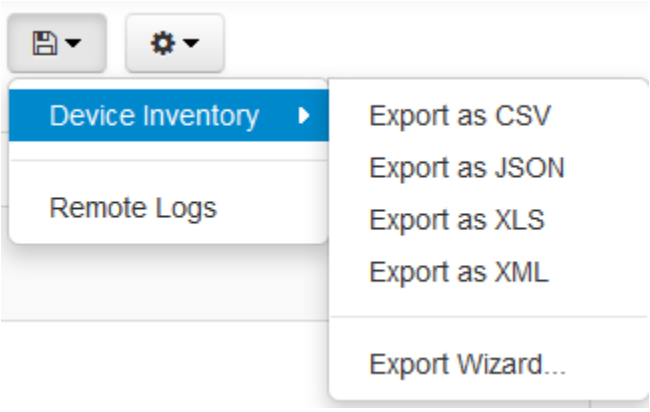
Once a group has been added to the **Groups** inventory list, it can then be applied to devices in the **Devices** inventory. To apply a group to a device:

1. From the **Devices** inventory table, select the device or devices to be added to a group.
2. Click on the **Groups** button in the **Actions Bar** at the top of the page. This will open the **Groups** dropdown menu.
3. Begin typing the name of the group in the **Groups** field. A dropdown menu will populate itself with the available group names as it is typed. Multiple groups may be applied by using this method.
4. If needed, groups can also be removed from this field by clicking on the X next to the group name. This is useful for cases in which a group that is not meant to be applied accidentally gets added to the list.
5. Once a device has the desired groups listed in the **Groups** field, click on the checkmark at the upper right hand corner of the **Groups** menu to apply the changes.

If a group is being applied based on Group Auto-Membership details, then existing devices will automatically update to include themselves as part of the group, and newly-added devices will be included in the group upon their first heartbeat to the server. If a group's membership is changed, devices will automatically update if they meet the requirements to join the group. Devices that no longer meet the group's membership requirements are automatically removed from the group.

3.6 Export

The **Export** tool in the **Devices** inventory table allows administrators to export the data contained within the **Devices** table to a file type of their choosing from the dropdown menu. **Remote Logs** for a device are also able to be exported as a word document file. This option is only available when devices have been selected.



3.7 Device Actions

The **Device Actions** button opens a dropdown menu that contains a large number of actions that can be used on a device, such as applying or cloning settings, rebooting the device, or initiating a Shadow session. Many of the options are outlined in later sections.

Device Actions may change based on devices selected. The actions that are made available depend on single and multi-device selection, selecting devices with varying operating systems, selecting devices with differing connectivity statuses, or even a variation of cross-possibilities.

Permissions will also affect the Device Actions a user can take. Active Directory groups with restrictions may not be able to access certain actions based on the permissions set.

- **View** - Viewing objects on a device requires device read permissions, as well as read permissions on the object type that is being viewed.
- **Apply** - Applying objects to a device requires write permissions to devices, and a minimum of read permissions for the object type that is to be applied to the device.
- **Clone** - Cloning objects from a device requires a minimum of read permissions to devices, but full write permissions for the object type that is being cloned from the device.
- **Remove** - Removing objects from a device requires write permissions to devices, and a minimum of read permissions for the object type that is being removed from the device.

Any unlisted actions require a minimum of write permissions to devices.

3.8 Device Power Options

Administrators are able to remotely power off and power on one or more thin clients that are managed by the Appliance. It is even possible to set a schedule so that managed devices are turned on, shut down, or restarted at the same time every day.

3.8.1 Reboot Device

This option will have all selected devices immediately reboot, or at a set time and date. Devices must be powered on, connected to the network, and associated with the Management Server when this task is distributed.

When to Run Administrators may choose to have the devices reboot immediately, or a schedule may be set so that the devices will always reboot at the same time for multiple instances. For more information on scheduling tasks, refer to the *Tasks* section.

3.8.2 Power Off Device

This option will have all selected devices shut down immediately, or at a set time and date. Devices must be powered on, connected to the network, and associated with the Management Server when this task is distributed.

When to Run Administrators may choose to have the devices shut down immediately, or a schedule may be set so that the devices will always shut down at the same time for multiple instances. For more information on scheduling tasks, refer to the *Tasks* section.

3.8.3 Wake-On-LAN

This option will have all selected devices power on immediately, or at a set time and date. Devices must be powered off, connected to the network, and associated with the Management Server when this task is distributed. A Network Administrator may need to be consulted to get the information required.

Note: Wake-On-LAN has the ability to work across subnets. This requires the router to be configured to forward broadcast packets.

Port to use for wakeup signal The port that will be used for a successful wake-up. This may need to be adjusted, depending on network settings.

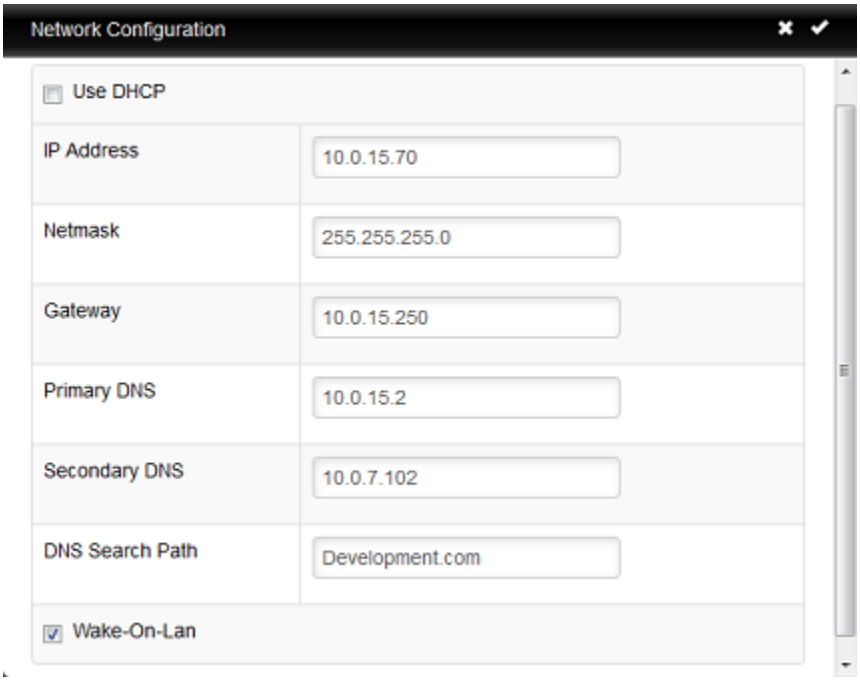
Subnet Mask/CIDR Length The subnet mask for the network. This is mandatory for a successful wake-up.

Subnet IP The subnet of the network. This is optional.

When to Run Administrators may choose to have the devices power on immediately, or a schedule may be set so that the devices will always power on at the same time for multiple instances. For more information on scheduling tasks, refer to the *Tasks* section.

3.9 Device Network Configuration

The Management Appliance provides the ability to remotely set the network configuration of a thin client. With this feature, Administrators are able to set a static IP to a device, or enable or disable Wake-On-LAN functionality. Only one device can be adjusted at a time. A Network Administrator may need to be consulted to get the information required here.



Use DHCP This option will enable a DHCP protocol for connectivity. This option is normally enabled by default on devices. When disabled, new fields will be available and static information can be set for the device.

Wake-On-Lan This option will enable or disable Wake-On-LAN functionality. By default, Wake-On-LAN is enabled. Wake-On-LAN also has the ability to work across subnets. This requires the router to be configured to forward broadcast packets.

3.10 Shadow

Administrators have the option to Shadow thin clients. With this feature, any Administrator or User account with approved permissions can remotely shadow a device, allowing interaction with the host unit that is being shadowed.

Before Shadowing can be permitted, the following settings will need to be established within the Management Appliance:

- **Number of Sessions:** The number of shadowing sessions that the server allow at one time. This can be adjusted based on the network.
- **Initial Client Port:** The client port opened for Shadow.
- **Initial Server Port** The server port opened for Shadow.

Furthermore, the following ports will need to be opened in order to successfully Shadow a device:

- **Ports 5500-5509:** This needs to be opened to allow device-to-server communication.
- **Ports 5999-6008:** This needs to be opened to allow web-to-server communication.

To Shadow a device:

1. From the **Devices** inventory table, select the device that will be shadowed. Only once device can be shadowed at a time.
2. Click the **Options** button at the top of the inventory panel. In the dropdown menu, choose the **Shadow** option.
3. A **Shadow** dialogue box will open with a couple of options:
   - **Timeout** - The amount of time given for the Shadow session to register to the host device. If this time expires before a connection is made, the Shadow session will not begin. This is also the amount of time needed before a new shadow session can be started on the device.
   - **Force Shadow** - This option prevents a prompt from displaying on the host device that allows the host user to confirm or deny the Shadowing session. Instead, the host will be immediately informed that they are being shadowed.
4. Click the checkmark in the top right corner of the **Shadow** dialogue box to start the shadowing session. A new window or tab will appear. If the host has approved the session, or if **Force Shadow** is enabled, then the desktop of the device will display. The device can now be interacted with.

3.11 Cloning Overview

The Management Appliance is able to clone the following types:

- **Connections** - Devices have the ability to connect to remote servers utilizing various types of protocols. The RDP® protocol is used to connect to Microsoft® Terminal Servers. The ICA® and XenAppView® protocols are used to establish connections to Citrix® servers. The VMware® Horizon View™ protocol allows a user to connect to a VMware Horizon View Server. Administrators may use the Management Appliance to clone these types of connections from one device, store them within their connections database, and then apply them to other devices.
- **Device Settings** - Device settings are the permissions, appearance, display, input, persistence, sound, printer, and time configurations for that particular device. Administrators may use the Management Appliance to clone these settings from one device, store them within the device settings database, and then apply them to other devices.
- **Profiles** - Profiles are a way to combine multiple choices from both the **Device Settings** and **Connections** configurations to create an arrangement of options tailored to the needs of the user. Administrators may use the Management Appliance to clone specific profiles to be applied to whichever devices require these combined settings.
- **Disk Images** - The fourth cloning option is the ability to clone the entire disk image of a device. A disk image includes everything that is stored on the DOM on that device, including the operating system itself. This does not include BIOS settings that have been saved elsewhere. Disk image clones are inventoried and managed by name within the disk images database, but are physically stored on an `nfs://`, `cifs://`, `http://`, `https://`, or `ftp://` server on the local area network.

When a clone is created, it will be included in its respective inventory table within the Management Appliance. If more than one item of the same type is cloned with the same name, the Management Appliance will include increments to the names as the clones are created.

3.12 Cloning Connections

Administrators are able to clone individual connections from a thin client and save them in the Management Appliance database. Administrators can easily create a desktop connection on a device and then propagate it to all of their other devices via a profile. All connections can be cloned, and the most common are listed below:

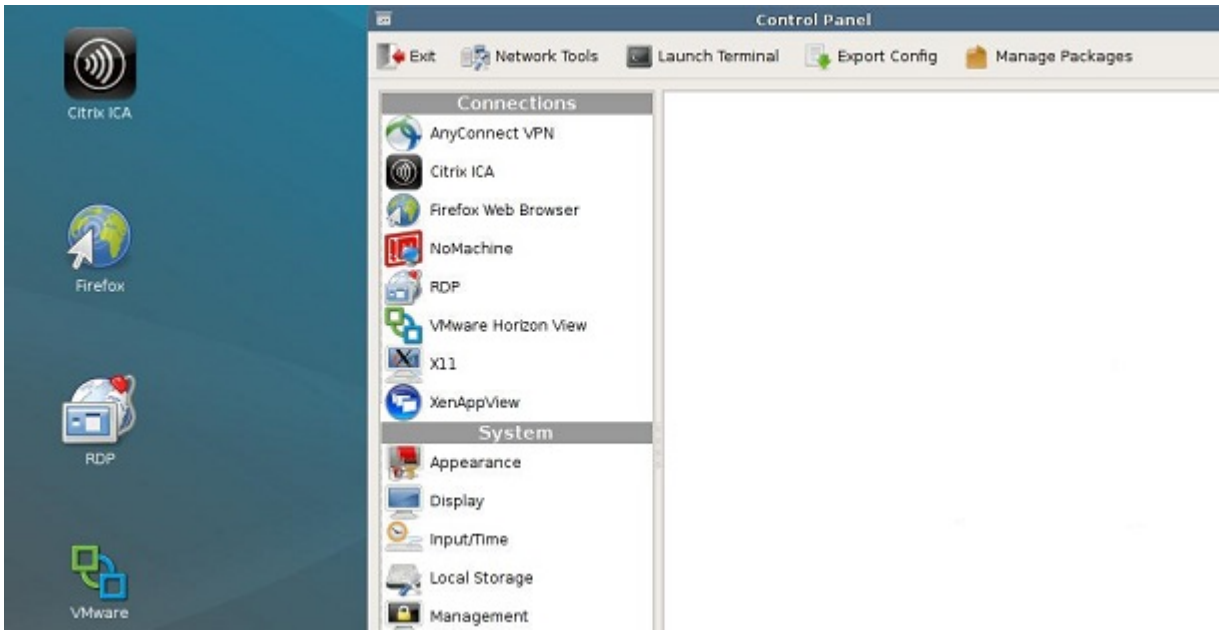
- **RDP** - One or more **.rdp** configuration files used for connecting to Microsoft® Terminal Servers.
- **ICA** - One or more **.ica** configuration files used for connecting to Citrix servers.
- **XenAppView** - Another option for accessing Citrix servers.
- **VMware** - The connection settings and configurations for the Horizon View client.
- **Firefox®** or **Internet Explorer®** - The local web browser and its starting URL.
- **AnyConnect® VPN** - Establishes a VPN connection.
- **NX** - Allows connectivity to a NoMachines session.
- **X11** - The settings and configurations for an X11 server or application.

3.12.1 How to Clone Connections

1. From the table of inventoried devices, select a device to clone connections from and then click on the **Options** button at the top of the inventory table.
2. In the dropdown menu, go to **Clone** and click on **Connections**.
3. A **Clone Connections** dialogue box will open with a field entitled **Connections**.
4. Click on the **Connections** field to view a dropdown list of the connections currently available for cloning from that device. Select one or several of the connections listed.
5. Click the checkmark in the top right corner of the **Clone Connections** dialogue box to create the clone.
6. The **Connections** tab will display the recently cloned connection entries in the inventory table.

3.12.2 Applying Connections to a Device

1. From the table of inventoried **Devices**, left-click on the checkbox to the right of a device to select it.
2. Click on the **Options** button at the top of the inventory table.
3. In the dropdown menu, go to **Apply** and click on **Connections**.
4. In the **Apply Connections** dialogue box, select which connections to apply by clicking in the **Connections** field and selecting from the options that are displayed. To select multiple connections, simply choose another from the dropdown menu and it will be added to the list.
5. Click the checkmark in the top right corner of the **Apply Connections** dialogue box to apply the desired connections to the device.



Note: There are a few differences in the way VMware Horizon View client connections are handled by Windows®-based systems, as compared to RDP and ICA connections. Only one VMware Horizon View client connection can exist per user. The configuration settings for a VMware Horizon View client connection are stored in the User account's registry hive, not in flat files like RDP and ICA. This is simply the nature of VMware's View client program and not in any way a limitation with the Management Appliance.

3.13 Connection Variable Substitution

Connection variable substitution is an advanced feature. This allows users to use a variable as a place holder for information. The information will be filled in with device-specific data when pushed to the client. This feature makes it more convenient for users who need to create multiple connections with minor variances but otherwise identical information. These variables are identical to the parameters exposed by the device endpoint on the ReST interface:

- `agent_version` - The agent version. This can be found in the "View Device" information window within the **Devices** inventory table.
- `description` - The device's description. This is a legacy option for older versions.
- `disk_image_md5sum` - The md5 sum of the disk image. This is a legacy option for older versions.
- `disk_image_version` - The disk image version. This can be found in the "View Device" information window within the **Devices** inventory table.
- `hostname` - The device's hostname. This can be found in the "View Device" information window within the **Devices** inventory table.
- `id` - The device's ID.
- `ip_address` - IP address of the device. This can be found within the **Devices** inventory table.
- `jid` - The server communication protocol (i.e. "SOAP" or "AMQP").
- `last_contact` - Time stamp of the last heartbeat sent from the device to Echo.
- `location` - The device's location. This is a legacy option for older versions.
- `mac_address` - The device's MAC address. This can be found in the "View Device" information window within the **Devices** inventory table.
- `name` - The device's name/ This can be found within the **Devices** inventory table.
- `serial` - The device's serial number. This can be found in the "View Device" information window within the **Devices** inventory table.
- `uuid` - The device's UUID. This can be found in the "View Device" information window within the **Devices** inventory table.

Advanced users may access data hierarchically by using `.` to access child properties. This allows the use of the following data:

- `product.id` - The ID of the device's product.
- `product.manufacturer` - The manufacturer of the device.
- `product.model` - The model of the device.
- `product.os` - The operating system of the device.

Note: Groups are not available for variable substitution.

As an example, a Firefox connection may be created that will connect to a URL based on its hostname. In the "Start URL" field, `{{hostname}}.example.com` may be entered. If this connection is later pushed to a device who's hostname is `host01`, it would try to connect to `host01.example.com`. If pushed to a device with the hostname `host02` it would connect to `host02.example.com`.

Variable substitution supports "regular expression replacement" through use of perl-compatible regular expression (PCRE) syntax. This allows for the replacement of substrings after a variable is substituted. This can be invoked with the following syntax:

```
{{replace variable s/search-string/replacement-string/g}}
```

If, for example, there was a Firefox connection that connects to a specific URL, it would be possible to replace a portion of the URL based on the numeric portion of the device's name in inventory. In the "Start URL" field, enter:

```
{{replace name s/\\w\*(\\d+)/there-are-\\1-lights/g}}.example.com
```

This connection, when pushed to a device named `device04`, will try to connect to `there-are-04-lights.example.com`.

Note: Forward slashes are the only supported separators. Any forward slashes that are part of either the search or replacement string will need to be escaped.

3.14 Cloning Device Settings

The following device settings to be cloned:

- **Permissions** - The Agent Password that has been assigned. If a password is set, Control Panel navigation will be restricted for non-password holders.
- **Appearance** - The way in which icons are displayed, sorted by either connection type or alphabetically by the connection's assigned name. This is a DeTOS-only setting.
- **Display** - The screen resolution, color depth, and refresh rate of the primary display device.
- **FBWF** - The settings for persistence that have been chosen for that device. This is a WES-only setting.
- **Input** - The keyboard, mouse settings, and locale of the device.
- **Sound** - Settings for the master volume and mute control.
- **Storage** - The storage option settings for that device. This only clones the **Storage Options**, and does not clone the persistence settings. This is a DeTOS-only setting.
- **Time** - Settings for the time zone.
- **USB** - The USB permissions granted to the device.
- **Printers** - Settings for a device's attached printer. This setting will not appear if the device does not have a printer plugged in with its properties established.

Note: Certain settings are only available to specific operating systems, and cannot have their clone applied to unsupported systems.

3.14.1 How to Clone Device Settings

1. From the **Devices** inventory table, select the device from which settings will be cloned from.
2. Click the **Options** button at the top of the inventory panel. In the dropdown menu, go to **Clone** and click on **Device Settings**.
3. A **Clone Device Settings** dialogue box will open with three fields to fill out:
    - **Name** - Enter a name for this clone. This name will be the name that Echo refers to for these settings in the future.
    - **Description** - Enter a short description for this clone.
    - **Device Settings** - Select the type of settings that will be cloned. Multiple options from the dropdown menu may be selected, and the selected modules will appear in a list within the **Device Settings** field. When cloning multiple device settings at once, these settings will be bundled together in the **Device Settings** table afterwards.
4. Click the checkmark in the top right corner of the **Clone Device Settings** dialogue box to create the clone.

5. The **Device Settings** tab will display the recently cloned connection entries in the inventory table.

3.14.2 Applying Settings to a Device

1. From the **Devices** inventory table, select the device or devices desired.
2. Click the **Options** button at the top of the inventory panel. In the dropdown menu, go to **Apply** and click on **Device Settings**.
3. From the **Apply Device Settings** dialogue box, select the cloned settings that will be applied from the dropdown menu.
4. Optionally, it is possible to reboot the device after the settings have been applied by selecting the checkbox under **Reboot on success**. If the new settings include network or persistence/FBWF changes, then enabling this checkbox is recommended. Otherwise, this box can be left unchecked.
5. Click the checkmark in the top right corner of the **Apply Device Settings** dialogue box to apply the cloned settings to the device or devices selected.

3.15 Disk Image Cloning

The Management Appliance allows administrators to perform full disk image cloning of devices, utilizing `ftp://`, `cifs://`, `http://`, `https://`, or `nfs://` protocols. Certain disk images are unable to support the disk image cloning process.

Note: To create a disk image clone from a WES® device, FBWF must be disabled. See the WES Administration Guide for instructions on how to do so.

3.15.1 How to Clone the Entire Disk Image

1. From the table of inventoried **Devices**, select a device and then click on the **Options** button. From the dropdown menu, go to **Clone** and click on **Disk Image**.
2. A dialogue box titled **Clone Disk Image** will open with four fields to be filled out:
   - **Name** - Enter a name for this disk image.
   - **Description** - Enter a short description for this disk image.
   - **Image Filename** - Enter the filename desired for the new disk image clone.
   - **Storage Location** - Select the storage location where the image will be saved from the dropdown menu. See *Storage Locations* for more information on setting up storage locations.
3. Click the checkmark at the top right corner of the **Clone Disk Image** dialogue box to begin the cloning process. This process may take a few moments, depending on the size of the device's flash disk and network traffic.
4. After completion, the newly cloned disk image can be seen in the inventory table of the **Disk Images** tab.

3.15.2 How to Add a Disk Image

New OS images can be added to the Management Appliance inventory.

1. Copy the image over to an `nfs://`, `ftp://`, `http://`, or `https://` server, or `cifs://` shared directory. If this directory is not already included in the Storage Location inventory, it will need to be added. Please see *Storage Locations* for instructions on how to add a storage location.
2. From the **Disk Images** tab, click on the **Add** button above the inventory table.
3. A dialogue box titled **Add Disk Image** will open displaying various fields used to add the disk image. The **Basic Information** required is:
   - **Name** - Enter a name for this disk image.
   - **Description** - A short description for this disk image can be entered here.
   - **Filename** - The full filename of the disk image, as it is shown on the server. This will need to include the file extension.
   - **Checksum** - Enter the hash of the disk image. This will be auto-generated if the disk image is being pulled from an `http://`, `https://`, or `ftp://` server, but may take a few minutes, depending on network connectivity.
   - **Product** - Select the product from the dropdown menu which this disk image can be applied to.
   - **Storage Location** - Choose the storage location where the disk image has been saved. A storage location must have been established beforehand. See *Storage Locations* for more information on how to include storage locations to the Echo inventory.
   - **MD5 SUM** - Enter the md5sum of the disk image. This field is not marked as required (*), however older versions of disk images will need this correctly filled.

   Note: If a thin client that is using DeTOS 7.3 or 7.4 is receiving a disk image upgrade through a Windows Share (`cifs://`) storage location, the SHA1 of the disk image will need to be entered in place of the checksum. This is always required regardless of legacy status.

   ---
4. Click the checkmark at the top right corner of the **Add Disk Image** dialogue box to add this disk image to the inventory of disk images.
5. In the **Disk Images** tab, the inventory table will now contain the recently added disk image. See the section titled applydiskimage-reference for instructions on how to apply the disk image to devices.

3.15.3 Applying a Disk Image to a Device

Caution: When applying disk images to devices, make sure to use the correct image for that particular model, otherwise the device may be rendered unbootable.

1. From the **Devices** inventory table, select a device or devices and then click the **Options** button. From the dropdown menu, go to **Apply** and then click on **Disk Image.**
2. In the **Apply Disk Image** dialogue box, select the desired disk image from the dropdown menu. To have the device reboot and apply the disk image immediately, click in the checkbox next to **Reboot on success**.
3. Click the checkmark at the top right corner of the **Apply Disk Image** dialogue box to begin applying the disk image.

Note: Using the search function while performing disk image applications is advised. For example, by searching for "DeTOS" will cause only devices running DeTOS to be displayed. By utilizing the search function, administrators can avoid accidentally applying a disk image to a device of the wrong type or that is running a different OS.

---

4. Click the **Submit** button to begin the re-imaging process.

The disk image will either reboot to begin the updating process, or it will update in the background so users do not have to be interrupted by the updating process. The status of the update can be viewed at any time by checking the **Device Logs**, either from the **Logs** inventory table or directly from the device from the **Devices** inventory table. The re-imaging process may take a few moments, depending on the size of the image and network traffic. During this time, there is no agent to heartbeat into the server, and therefore the timestamp in the **Last Contact** field of the **View Device** dialogue box will remain unchanged. Once the re-image is complete, the device will be free to be rebooted at the earliest convenience, or will automatically reboot if **Reboot on Success** was selected. The agent will heartbeat into the server, which in turn will update the **Last Contact** field. This update to the current time in the **Last Contact** field means that the re-imaging process is complete.

3.16 Profiles

The profile feature allows administrators to assign connections and settings to one or more device. Profiles are useful for administrators that wish to affect updates on many devices at once. For instance, sometimes it becomes necessary to change the details of a connection that is used for multiple devices. If a profile has already been applied to those devices that contains the connection details, simply updating the connection details will automatically adjust the devices to use these new settings. The next two sections describe the necessary steps for creating and applying profiles.

3.16.1 How to Create a Profile

1. Open the **Profiles** tab to be taken to the profile inventory table.
2. Left-click on the **Add Profile** button above the inventory table.
3. The **Add Profile** dialogue box will open with seven fields to enter information in:

   Name Enter a name for this profile.

   Description Enter a description about the profile.

   Mode Select between the following profile application options:

   - **Default Profile** – Apply to all devices on the server. If an operating system normally runs a wizard on its first boot, the first boot wizard will be overridden by the profile. This will occur even if the profile contains no applicable items.
   - **Select Devices** – Manually select devices by name. This mode will override Default profiles. Once **Select Devices** is chosen, a **Devices** field will open where the administrator can choose individual devices to apply this profile to by name.
   - **Apply by terminal details** – This will apply to all devices that meet the specifications that are entered. When selected, the profile can specifically be applied by **Device Name**, **IP Address, Range or Subnet**, Device **Model**, or by **OS**.
   - **Apply by group membership** – Applies the profile to all devices that have been assigned to one or more selected groups. When this option is chosen, a drop-down menu of all available groups is made available.

   Disk Image In the drop-down menu, if the administrator adds an image to the profile, the Management Appliance will re-image the device every time it boots if it doesn't already have the specific image listed here.

   Connections Assign connections to this profile by clicking in the field and choosing which connections to include. It is also possible to select none at all.

   Device Settings Assign cloned settings to this profile by clicking in the field and choosing which settings to include. It is also possible to select none at all.

   Certificates A certificate can be included to allow entry to servers with security restrictions, or for 802.1x network connections.

Software Packages Software Packages can be deployed to multiple devices when applied to Profiles. Be aware that devices will still need to be rebooted before a deployed software package will properly load onto the device.

4. Once all of the information is correct, click on the checkmark on the top right hand corner of the **Add Profile** dialogue box.
5. The new profile entry is now listed in the **Profiles** inventory table.

3.16.2 Applying a Profile

Once a profile has been created as described in the section above, it will automatically apply the associated connections and settings the next time the devices included in the **Mode** field are rebooted. However, if to make the changes take effect immediately, the profile may be manually applied by following the steps below:

1. From the table of inventoried **Devices**, select a device and then click on the **Options** button. From the dropdown menu, go to **Apply** and click on **Profile**.
2. From the dropdown under **Profile**, select which profile will be applied.
3. Click the checkmark at the top right corner of the **Apply Profile** dialogue box to confirm this change.
4. Connection shortcuts are automatically created on the device's desktop. The end-user can simply double-click these icons to initiate the connection.

Profiles are able to be applied to devices that have not yet run the First Boot Wizard. In the case of newly-reflashed devices, the Profile will overwrite the need to run a First Boot Wizard.

Note: Even if a profile is devoid of options, it will still override the First Boot Wizard. The desktop will be presented with default settings.

3.17 Certificates

Some connection sessions may require a security certificate to allow access. Some 802.1x network connections may also need a certificate. The Management Appliance can push these certificates to multiple devices.

Note: Certificates are only supported on DeTOS-based machines. WES-based machines will not accept certificates.

3.17.1 Adding a New Certificate

1. Open the **Certificates** tab to be taken to the Certificates inventory page.
2. Click on the **Add Certificate** button above the inventory table.
3. **The following information will need to be entered for the new certificate:**

   Name This is the name of the certificate, as assigned by an Administrator.

   Description Entering a description will give more information about the certificate and the purpose it will serve. This is an optional field, but inclusion is recommended for clarity purposes.

   Certificate Clicking on the **Browse** button will have Administrators locate the certificate file locally to upload to the Management Server. The following certificate types are accepted: *.cer*, *.crt*, *.csr*, *.key*, *p7b*, and *.pem*.
4. Once all of the information is correct, click on the checkmark on the top right hand corner of the **Add Certificate** dialogue box.
5. The new certificate entry is now listed in the **Certificates** inventory table.

3.17.2 Applying a Certificate

To apply a certificate to devices:

1. From the table of inventoried **Devices**, select all of the devices that will receive the certificate, then click on the **Options** button. From the dropdown menu, go to **Apply** and click on **Certificates**.
2. From the **Certificates** dropdown options, select which certificates will be applied. Multiple certificates may be applied at one time.
3. Click the checkmark at the top right corner of the **Apply Certificates** dialogue box to confirm this change. All devices that have received a certificate do not need to be rebooted.

3.18 Software Packages

3.18.1 How to Add a Software Package

Software packages are used in order to apply specific updates or changes to devices without having to update the entire image. Some examples for software packages would be custom wallpaper images, updating software clients like VMware Horizon View, Citrix, or RDP, potentially providing bug fixes, and more.

At this time, customer-created packages are not supported. In order to add a software package to the Software inventory:

1. Click on the **Software** button to view the software inventory table.
2. Click the **Add** button at the top of the inventory table.
3. An **Add Software** dialogue box will open with several fields:
    - **Name** - Enter a name for this software package.
    - **Description** - A short description for this software package can be entered here.
    - **Filename** - The full filename for the software package being added. The file extension will need to be included.
    - **Checksum** - Enter the hash of the software package. This will be auto-generated if the software is being pulled from an `http://`, `https://`, or `ftp://` server, but may take a few minutes, depending on network connectivity.
    - **Product** - Select the product from the dropdown menu which this software package can be applied to.
    - **Storage Location** - Select the storage location where the disk image has been saved.
4. Click the checkmark at the top right hand corner of the **Add Software** dialogue box to add the desired software package to the software inventory.

3.18.2 Applying a Software Packages to a Device

Note: Software Packages are only supported on DeTOS-based machines. WES-based machines will not accept software packages.

1. From the **Devices** inventory table, select a device or multiple devices and then click the **Options** button.
2. Select **Apply** and then click on **Software.** This will open the **Apply Software** dialogue box.

   Note: Packages that are incompatible with the selected devices will not display in the dropdown menu.

3. From the **Software** dropdown list, select the package that will be applied.
4. Click the checkmark at the top right hand corner of the **Apply Software** dialogue box to add the desired software package to the selected devices.

3.18.3 Removing a Software Packages from a Device

1. From the **Devices** inventory table, select a device and then click the **Options** button.
2. Select **Remove** and then click on **Software**. This will open the **Remove Software** dialogue box.
3. In the **Software** field, select the desired software packages to be removed from the device. Multiple packages may be selected, if needed.
4. Click the checkmark at the top right hand corner of the **Remove Software** dialogue box to remove the selected software packages from the devices selected. The software package will be completely removed on the device's next reboot.

3.19 Tasks

Device activities can be deferred for later execution, and can be set to repeat at a schedule, if desired.

3.19.1 How to Create a New Task

1. From the **Devices** inventory table, select one or more devices that will be receiving a new task.
2. Many device activities are eligible to be assigned as a scheduled task. This includes applying to devices and powering off, powering on, and rebooting devices.
3. When the activity has been selected, there will be the option to execute the action immediately, or to schedule it as a task for later. When creating a task, the following options are available:
    - **Task Name** - Enter a name for the task.
    - **Date/Time** - Select the date and time for the task to begin its initial run.
    - **Retries** - The number of attempts the Management Appliance will make to execute the task should networking or other issues occur while the task is being executed.
    - **Frequency** - The rate at which the task will be performed. A custom frequency can also be entered.
4. Click the checkmark at the top right corner of the panel to assign the task. The task will remain in the **Tasks** inventory table, even after it has completed its run.
5. If a task is still running, it can be edited within the **Tasks** inventory table by clicking on the **Edit** icon next to the task's name. This will allow changes to a task's schedule or even halt the actions of a task, if necessary.
    - **Grey Dot** - The task is **Ready**, but has not yet run.
    - **Spinning Circle** - The task is currently **Running**.
    - **Green Checkmark** - This indicates the task is **Finished** if it was meant to be executed once, is **Passing** is the task is to repeat, or is **OK** if the task has completed all reoccurring instances.
    - **Yellow Exclamation Point** - This task is currently **Failing**.
    - **Red X-mark** - The task has **Failed**.

Tasks that are scheduled to continue running will display the date and time of its next scheduled run. If a task is set to only run once, then no date or time will appear once the run has been completed.

CHAPTER 4

Appliance Settings

At the top of the **Administration Page** is a link titled **Settings**. The **Settings** section handles additional features that can be used to customize storage locations, groups, and maintenance and recovery options.

4.1 Server Settings

Users can adjust the Web Application settings. The table of settings notes whether the setting is an Integer or a String, the current value of the setting, and the default value. Settings will apply after a server restart.

HostAgent/Heartbeat/Max Sets the maximum amount of time, in seconds, on the interval of a device's heartbeat. This reduces flooding the network with information from multiple devices at once.

HostAgent/Heartbeat/Min Sets the minimum amount of time, in seconds, on the interval of a device's heartbeat. This reduces flooding the network with information from multiple devices at once.

HostAgent/Heartbeat/Timeout Sets the amount of time, in seconds, before the server will consider a device that is not sending a heartbeat to be offline. Offline devices will display with a red dot in the Devices inventory table.

Inventory/SyncDeviceNameToHostname Sets a device name to match the device hostname, when the device hostname changes. Set this value to 0 to disable, or 1 to enable. This settings requires a server restart to apply the change.

Server/Audit/MaxEntries Sets the maximum number of entries saved in the Audit Trail logs. This value may be set at *-1* for no entry limit, or *0* to disable audit trail logging.

Server/EthInterface Sets the ethernet interface that the server runs on. Leave this at the default value.

Server/IdleTimeout Sets the time, in seconds, of inactivity before the Web Application automatically logs out. There is a 30 second warning before the logout occurs. Setting this value to *-1* disables the idling timer. Refreshing the page applies this setting instead of rebooting the server.

Server/LibPath Sets the path for the server's dependencies. Leave this at the default value.

Server/Logs/MaxEntriesPerDevice Sets the maximum number of log entries saved per device. Setting this value to *-1* will remove the entry limit.

Server/MaxActiveDiscoveries Sets the maximum number of devices that Rangewalk may discover simultaneously. These requests are processed in chunks, so large ranges are acceptable.

Server/MaxDeviceActionThreads Sets the maximum number of simultaneous device actions that the server can perform at once. These requests are processed in chunks, so large ranges are acceptable.

Server/RunPath Sets the path of the server's executable. Leave this at the default value.

Server/Scep/CertificateRequestAddress Sets the address where the client device will request the certificate from. This will usually be *http://<WindowsServerDN>/CertSrv/mscep/mscep.dll*.

Server/Scep/ChallengeAddress Sets the address where the management server will retrieve the enrollment challenge information to forward to the client device. This will usually be *http://<WindowsServerDN>/CertSrv/mscep_admin/*.

Server/Scep/Identity Sets the anonymous identity used during the first phase of EAP-TLS authentication. This is usually the same account that is running the NDES service on Windows Server.

Server/Scep/Password Sets the password of the user account that will retrieve the SCEP challenge information.

Server/Scep/Username Sets the username of the user account that will retrieve the SCEP challenge information. This authenticates against the MSCEP IIS website.

Server/SocketPath Sets the path of the server's communication socket. Leave this at the default value.

Server/Username Sets the system user that executes the server. Leave this at default value.

Server/ShadowTimeout Sets the time, in seconds, before an idle Shadow connection times out. This timer is specific to inactivity from the administrator's window, not from the client desktop.

Server/WWWGroup Sets the Unix group that the web server runs under. Leave this at the default value.

> **Caution:** Adjusting the *Server/EthInterface*, *Server/LibPath*, *Server/RunPath*, *Server/SocketPath*, *Server/Username*, or *Server/WWWGroup* settings will result in the server failing to run.

4.2 Licenses

The **Licenses** tab can be used to apply licensing keys for the VDI Blaster™ software. To add a license to the inventory:

1. From the **Licenses** inventory table, click the **Add** button at the top of the page. This will open the **Add License** menu.
2. In the field labeled **License Key**, enter in the VDI Blaster key exactly as it appears.
3. Once the key has been correctly entered, click on the checkmark at the top right hand corner of the **Add License** menu to apply the license to the Management Appliance.

Once a key has been applied, it will appear in the **Licenses** inventory table. Each key allows a limited number of devices to be managed by the Management Appliance, and this number is listed in the **Allowed Devices** column. Keep in mind that these licenses are applied in a first-come, first-served manner.

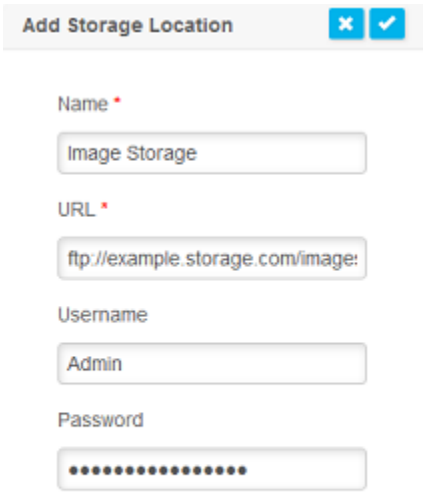
4.3 Products

When a device with an unknown product type is added to the inventory, the management platform will automatically add the product to the known products list. Products may then be used to restrict actions to a subset of the inventory. For instance, a product may be specified when creating a Software Package, to ensure that the software can only be applied to devices running DeTOS.

Note: Removing a Product from inventory will also remove all Devices, Disk Images, and Software Packages that are associated with the product.

4.4 Storage Locations

Storage locations are server locations where data such as disk images or software packages can be kept. In order to add a new storage location to the **Storage Locations** inventory:



1. From the **Storage Locations** inventory tab, click on the **Add** button at the top of the page.
2. The **Add Storage Location** dropdown menu will open. There are four fields that must be filled out in order to successfully add a new storage location:
   - **Name** - Enter a name for the storage location being added.
   - **URL** - Enter the complete URL of the storage location.
   - **Username** - If a username is needed to access the storage location being added, enter it in this field.
   - **Password** - If a password is needed to access the storage location being added, enter it in this field.

3. Once all of the fields have been correctly filled out, click on the checkmark in the top right corner of the **Add Storage Location** menu to add the new entry.

Once completed, the new location will appear in the list of inventoried storage locations. Entries in this table will be included in the **Storage Location** fields when choosing where to save disk images and packages.

Note: Removing a Storage Location from inventory will also remove all Devices, Disk Images, and Software Packages that are associated with the product.

4.5 Groups Settings

Administrators have the option of creating **Groups** within the management console in order to help them organize their devices. Individual devices can belong to multiple groups. To create new groups:

1. From the **Groups** inventory table, click the **Add** button at the top of the page.

2. The **Add Group** menu will open with two fields:

   Group Information

   - **Name** - Enter a name for the group being created.
   - **Color** - Click on the **Color** field to open a color wheel and select the desired color.

   Automatic Membership

   - **IP Address/Subnet** - This will allow the group to be automatically applied to any devices that use this IP Address or falls under the subnet. Use a comma-separated list to add multiple IP Addresses.
   - **Model** - This lets all of the specified models within the Management Server become a member of the group. Only one model may be selected.
   - **OS** - The Operating System of the devices that will be a member of this group. Only one OS may be selected.
   - **MAC Address - The MAC address of the devices that will be a member of** this group. Use a comma-separated list to add multiple MAC addresses.
   - **Hostname** - The hostname of the devices that will be a member of this group. Use a comma-separated list to add multiple hostnames.

- **Serial Number - The serial number of the devices that will be a member** of this group. Use a comma-separated list to add multiple serial numbers.
- **Location - The location of the devices that will be a member of** this group. Use a comma-separated list to add multiple locations.
- **UUID - The UUID of the devices that will be a member of** this group. Use a comma-separated list to add multiple UUIDs.
- **Disk Image Version - The disk image version of the devices that will** be a member of this group. Use a comma-separated list to add multiple disk images.
- **Agent Version - The agent version running on the devices that will be** a member of this group. Use a comma-separated list to add multiple agents.
- **Protocol - The protocol of the devices that will be a member of** this group. Select **Any**, **SOAP**, or **AMQP** from the list. Only one protocol may be selected.

3. Once all relevant information has been entered, click on the checkmark at the upper right hand corner of the **Add Group** menu. The new group will appear in the **Groups** inventory.

Note: A device that no longer qualifies as a member of a group will automatically leave the group.

4.6 Database Hotcopy

A back up of the management server can be created from the main **Database Hotcopy** tab. The method used is referred to as a 'Hotcopy' since the backup is created while the system is running. There is no need to stop or suspend the Management Appliance for the backup. To execute a Hotcopy, perform the following procedure:

1. Click on **Backup Server** button at the top of the **Database Hotcopy** page.
2. A **Backup Server Settings** dialogue box will open. Administrators can then select which tables should be included within the Hotcopy being created by checking or unchecking the boxes next to the various options.
3. Once all of the needed adjustments have been made, click on the checkmark at the top right hand corner of the **Backup Server Settings** dialogue box to begin making the Hotcopy itself.
4. The result of the Hotcopy will create a binary (**.BIN**) backup file that will be downloaded to the local machine. Click **Save File** and make a note of where the file is saved, as it will be needed it in the future to perform a restore.

4.7 Restore Server

A restore deletes all existing configuration and data on the Management Appliance and overwrites it with the information contained in a previously created Hotcopy backup file. To perform a restore, follow these steps:

1. In the **Database Hotcopy** tab, click the **Restore Server** button at the top of the page.
2. A **Restore Server** dialogue box will open. In the **Choose File** field, navigate to the .bin file containing the server data needed.
3. After the path to the backup file has been entered, click the checkmark at the top right corner of the **Restore Server** dialogue box to restore the server settings to those contained in the Hotcopy.
4. In the **Database Hotcopy** tab, click the **Legacy Restore** button at the top of the page.
5. A **Legacy Restore** dialogue box will open. In the **Choose File** field, navigate to the .bin file containing the server data needed. Below the Browse button is an option that states "Force restore even if some records can't be processed". This option is available due to differences that can occur between a legacy version and the current version of the Management Appliance, but is not required.
6. After the path to the backup file has been entered, click the checkmark at the top right corner of the **Legacy Restore** dialogue box to restore the server settings to those contained in the Hotcopy.

4.8 Permissions

Permissions can be set for the accounts of Active Directory groups that will be using the Management Appliance. To select permissions for group accounts, the Management Appliance must first join Active Directory. Refer to the activedirectory-reference section.

1. Click on the **Permissions** button to access the Permissions inventory table.
2. Create a new group by clicking on the **Add** button at the top of the page.
3. The **Groups** dropdown menu will display all groups that were included during the Active Directory configuration process. A search bar is also available to locate specific groups. If a group is not displaying, click on the **Refresh** button to reload the group inventory. The **Restrict to Groups** option will restrict an Active Directory group's permissions to devices within the specified device groups.
4. Once a group has been selected, all of the **Read/Write** access can be chosen for that group. Click on the **Read All** or **Write All** buttons to allow privileges for all options. Write permissions are not available without Read permissions.
5. After all permissions have been set for that group, click on the checkmark at the top right corner to apply those permissions settings. Repeat this process for all groups as necessary. It is recommended that any Administrator groups have full Read and Write access.

Once Permissions have been established, Active Directory accounts may be used as login credentials.

4.8.1 Role-Based Inventory Filter

If necessary, an account may also have limited access to certain settings and inventories with a Role-Based Inventory Filter in place. Similar to standard Permissions, this inventory filter is applied based on Active Directory group memberships and restrictions.

4.8.2 Extra Permissions

Miscellaneous permission options are available as optional inclusions for group and account permissions. These options can be set based on security preferences for devices.

Override Shadow Confirmation This option will determine if a prompt will appear for devices that the Management Appliance requests to Shadow. This prompt, if accepted, grants the Management Appliance permission to shadow. If **Allow Override** is enabled, the device will simply be notified that it is being shadowed.

Allow Shadow without Device Write Permissions This option will allow groups without write permissions to Shadow a device. This may be necessary if an Active Directory group is restricted to certain device groups or otherwise does not need device write permissions.

> **Warning:** Enabling this option will give the Shadow initiator the ability to open and adjust Control Panel settings of the device that is being Shadowed. To prevent potential adjustments, the Control Panel should be password protected before a shadowing session is started. For more information on Control Panel security, refer to device's respective operating system guide.

4.9 Appliance Upgrades

The following is the recommended procedure for upgrading the Management Appliance to a newer version:

1. **Backup** - Back up the server's current configuration and data prior to performing an upgrade using the Hotcopy procedure. Refer to the **Database Hotcopy** section for details on this step.
2. **Upgrade** -
   - Shut down the appliance server (Select option 9, **Halt Machine**, from the **Main Menu**).
   - Download the latest management console appliance.
   - Extract the contents and point the VMware Server to the new file.
   - Restart the virtual appliance.
3. **Restore**- Once the upgrade is finished and the new appliance is online, the management server will be ready for restoration. Refer to the **Restore Server** section for details on the restore process.

4.10 Package Management

Packages are available for the Management Appliance, allowing an Administrator to remotely upgrade the version of the server without performing a virtual appliance replacement.

Note: In order to perform a successful upgrade, the previous version of the Management Appliance must be in use. The Management Appliance will only accept upgrades from its subsequent version. The upgrade will not go through if the appliance is at least two versions behind the package's version.

---

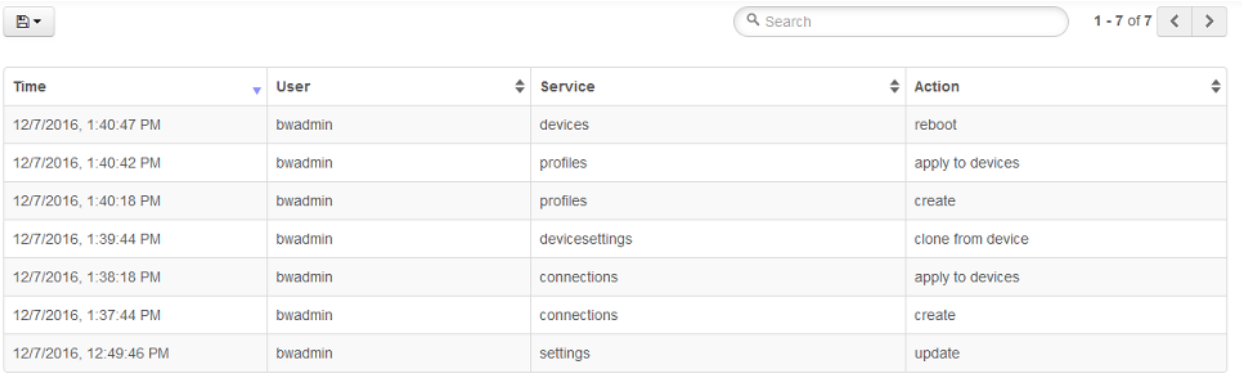
1. Download all available package files, then access the **Settings** page of the Management Server.
2. Click on **Add Package** button at the top of the **Package Management** page. Click on the **Browse** button and locate the first package file. Once the file has been selected, click on the checkmark icon on top right hand corner of the **Add Package** dialogue box to begin the package application.
3. The first package will begin to apply itself. This may take a few moments to complete. As each package is being applied, the **Logs** will update automatically, displaying the current progress and errors, if any. When the first package finishes applying, repeat the process to apply the next package. The final package will initiate the update process. Once finished, the Management Appliance will automatically restart to apply the packages. The restart process may take a few moments to complete. During this time, the web user interface will be inaccessible until the restart is finished. Once this process is completed, the Management Appliance will clean up the package and the server will be ready for use.

Warning: It is important to make sure that the packages are applied in order. Failure to do so may result in errors during the update process.

Warning: Be aware that once an update has been applied, it is not possible to roll back the server. For best results, take a snapshot of the virtual machine that is running the Management Appliance before applying the packages. The availability and location of the snapshot option will vary, depending on the platform used. It is also recommended to create a Database Hotcopy of the server before packages are applied. This is not meant to be a substitution for an appliance snapshot. For more information on creating a hotcopy, refer to hotcopy-reference.

4.11 Audit Trail

The Audit Trail is available for Administrators who wish to view previous actions performed within the Web Application. The Audit Trail will display the time, date, and location where an action occurred and by which user.



Time	User	Service	Action
12/7/2016, 1:40:47 PM	bwadmin	devices	reboot
12/7/2016, 1:40:42 PM	bwadmin	profiles	apply to devices
12/7/2016, 1:40:18 PM	bwadmin	profiles	create
12/7/2016, 1:39:44 PM	bwadmin	devicesettings	clone from device
12/7/2016, 1:38:18 PM	bwadmin	connections	apply to devices
12/7/2016, 1:37:44 PM	bwadmin	connections	create
12/7/2016, 12:49:46 PM	bwadmin	settings	update

The Audit Trail logs a maximum number of entries by default. To change the entries available, access the **Server Settings** page and edit the parameters listed under the *Server/Audit/MaxEntries* entry. Setting this entry to *-1* will disable the entry limit.

4.11.1 Saving Audit Trail Logs

Download the Audit Trail logs by clicking on the Save icon above the table and selecting the format to save the logs as.

4.12 Automatic SCEP

Automatic SCEP server support is available on DeTOS for users who wish to use an automatic method for accessing secure networks.

SCEP is currently only supported on a Windows Server (NDES).

Note: Echo and the NDES server will both need to be visible on the unsecured network for this process.

4.12.1 Deploying SCEP

The following settings must be entered on the Server Settings page before SCEP can function properly on devices. See serversettings for more information on Server Settings.

Server/Scep/CertificateRequestAddress Sets the address where the client device will request the certificate from. This will usually be *http://<WindowsServerDN>/CertSrv/mscep/mscep.dll*.

Server/Scep/ChallengeAddress Sets the address where the management server will retrieve the enrollment challenge information to forward to the client device. This will usually be *http://<WindowsServerDN>/CertSrv/mscep_admin/*.

Server/Scep/Identity Sets the anonymous identity used during the first phase of EAP-TLS authentication. This is usually the same account that is running the NDES service on Windows Server.

Server/Scep/Password Sets the password of the user account that will retrieve the SCEP challenge information.

Server/Scep/Username Sets the username of the user account that will retrieve the SCEP challenge information. This authenticates against the MSCEP IIS website.

After applying these settings, restart the Echo server. Once Echo resumes activity, SCEP can be provisioned for devices with the following steps:

1. Access the Web Application. Open the **Settings** tab at the top and click on the **SCEP** inventory page.
2. Click on the **+** icon to add a new device to support SCEP. Enter the device's MAC address to add it to the inventory.

Note: Devices that are not part of the Echo Appliance's device inventory are included upon completion of this process.

---

3. Power on the device that has been configured for SCEP and connect to the unsecured ethernet. Once the device connects to the Management Server, Echo will begin SCEP enrollment process by requesting a challenge password from the NDES server and sending the response along with the certificate request address to the device. The device will then request a certificate using the challenge password provided to it by Echo. upon success, the device will receive the SCEP server's CA certificate, its own client certificate and private key. From there, 802.1X will be configured, overwriting any previous 802.1X configurations.

Once SCEP is deployed with all relevant information, connect the device to the secure 802.1X port. If the device was already part of the Appliance's device inventory, reboot it before connecting to the 802.1X network.

CHAPTER 5

Terminology

This section covers terms and descriptions that Echo uses throughout the user interface.

5.1 General Terms

Navigation Tabs A term used to reference the various tabs located on the left-hand side of the Echo Administration screen. These tabs provide quick access to the various inventory tables.

Inventory Tables Inventory Tables are the lists of items presented in a table format that is located in the middle area of the Echo Administration screen. Upon clicking on Navigation Tabs such as Devices or Profiles, among others, an inventory table will open for those specific sections.

Device This is the device in front of the user, to which their screen, keyboard and mouse are attached. In Echo, the Devices tab will display an inventory containing all of the devices being managed by the Echo server.

Shadow Shadow is a method that allows Administrators and Users with approved permissions to shadow one host device at a time. This allows Echo to view and interact with the desktop of the host device.

Connection A connection is a method used to connect a device to a remote server. The Connections tab in Echo will display an inventory containing all of the RDP, ICA, VMware View, and other connections that have been created.

Profile A profile is a combination of device settings and connections that can be created in order to provide easily applied groupings of settings to multiple devices. The Profiles tab is where the administrator can create, edit, and apply these profiles to the devices.

Disk Image A disk image is a file that contains an all encompassing set of information that can be applied to a device, including the operating system. The Disk Images tab opens the inventory table that allows users to create, edit, and apply disk images as needed.

Device Settings Device settings are limited to the display, sound, keyboard, mouse, and password configurations for a device. The Device Settings tab displays the inventory table containing the groups of settings that have been cloned from devices. Applying device settings to a device is performed through the Device inventory table.

Certificate Certificates provide users with the credentials needed to access certain websites or services. While certificates can be obtained in a number of ways, the Certificates tab in Echo allows users to

store specific certificates that can then be applied to devices through the Device inventory table.

Software Software packages allow administrators to patch existing images on devices or update to new versions of existing software. The Software tab in Echo displays the inventory of administrator-approved packages.

Tasks Tasks allow users to schedule device activity for later execution. Tasks must be scheduled from the Devices tab. The Tasks tab will allow users to view the status and schedule of all tasks that have been set on the server.

Logs Logs are records of server events that administrators can use to keep track of what is occurring with the managed devices.

Settings The Settings tab is used in Echo as a reference to the process of maintaining and updating the Echo server itself. The Settings tab has several subsections that allow an administrator to carry out a number of useful processes to keep the server running smoothly.

Help Help is a tab where the user can view a number of resources to assist with running Echo. There is also a brief administration guide and a link to the full length Echo Administration Guide.

5.2 Device Details

Name Name of the device. For newly discovered devices, the default name given to the device is its hostname. Change the name of a device by left-clicking on the desired device in the Devices table and entering a new name in this field. Click on the check mark to apply these changes.

Description A human readable description of the device, as entered by the administrator.

Last Contact The date and time of the last heartbeat sent. This will automatically update every 60 seconds by default, so long as a connection can be established.

MAC Address The ethernet address of the device.

Hostname The hostname of the device.

IP Address The IP address assigned to the device.

Serial Number The serial number of the device.

Location A human readable location such as "Test Lab" or "Office 325." This field was used in older versions of the server, consider using Groups instead to convey this information.

UUID The universally unique identifier (UUID) for the device. This is burned into the device at the factory and is used to uniquely identify the device as its network address changes.

Disk Image Version The version of the disk image the device is currently using.

Disk Image MD5 Hash The hash of the disk image being run by the device. This can be auto- generated if the disk image came from an `ftp://`, `http://`, or `https://` server.

Agent Version The version of the Echo Agent that the device is currently using to communicate with the Echo server.

Product The brand, device name, and operating system that the device is running, as reported by the device via the Echo Agent.

Groups The group or groups that the device is assigned to.

5.3 Connection Details

There are a wide variety of connection types that can be managed through the Echo software. Since each connection type has different options available, this section is broken down into the different panes that are present for each connection type.

5.3.1 JavaWS

JavaWS connects to Citrix desktops through the JavaWS Client.

Basic Information

Name The name of the connection. The name is a required field when a new connection is created.

Local Display Name The local display name is what the connection will be labeled with on the device. This field is required in order to create a new connection.

Description A description such as "Kiosk Connection" or "Presentation Connection." The description field is optional, but it is recommended to use descriptions to help organize connections.

Protocol The protocol used in the connection is displayed here.

General

Server URL The name or IP address of the JavaWS server.

Autostart Causes the connection to start as soon as the device is powered on.

Auto Restart Causes the connection to be restarted if it is closed. This is useful for administrators that wish to limit the ability of a user to access the device.

Disable Desktop This will disable desktop access, ensuring that users only access this specific workstation with the specific credentials applied to the connection. Logging off from the server will power off the thin client, and powering on the thin client will bypass the operating system's desktop and immediately log in to the server. This feature is not supported for Windows-based operating systems.

5.3.2 AnyConnect VPN

The AnyConnect VPN protocol allows connections to a VPN service.

Basic Information

Name The name of the connection. The name is a required field when a new connection is created.

Local Display Name The local display name is what the connection will be labeled with on the device. This field is required in order to create a new connection.

Description A description such as "Kiosk Connection" or "Presentation Connection." The description field is optional, but it is recommended to use descriptions to help organize connections.

Protocol The protocol used in the connection is displayed here.

General Settings

Host The host address or IP address of the VPN service.

Username The default username for the VPN connection. Leaving this field blank will allow those who use this connection to log in with their desired username when they connect.

Group The default workgroup that will be accessed.

5.3.3 Firefox

Firefox is a local web browser. This connection can not be applied to Windows-based operating systems.

Basic Information

Name The name of the connection. The name is a required field when a new connection is created.

Local Display Name The local display name is what the connection will be labeled with on the device. This field is required in order to create a new connection.

Description A description such as "Kiosk Connection" or "Presentation Connection." The description field is optional, but it is recommended to use descriptions to help organize connections.

Protocol The protocol used in the connection is displayed here.

General Settings

Start URL The URL that Firefox will automatically open upon starting.

Autostart Allows the administrator to cause a connection to start as soon as the device is powered on.

Auto Restart Causes the connection to be restarted if it is closed. This is useful for administrators that wish to limit the ability of a user to access the device.

Disable Desktop This will disable desktop access, ensuring that users only access this specific workstation with the specific credentials applied to the connection. Logging off from the server will power off the thin client, and powering on the thin client will bypass the operating system's desktop and immediately log in to the server. This feature is not supported for Windows-based operating systems.

Proxy Settings

Select a Proxy Setting Allows users to select from the various proxy setting options.

Kiosk Mode

Show Menubar Determines whether or not the menubar is displayed to the user.

Use Appmenu Button If the menubar is enabled, an appmenu button may be available for users who wish to access non-standard features. This is a legacy option to support older versions of the application.

Enable Kiosk Mode Toggles Kiosk Mode on or off. When in Kiosk mode, the user is only able to access a limited number of the options Firefox contains.

Show Toolbar Toggles the Firefox toolbar on or off.

Autohide Navbar in Kiosk Toggles whether or not the user can access the Firefox navigation bar.

Allow Quit Determines whether or not the user can quit Firefox.

Advanced Options

Enable Javascript Toggles javascript capabilities for Firefox.

Enable Popup Blocker Toggles the popup blocker abilities of Firefox.

5.3.4 RDP

The RDP protocol is used to connect to Microsoft Windows Device Servers.

Basic Information

Name The name of the connection. The name is a required field when a new connection is created.

Local Display Name The local display name is what the connection will be labeled with on the device. This field is required in order to create a new connection.

Description A description such as "Kiosk Connection" or "Presentation Connection." The description field is optional, but it is recommended to use descriptions to help organize connections.

Protocol The protocol used in the connection is displayed here.

General

Server Name The name or IP address of the RDP server.

Port The port used to access the RDP server.

Username The default username for the RDP server. Leaving this field blank will allow those who use this connection to log in with their desired username when they connect.

Password Setting a password in this field, combined with entering a username above, will enable automatic login as the specified user. This is a legacy option to ensure compatibility with older devices.

Domain The domain name of the user being logged in.

Display

Display The three options listed allow the administrator to set a default display setting for users using this connection. If no option is specified in Echo, the session opens in full screen mode.

Color depth for this connection Allows the administrator to specify a desired color depth for those using this connection.

Use All Monitors This option, when selected, will allow multi-monitor usage for the RDP connection.

Local Resources

Sound Settings Creates a default state for sounds to play through this connection.

Other Settings The administrator can enable a variety of different functions to be available to those using this connection by checking the boxes next to the desired settings.

Start a Program

Program path and filename Entering the path and filename of a program in this field makes it so that when this connection is used, only that specific program can be used in the RDP session.

Working Directory Can be used in conjunction with Program path and filename to specify the specific directory where the file can be found.

Maximize Program Runs the program at maximum size.

RD Gateway

RD Gateway Host The host that will be used for RD Gateway.

RD Gateway Credential Source The method of login access for RD Gateway. You can select password entry, smartcard access, or have the credential source selected on login.

RD Gateway Profile Method The profile method that will be used for RD Gateway. You can select a default mode or use specific settings.

RD Gateway Usage The usage for RD Gateway. You can select always, only if direct connection is unavailable, or just use default settings.

Reuse RD Gateway Credentials When enabled, this will allow the RD Gateway credentials to be reused.

RemoteApp

Application Name Sets the name of the Application.

Application The filename of the Application to be used.

Command Line Enables command line use.

Expand Command Line Expands the Command Line.

Expand Working Directory Expands the working directory.

Application File The filepath for the application.

RemoteApp Mode Set the session for RemoteApp. Users can select between a normal session and a RemoteApp session.

Disable RemoteApp Support Checking When selected, this will disable RemoteApp Support Checking.

Performance

Experience Options This allows adjustments to various settings to suit the user experience desired. These options will determine the connection speed of the network.

Enable bitmap caching This option will allow common .bmp-based images from the session desktop to be stored on the local hard drive. Selecting this option may improve connection performance.

Disable cursor from blinking Indicates that cursor blinking should be disabled during the session.

Scale desktop when resizing session window If the connection session window can be resized, this will allow the session desktop to scale with the window resizing.

Enable window manager's key bindings By default RDP® attempts to grab all keyboard input when it is in focus.

Display the connection bar A connection bar will display at the top when a session is active. This connection bar displays the connection's address and offers other options.

Attach to the console of the server The session will connect to the console of the server (requires Windows® Server 2003 or newer).

Enable RemoteFX Toggles whether or not the connection will use the RemoteFX® feature.

Enable font smoothing This will enable ClearType for the RDP session, making font appear smooth and more clear.

Options

Enable compression of the RDP datastream Depending on network latency, utilizing datastream compression can improve overall communication performance.

Autostart Causes the connection a connection to start as soon as the device is powered on.

Auto Restart Causes the connection to be restarted if it is closed. This is useful for administrators that wish to limit the ability of a user to access the device.

Restart When enabled, the session will restart if the server is disconnected.

Enable CredSSP This will enabled the Security Support Provider for the server. This option is enabled by default.

Disable Desktop This will disable desktop access, ensuring that users only access this specific workstation with the specific credentials applied to the connection. Logging off from the server will power off the thin client, and powering on the thin client will bypass the operating system's desktop and immediately log in to the server. This feature is not supported for Windows-based operating systems.

5.3.5 X11

X11 connections are used to run an X11 application through SSH or to connect to a server via XDMCP.

Basic Information

Name The name of the connection. The name is a required field when a new connection is created.

Local Display Name The local display name is what the connection will be labeled with on the device. This field is required in order to create a new connection.

Description A description such as "Kiosk Connection" or "Presentation Connection." The description field is optional, but it is recommended to use descriptions to help organize connections.

Protocol The protocol used in the connection is displayed here.

General

Session Type The session type for the X11 connection. Users can choose between using an XDMCP connection or using the X11 SSH application.

Server URL The URL (or IP address) of the X11 server.

Username The default username for the X11 session. Leaving this field blank will allow those that use this connection to log in with their desired username when they connect.

Password Setting a password in this field, combined with entering a username above, will enable automatic login as the specified user.

Application Name If the session type selected is X11 SSH App, then an application's filepath can be entered here. Otherwise this field can be left blank.

Screen Resolution The screen resolution for the X11 session. If an X11 SSH App session is in use, then some applications may not support all available resolutions.

Autostart Causes the connection to start as soon as the device is powered on.

Auto Restart Causes the connection to be restarted if it is closed. This is useful for administrators that wish to limit the ability of a user to access the device.

Disable Desktop This will disable desktop access, ensuring that users only access this specific workstation with the specific credentials applied to the connection. Logging off from the server will power off the thin client, and powering on the thin client will bypass the operating system's desktop and immediately log in to the server. This feature is not supported for Windows-based operating systems.

5.3.6 ICA

The ICA protocol is used to establish connections to Citrix servers.

Basic Information

Name The name of the connection. The name is a required field when a new connection is created.

Local Display Name The local display name is what the connection will be labeled with on the device. This field is required in order to create a new connection.

Description A description such as "Kiosk Connection" or "Presentation Connection." The description field is optional, but it is recommended to use descriptions to help organize connections.

Protocol The protocol used in the connection is displayed here.

Connection

Connection Type Allows the connection setting to be changed between a local area network and a wide area network.

Server Location The IP address of the ICA server.

Protocol The type of protocol being used to connect to the ICA server.

Session Type Allows the administrator to select if the connection should be a server connection or a published application.

Name The name of the server or published application desired for this connection.

Options

An administrator can use the dropdown menus in the Options pane to select a number of different display and audio features to customize the connection.

Autostart Allows the administrator to cause a connection to start as soon as the device is powered on.

Auto Restart Causes the connection to be restarted if it is closed. This is useful for administrators that wish to limit the ability of a user to access the device.

Use data compression Depending on network latency, utilizing datastream compression can improve overall communication performance.

Use disk cache for bitmaps Determines whether or not the disk cache is used to when processing bitmaps.

Disable Desktop This will disable desktop access, ensuring that users only access this specific workstation with the specific credentials applied to the connection. Logging off from the server will power off the thin client, and powering on the thin client will bypass the operating system's desktop and immediately log in to the server. This feature is not supported for Windows-based operating systems.

Firewall Settings

Use alternate address for firewall connection If checked, allows users to use the Proxy Type options.

Proxy Type Allows users to choose between SOCKS or HTTPS for the firewall proxy.

Proxy Address The IP address of the proxy server.

Proxy Port The proxy port number to be used for this connection.

User Logon

Username The default username for the ICA connection. Leaving this field blank will allow those that use this connection to log in with their desired username when they connect.

Domain The domain name of the user being logged in.

Application

Application Entering the path and filename of a program in this field makes it so that when this connection is used, only that specific program can be used in the ICA session. This field does not need to be filled out if the session type is a published application.

Working Directory Can be used in conjunction with Application to specify the specific directory where the file can be found.

5.3.7 XenAppView

The XenAppView protocol is also used to establish connections to Citrix servers.

Basic Information

Name The name of the connection. The name is a required field when a new connection is created.

Local Display Name The local display name is what the connection will be labeled with on the device. This field is required in order to create a new connection.

Description A description such as "Kiosk Connection" or "Presentation Connection." The description field is optional, but it is recommended to use descriptions to help organize connections.

Protocol The protocol used in the connection is displayed here.

General Settings

Server Address The URL or IP address of the XenAppView server.

Username The default username for the XenApView connection. Leaving this field blank will allow those that use this connection to log in with their desired user name when they connect.

Domain Name The domain name of the user being logged in.

Autostart Allows the administrator to cause a connection to start as soon as the device is powered on.

Auto Restart Causes the connection to be restarted if it is closed. This is useful for administrators that wish to limit the ability of a user to access their desktop.

Launch in Fullscreen Launches the desktop in XenAppView's fullscreen mode.

Disable Desktop This will disable desktop access, ensuring that users only access this specific workstation with the specific credentials applied to the connection. Logging off from the server will power off the thin client, and powering on the thin client will bypass the operating system's desktop and immediately log in to the server. This feature is not supported for Windows-based operating systems.

5.3.8 Internet Explorer

Internet Explorer is the native browser on Windows-based clients.

Basic Information

Name The name of the connection. The name is a required field when a new connection is created.

Local Display Name The local display name is what the connection will be labeled with on the device. This field is required in order to create a new connection.

Description A description such as "Kiosk Connection" or "Presentation Connection." The description field is optional, but it is recommended to use descriptions to help organize connections.

Protocol The protocol used in the connection is displayed here.

General Settings

Start URL The URL that Internet Explorer will automatically open upon starting.

Enable Kiosk Mode Toggles Kiosk Mode on or off. When in Kiosk mode, the user is only able to access a limited number of the options Internet Explorer contains.

Autostart Allows the administrator to cause a connection to start as soon as the device is powered on.

Auto Restart Causes the connection to be restarted if it is closed. This is useful for administrators that wish to limit the ability of a user to access the device.

5.3.9 VMware Horizon View

VMware Horizon View connections are used for connecting to VMware Servers.

Basic Information

Name The name of the connection. The name is a required field when a new connection is created.

Local Display Name The local display name is what the connection will be labeled with on the device. This field is required in order to create a new connection.

Description A description such as "Kiosk Connection" or "Presentation Connection." The description field is optional, but it is recommended to use descriptions to help organize connections.

Protocol The protocol used in the connection is displayed here.

General

Server URL The URL (or IP address) of the VMware Horizon View server.

Username The default username for the VMware Horizon View session. Leaving this field blank will allow those that use this connection to log in with their desired username when they connect.

Password Setting a password in this field, combined with entering a username above, will enable automatic login as the specified user.

> **Caution:** Passwords cannot be deleted once they have been applied to a connection. If the password field needs to be emptied, a new connection must be made.

Domain The domain name of the user being logged in.

Desktop Name The name of the desktop that the user will connect to. If no desktop is specified, the desktop inventory will display upon user login and a selection can be made there.

Enable Background on Startup This will allow VMware Horizon View to run in the background on start up. This is a legacy option available for devices that are running older versions of the agent.

Protocol The protocol for the server that is being accessed. VMware Horizon View supports RDP and PCOIP protocols.

Desktop Layout The window layout for the VMware Horizon View connection. This option offers a selection of preferred window-mode sizes and a multi-monitor option for extended desktops.

Autostart Causes the connection to start as soon as the device is powered on.

Auto Restart Causes the connection to be restarted if it is closed. This is useful for administrators that wish to limit the ability of a user to access the device.

Disable Desktop This will disable desktop access, ensuring that users only access this specific workstation with the specific credentials applied to the connection. Logging off from the server will power off the thin client, and powering on the thin client will bypass the operating system's desktop and immediately log in to the server. This feature is not supported for Windows-based operating systems.

Options

Disable Menubar The VMware Horizon View menu bar will be hidden from the desktop.

Run Once This will close the VMware Horizon View client completely upon logging out or disconnecting from the server, rather than returning users to the desktop selection options of the client.

Enable kiosk login mode A kiosk-based login mode will be enabled. This option will need to be enabled server-side in order to function.

Lock the server URL field This option prevents users from changing the server or selecting a different server from the client's server selection menu.

Start a Program

Application Name The name of the application that will be run upon server login.

Application Size The window layout for the application that will be run. This option offers a selection of preferred window-mode sizes and a multi-monitor option for extended desktops.

5.3.10 SSH

The SSH protocol is used to connect to a device through SSH.

Basic Information

Name The name of the connection. The name is a required field when a new connection is created.

Local Display Name The local display name is what the connection will be labeled with on the device. This field is required in order to create a new connection.

Description A description such as "Kiosk Connection" or "Presentation Connection." The description field is optional, but it is recommended to use descriptions to help organize connections.

Protocol The protocol used in the connection is displayed here.

General

Server Address The hostname or IP address of the device to SSH into.

Username The default username to login through SSH. Leaving this field blank will allow those who use this connection to log in with their desired username when they connect.

Port The port used to access the device via SSH. Port 22 is the default port.

Host Key The encryption type and host key for the connection.

5.3.11 Telnet

The Telnet protocol is used to connect to a device through Telnet.

Basic Information

Name The name of the connection. The name is a required field when a new connection is created.

Local Display Name The local display name is what the connection will be labeled with on the device. This field is required in order to create a new connection.

Description A description such as "Kiosk Connection" or "Presentation Connection." The description field is optional, but it is recommended to use descriptions to help organize connections.

Protocol The protocol used in the connection is displayed here.

General

Type The type of Telnet connection being run. Certain types have different login options available.

Server Address The hostname or IP address of the device to Telnet into.

Username The default username to login through Telnet. Leaving this field blank will allow those who use this connection to log in with their desired username when they connect. This is only available for *Type: TELNET*.

Port The port used to access the device via Telnet. The default port will change if SSL is enabled or disabled.

Use SSL Enables or disables the use of SSL.

5.4 Profile Details

Name The name of the profile. The name is a required field when a new profile is being created.

Description A human readable description such as "Demonstration Profile." The description field is optional, but it is generally a good idea to utilize descriptions to help organize profiles.

Mode The Mode dropdown menu provides four methods that can be used to apply the selected profile to devices. These modes are prioritized, meaning that if users attempt to apply two profiles to the same device using different modes, the profile with the higher priority mode assigned to it will be implemented while the other is ignored. These modes, in order of priority from highest to lowest, are:

Default Profile A profile created in the Default Profile mode is automatically applied to any new device that connects to the Echo server.

Select Devices The administrator directly chooses which devices the profile is applied to. If two or more profiles with overlapping options are applied to the same device using the Select Devices mode, the most recently applied profile takes precedent for that option. If Select Devices is chosen, the Devices dropdown menu will appear to allow the administrator to select which devices to apply the profile to.

Terminal Details A profile created with the Apply by terminal details mode specifically targets certain types of devices to apply itself to. Device name, IP Address or range, model, and operating system are all options an administrator can use to specify devices. If Apply by terminal details is

chosen, Details options will appear. The administrator can fill out the fields as needed to target the desired devices.

Group Membership A profile created for specific groups that devices apply to. The profile can apply to multiple groups, if necessary. If Apply by group membership is chosen, the Groups dropdown menu will appear to allow the administrator to select which group to apply the profile to.

Disk Image An administrator can use the dropdown menu in the Disk Image section to select which saved disk image will be included in the profile.

Connections An administrator can use the dropdown menu in the Connections section to select which saved connections will be included in the profile.

Device Settings An administrator can use the dropdown menu in the Device Settings section to select which saved device settings will be included in the profile.

Certificates An administrator can use the dropdown menu in the Certificates section to select which saved certificates will be included in the profile.

Software Packages An administrator can use the dropdown menu in the Software Packages section to select which saved software packages will be included in the profile.

5.5 Disk Image Details

5.5.1 Basic Information

Name The name given to a disk image when it is created. This is a mandatory field when creating a new disk image, but can be changed later if needed.

Description Entering a description for a disk image is optional, but doing so is highly recommended.

Filename The filename to be given to the disk image file. The name of the file and the file extension need to be entered here.

Checksum The hash for the disk image. This field will auto-generate if the disk image is coming from an HTTP, HTTPS, or FTP server.

Product Select the product of the disk image from drop-down menu.

Storage Location The storage location that will hold the disk image. The location must have been previously entered in the server's Storage Location tab.

5.5.2 Legacy Options

These options are for when a legacy disk image is being added to the server.

MD5 Sum This is the MD5 sum of the disk image. When applied via a profile, if the two images are the same, nothing will happen. If they differ, the device will apply the image in the profile.

Note: If a thin client that is using DeTOS 7.3 or 7.4 is receiving a disk image upgrade through a Windows Share (`cifs://`) storage location, the SHA1 of the disk image will need to be entered in place of the MD5 Sum. This is always required regardless of legacy status.

5.6 Device Setting Details

5.6.1 Basic Information

Name A mandatory field used to provide a name for the saved set of device settings.

Description An optional description that can be used to provide more information about what is contained in the saved device settings.

Device Settings A list containing all of the cloned settings. Sound, network, time, input, display, permissions, USB permissions, printers, and persistence are all possible options.

5.7 Certificate Details

5.7.1 Name and Details

Name The name given to the certificate by the administrator.

Description An optional field used to provide more details about the certificate.

Certificate The Browse button allows users to browse through files in order to locate a certificate to include in the Certificates section.

5.7.2 Certificate Details

The fields viewed through View Certificate can not be altered manually. These fields are automatically filled in when a certificate has been created or updated and are populated by information provided by the certificate itself. To access this information, click on the Information button that is next to the certificate's name.

Organization The name of the certificate provider.

Organizational Unit The classification of the certificate in the digital hierarchy.

Common Name A name given to the certificate by its creators.

Country The country where the certificate was created.

State The state (in the United States) where the certificate was created.

Locality The city or general area where the certificate was created.

Effective Date The date that the certificate becomes valid for use.

Expire Date The date that the certificate expires and may need to be replaced or updated.

5.8 Task Details

5.8.1 Update Task

When to Run Determines whether the task is to be run immediately or if it is to be executed at a later time.

Task Name The name of the task.

Date/Time The date and time that the task is to be initially executed.

Retries The number of attempts the server will make to execute the task, in case the task is not executed correctly during its schedule.

Frequency The rate at which the task will be executed. If preferred, a custom frequency can also be set.

5.8.2 Task History

Started The start time for the scheduled task.

Finished The completion time for the scheduled task.

Output Output information from the task.

Result The final results of a task.

CHAPTER 6

Legal