verde™ VDI

Administration and Management Guide

Version 8.2

NComputing

NComputing Global, Inc.
1875 S. Grant Street
Suite 570
San Mateo, CA 94402

Phone: 1.650.409.5959
Fax 1.650.409.5958

CONTENTS

Preface

Welcome to VERDE VDI

VERDE, the next generation of VDI, removes the management burden, complexity, and costs associated with desktop virtualization. With hundreds of millions of professional desktops set to refresh, organizations of all sizes are turning to VERDE to provide an easy-to-use, cost-effective approach to provisioning, managing, updating, and securing PC and BYOD (bring your own device) environments.

What is VDI?

With Virtual Desktop Infrastructure (VDI), all programs, applications, and data that traditionally resides on local storage of a desktop is “virtualized” and stored on a remote central server.

What does VDI mean for business?

Organizations enjoy reduced risk and lessen needless downtime. With VDI, your business has greater control over a user' desktop and corporate data. Whether on site or remote, VDI offers real protection to ensure valuable data is no longer stolen, lost, or destroyed.

What does VDI mean for IT?

VDI means not having to rollout an update to every PC individually. With VDI, desktops are managed from a central location. Whether migrating to the latest Windows, installing a new security patch, or re-imaging a single machine, it is easier than ever to administer a PC environment, even across tens of thousands of machines. IT can create a single image and seamlessly roll it out to every machine on the network with the push of a button.

Additionally, should instability occur, the IT administrator can simply rollback to the most recent acceptable state and redeploy.

What does VDI mean for the end user?

End users can access their desktop from any device (PC, notebook, tablet, thin client) and from any location (work, home, library, or while traveling) and access all data. Additionally, VDI often improves productivity by delivering LAN performance for remote branch office users

VERDE VDI and Desktop Cloud Fabric

VDI focuses on the total value delivered, not just in terms of cost, but in other areas such as security, resiliency, continuity, agility, and efficiency. VDI is about helping organizations future-proof their operations for change. If you've done a good job providing that value, then the introduction (and mass adoption) of devices like androids, becomes just another endpoint to support, not an either or proposition.

We've come a long way since first-generation server-hosted desktop solutions that were not only costly, but also complex. VDI enables companies to deliver on the promises of VDI, removing the cost and complexity burdens by offering features that include: integrated online and branch VDI; the ability to transcend on-premises and cloud; unified endpoint management and a high definition end-user experience.

SUPPORTED LANGUAGES

The following languages are available for VERDE and User Consoles.

- Chinese (Simplified)
- Chinese (Traditional)
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Spanish

CONTACT INFORMATION

NComputing Global, Inc.

1875 S. Grant Street

Suite 570

San Mateo, CA 94402

Phone: 1.650.409.5959

Fax 1.650.409.5958

Email: info@NComputing.com.

CHAPTER 1

Introduction

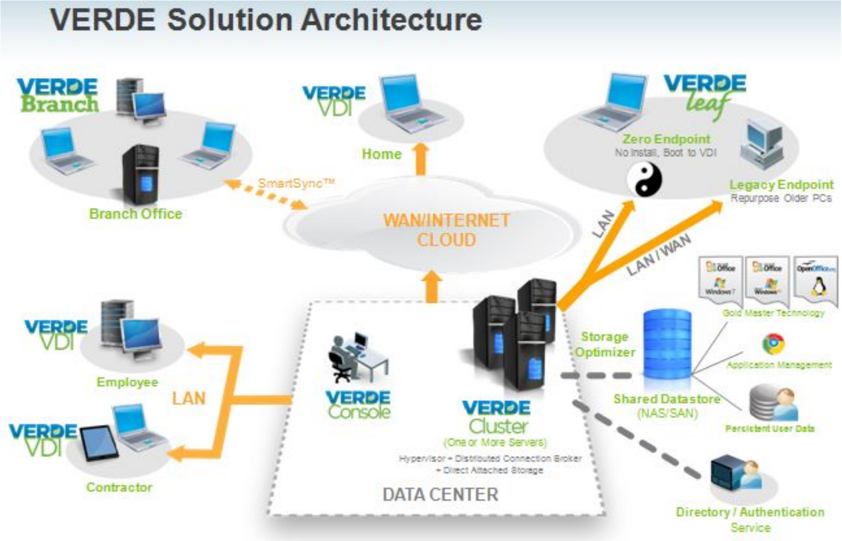
This chapter discusses the following.

VDI is increasingly used by enterprises to evolve IT's desktop delivery strategies. The VERDE software platform powers the deployment of cost-effective, secure, and centrally managed VDI solutions that enable user mobility, business continuity, and significantly lower IT costs in the following ways:

- Cost
  - Requires fewer servers due to high densities for desktop workloads.
  - Works with cost-effective and efficient NAS storage.
- Complexity
  - Offers a single product that installs on all servers and scales horizontally.
  - Offers a single management console for all desktop and operational management.
- Coverage
  - Provides a best-of-breed VDI solution that covers the most comprehensive set of use cases from fully non-persistent desktops to static desktops, and scenarios in between.
  - Offers unique VERDE Branch capabilities that provide a LAN experience for remote offices, enable regional data centers, and offer a hybrid solution with management in the cloud and deployment on premise.
  - Supports both Windows and Linux virtual desktops with feature parity.

VERDE Architecture

The following diagram displays one type of VERDE deployment architecture for a private cloud deployment.



This sample architecture includes a VERDE cluster, console, and branch office. The console and cluster are installed and managed in the data center.

The cluster is attached to the main directory or authentication service to leverage existing user data and policies. The cluster also attaches to the shared storage device and uses it to store master Gold Images of the Windows and Linux desktops.

VERDE Solution Components

The following components make up the VERDE solution:

- VERDE Server and Distributed Connection Brokers
- Master Gold Images
- VERDE Management Console, VERDE User Console, and VERDE native clients
- VERDE Cloud Branch Server
- VERDE Integrations
- RX300 Thin Client

VERDE SERVER AND DISTRIBUTED CONNECTION BROKERS

Each VERDE Server includes an integrated connection broker, a hypervisor to run VDI sessions, and a single management console (VERDE Management Console).

Up to 10,000 servers can be clustered with the VERDE stateless cluster algorithm to provide a highly scalable VDI solution that can support up to one million users.

MASTER GOLD IMAGES

The VERDE Gold Image model enables creation and management of a few desktop images that are accessed by any number of users. VERDE supports Windows Server 2008 and 2012 R2, Windows 7, Windows 8.1, Windows 10, and different Linux desktops from the same infrastructure. Users run a non-persistent copy of the Gold Image with all of their personal settings and documents written to a separate persistent disk.

This model reduces the number of images to manage, which reduces storage and maintenance costs. Because images are read-only, this solution provides native malware resistance to all desktop sessions.

VERDE MANAGEMENT CONSOLE AND VERDE USER CONSOLE

A single web-based VERDE Management Console provides centralized Gold Image management to create, publish, update, clone, and delete images. The VERDE Management Console enables granular desktop security and session policies based on Active Directory or any other directory server.

End user desktop sessions are started through the VERDE User Console and the VERDE Client. The VERDE User Console is now HTML5-based and can be utilized without installing additional software to the client.

VERDE CLOUD BRANCH SERVER

VERDE Cloud Branch solution provides a LAN experience to branch office users. This eliminates the need to connect over slow or unreliable WAN connections. The VERDE Cloud Branch Server connects to the central VERDE Cluster and Gold Image repository to replicate the Gold Images and subsequent updates. The virtual desktop sessions are served locally from the VERDE Cloud Branch Server(s). Gold Images updates can also be performed from the Branch Server. Changes are then synchronized with the image at the data center.

VERDE INTEGRATIONS

- **Directory Servers**. VERDE integrates with LDAP-compliant directory servers that are deployed inside the data center. Administrators can assign Gold Images to directory users or groups. When users log into VERDE, they are authorized to use one of the Gold Image sessions.
- **Shared Storage**. VERDE connects to NAS shared storage. Shared Storage acts as the repository for VERDE Cluster settings, Gold Master Images, and the user's personal data such as documents, settings, and profiles.

Note: The VERDE solution does not require an external database.

RX300 THIN CLIENT

NComputing's RX300 provides a single vendor end point that is designed and supported as a complement to the VERDE VDI software. The RX300 supports RDP, HTML5, and UXP protocol for all VERDE supported Windows desktops. In addition to standard protocol based desktop support, the RX300 is bundled with support for the NComputing VCast video streaming acceleration when combined with the Google Chrome browser. Remote management, software and firmware updates can be deployed remotely to all devices registered with the NComputing Pi Management Console.

LIST OF VERDE DEVICES

- ✓ Windows 7 (32 and 64-bit)
- ✓ Windows 8.1 (32 and 64-bit)
- ✓ Windows 10 (32 and 64-bit)
- ✓ Red Hat & CentOS 6.6 - 6.9
- ✓ Ubuntu 12.04 - 16.04
- ✓ HTML 5 enabled Web Browsers
- ✓ NComputing's award-winning RX-300 Thin Clients
- ✓ Ask your NComputing representative for other currently supported devices.

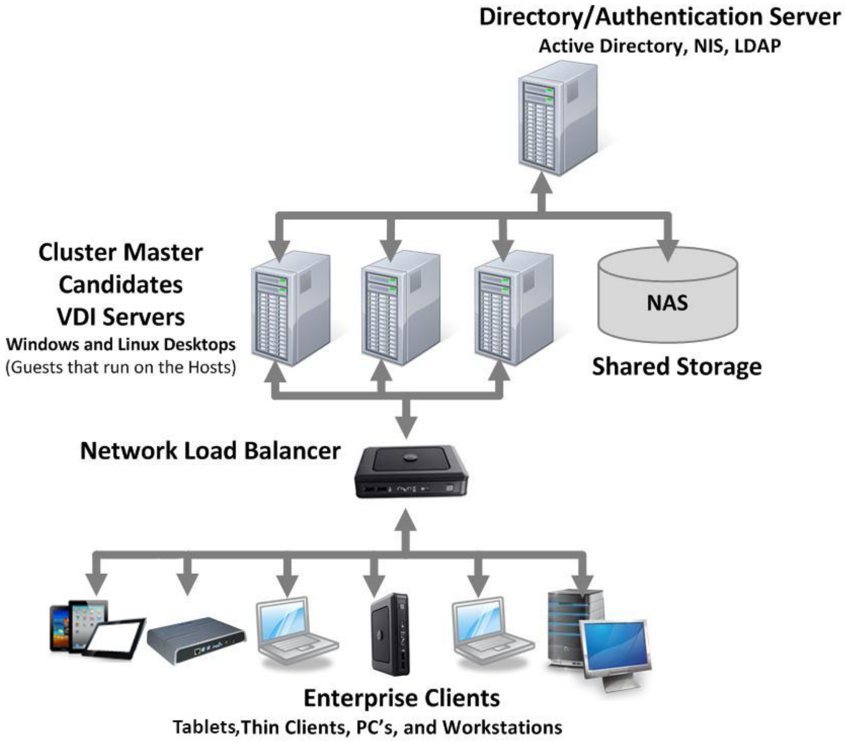
CHAPTER 2

VERDE Server Components and Clustering

This chapter discusses the following.

VERDE offers a highly scalable clustering mechanism to serve hundreds, thousands, or even hundreds of thousands of virtual desktops. A VERDE cluster can scale from two to 10,000 servers, and can host up to one million concurrent virtual desktop sessions, given enough storage and network capacity.

The following diagram illustrates a sample cluster.


Directory/Authentication Server
Active Directory, NIS, LDAP
Cluster Master
Candidates
VDI Servers
Windows and Linux Desktops
(Guests that run on the Hosts)
NAS
Shared Storage
Network Load Balancer
Enterprise Clients
Tablets,Thin Clients, PC's, and Workstations

VDI Server

The VERDE VDI server is one of many nodes in the cluster that serve virtual desktops to users. Users connect to the cluster using an entry point and a session point.

The entry point is any VDI server in the cluster. When a new connection starts, the VDI server automatically checks for either a matching persistent session (if one exists), or a recommended VDI server to host the new session. The VDI server communicates this information back to the client as a referral.

The session point is the referral's IP address. Clients disconnect from the entry point and connect to the session point. Because connections are stateless, the session will have a reservation on the particular server that receives it. Users then authenticate against the configured repository and are either connected to an existing persistent session or given a new session.

CLUSTER MASTER

Within each VERDE cluster, one server is singled out as a managing entity, functioning to control session traffic and distribute activity equally among available servers. This server is the Cluster Master.

The Cluster Master relies on VDI servers to provide and maintain the state information collected from the applications running on those systems. The Cluster Master utilizes this information to relay load balancing results in the form of referrals when new clients connect to the cluster. Existing clients are referred to the VDI servers already running active sessions.

There is only one active cluster master, but any number of VDI servers can be designated a Cluster Master candidate for fail over purposes. VERDE automatically assigns the role of cluster master to one of the candidate servers. A cluster master candidate is defined through the VERDE Menu.

More about the Cluster Master:

- Keeps track of:
  - The status of the other nodes in the cluster.
  - The License utilization, which is managed globally at the cluster level.
  - Logged in users, overall and per server to balance the load across the entire cluster.
- A server designated as the Cluster Master can run with other VERDE Services, but it can also be configured as Cluster Master only. When a server is configured as a “Cluster Master Only,” it’s unnecessary to run the other VERDE Core services (such as Connection Broker, Hypervisor, CacheIO, SmartSync) that are usually required to run virtual desktops. By effect, the server specifications are much lower, allowing the server the ability to run a virtual machine if needed.
- The file that acts as the functional core of a Cluster Master’s processes is located in central storage: `/home/vb-verde/.verde-local/dbaddress`
- Accessed through secure (https) port 8443. Any candidate must assign this port to Cluster Master communication.
- The Cluster Master is stateless; it maintains all state in RAM.

- When the Cluster Master node starts, its internal tables are empty.
- When VDI servers start, they immediately attempt to broadcast their system-level status (CPU load, total session count) to the Cluster Master, and retry every three seconds if previous attempts are unsuccessful.
- Practices a simple fail-over/recovery plan. If a Cluster Master fails, another candidate will be promoted to active Cluster Master, and VDI servers will continue to operate and retry to connect to the stand-in Cluster Master. Once a Cluster Master becomes available again, the existing state is automatically transmitted to it, and within seconds, the Cluster Master will contain all the information about the cluster that it missed when it was down.
- VDI servers broadcast session start/stop information to the cluster master as it happens, unless they are connecting (or reconnecting), in which case all the information is sent at once.
- The load balancing algorithm may result in new sessions always starting on the same server until that server's cumulative load rises to the level of the other servers.
- The VERDE Console – Management Console (MC) is also active on the same server as the Cluster Master. It works with the Cluster Master to fulfill user authentication and desktop provisioning, as well as VERDE Cluster Configuration and monitoring.

Cluster Master Fail-over Process

Any VDI server can be designated a Cluster Master candidate. There is no limit to the number of cluster master candidates per cluster. Any VDI server can be set as a candidate for fail over as long as it meets the Cluster Master system requirements.

It takes between 90 seconds and two minutes for the automatic fail-over to take place. During that time, the user sessions remain active, only new sessions cannot be started.

The secure (https) port 8443 must be the same on every cluster node.

MANUAL FAIL-OVER

To stop a cluster master, stop the VERDE service on that node. To manually assign a cluster master candidate as the cluster master, confirm that it is the first server to start.

Important: Wait 90 seconds to two minutes before starting the other cluster master candidate nodes.

VERDE MANAGEMENT CONSOLE FAIL-OVER

The VERDE system has one exclusive component on each cluster, which is the VERDE Management Console database. The VERDE Management Console runs on the same server as the active Cluster Master and manages its own database engine on the local node. Regardless of where the engine is running, the database files are located in shared storage.

When a cluster master fail-over occurs, the VERDE Management Console will also fail-over automatically. There is no need to know which server is running the VERDE Management Console, the request is automatically redirected to the active console. To access the VERDE Management Console, enter the URL of any cluster node.

```
https://<Server-IP>:8080/mc

or

https://<Server-IP>:8443/mc
```

Clustering System Requirements

This section discusses system requirements for the VERDE clustering components. The following should be considered prior to installing VERDE:

- Multiple cluster master candidates can be configured.
- Confirm that the DNS entries for host names exist on the DNS server.
- During cluster set up when using Network File System (NFS) export, `no_root_squash` is required to allow clients to connect.
- The role of each node is configured in the VERDE Menu or from the VERDE config script.
- The VERDE license is managed centrally from the VERDE Management Console for the entire cluster, not at the node level.
- If the node will function as a cluster master candidate and a VDI server, the node needs to meet both sets of requirements.

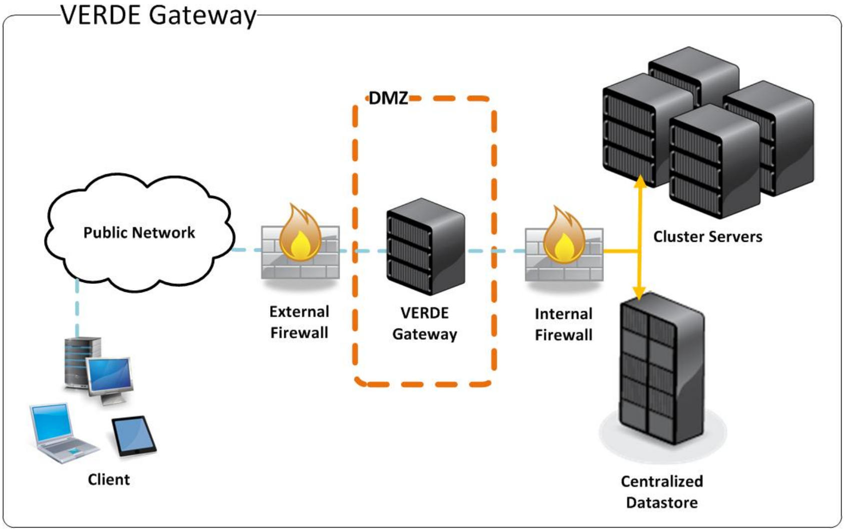
System	Requirements
CLUSTER MASTER SYSTEM	Linux server with 64-bit x86 Intel or AMD processor. See "Supported Platforms" in the **Configuration Planning and Installation Guide** for more details. 8 GB RAM minimum. Ethernet networking (Gigabit recommended). 10 GB free local storage minimum. If the cluster master is running as a standalone, not combined with a VDI node, it can run in a virtual machine.
VDI SERVER SYSTEM	Linux server with 64-bit x86 Intel or AMD processor, VT/AMD-V capable, multiple sockets (multiple cores per socket). See "Supported Platforms" and "Sizing for Desktops" in the **Configuration Planning and Installation Guide** for more details. 8 GB RAM minimum for the system in addition to the RAM required for the guest sessions. Ethernet networking (multiple adapters with gigabyte or faster capacity recommended). The Gold Images and user data are stored on the shared storage, but it is recommended to use the local server drive for optimal and transient storage. See "Shared Storage Planning" in the **Configuration Planning and Installation Guide** for more details.

AUTHENTICATION SERVER	Any LDAP-compliant platform, including Microsoft Active Directory Gigabit, or faster, networking capacity. **Note:** The AD server can be run as a VM in a VERDE Desktop VM using Microsoft Server 2012 R2 or Server 2016 as the desktop. Contact **NComputing support**for more details.

VERDE Gateways

A gateway is a server network node that provides access into and out of a network. Set up VERDE Gateways to communicate with VERDE servers located in a secure environment. VERDE Gateways reside within the Demilitarized Zone (DMZ) to reduce exposure to internal servers. VERDE Gateways provide secure public network access and grant remote users proper access to the internal network where VERDE, applications, resources, and internal data resides. Communication between client devices and the isolated gateway is encrypted. Users must log in to the secure network with valid user credentials to access their virtual desktop (s).

This figure shows one of many ways to set up this configuration.



REQUIREMENTS FOR A GATEWAY ENVIRONMENT

An isolated gateway requires the following:

- At least one VERDE server.
- At least one network interface controller (NIC) with access to both internal and public networks, or two NICs (one for internal access and one for external).
- Configure Isolated Gateway Servers to reside within the authorized demilitarized zone (DMZ).

Note: The VERDE Gateway server can be run as a standalone VERDE component in a virtual machine. Contact **NComputing support** for more details.

PREPARATION FOR A GATEWAY ENVIRONMENT

Before configuring the cluster master and the VERDE Gateway servers, prepare the following:

- Download the VERDE installation package onto the cluster master candidates and the Isolated Gateway server(s).
- On the GTW server, designate a system user (vb-verde) with the same UUID and GUID as the infrastructure. The system user is the designated isolated gateway administrator role.
- Determine the IP addresses of each cluster master candidate. Set up of Isolated Gateways requires a list of assigned server IP addresses for use during VERDE configuration.

Set up the following ports to facilitate communication between the public network and the internal data center via the Isolated Gateway host(s).

Table 2-1 Public Network to DMZ

Public Network Connection Port (Public IP)	DMZ Connection Port (Gateway IP)
48622	48622
443	8443

Table 2-2 DMZ to Internal Network

DMZ Port (Gateway IP)	Internal Network Connection Port (*CM or **VDI Server)
48616	48616*
48622	48622**

Note: Configure the VERDE gateway in a test environment prior to implementing it in a production environment to ensure that all settings work correctly.

VERDE Cloud Branch Environment

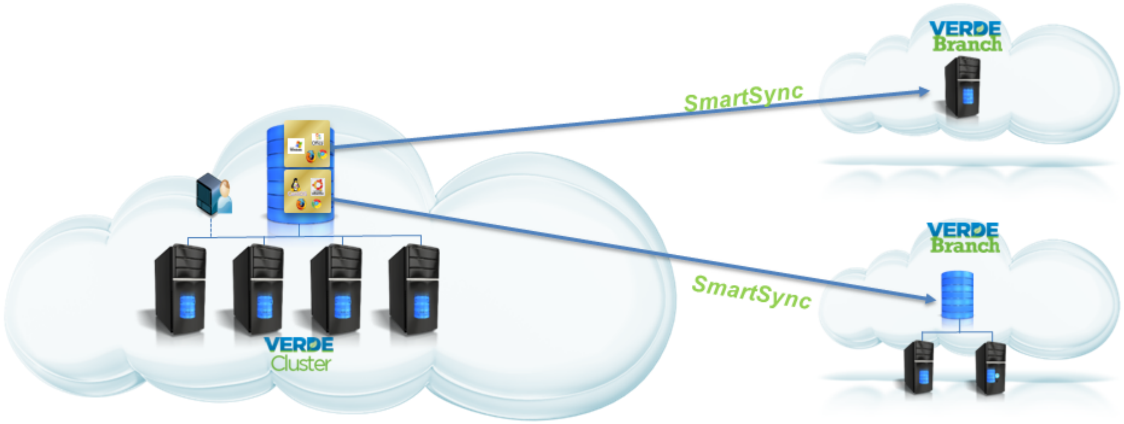
VERDE Cloud Branch allows you to centralize the management of remote facilities (branches, regional data centers) to large enterprises with multiple locations and Managed Service Providers (MSP's). The VERDE Cloud Branch solution includes:

- The desktop runs locally.
- Automatic Replication Technology using our SmartSync™ Protocol.
- Tolerates Intermittent Branch Connectivity.
- Security isolation. There is no requirement for Core to Branch Network.
- OS Gold images, policies, and critical data are synchronized between the central cluster and regional data center or branch office.

The Cloud Branch can be a single machine serving a handful of users, or a large cluster of VERDE servers in a regional data center that may be serving thousands of users. No matter the size, the management will remain centralized.

The Cloud Branch solution consists of two parts:

- **In the Data Center**. A VERDE Server or cluster with access to Gold Image storage and provisioned users at the data center. The Gold Images and system and user policies are automatically synchronized via the Smartsync™ protocol between the Data Center (DC) and the regional Data Center or Branch Office.
- **In the Branch**. A VERDE Server or cluster synchronizing Gold Images from the data center, and serving dynamic instances of the cached Gold Image to its own set of users. The virtual desktops run locally, providing LAN performance and availability to the Cloud Branch users. Because the Gold Images and user data are stored locally, the branch does not require a permanent connection with the Data Center, and can operate even if the Data Center is down or connectivity to the Data Center is severed. Like the Data Center, the Branch can scale horizontally from one to hundreds of servers.



CLOUD BRANCH DEPLOYMENT

Gold Images can be checked out to the branch server and modified at the branch. The changes to the image are saved when the image is checked in. The VERDE Management Console maintains a history of the images and their locations. The branch server synchronization daemon contacts the data center at a defined interval (five minutes by default) to check for additional updates.

Users can be created and managed at the local branch, or managed at the data center with a centralized authentication system, such as Active Directory. Centralized user management requires that the Cloud Branch server be joined to the domain. Using Active Directory replication is possible; users can login via their AD credentials, even if the branch is temporarily disconnected from the central VERDE server.

The following steps outline the workflow for the cloud branch and data center relationship:

- VERDE is installed in the central data center/headquarters and in the remote branch location.
- For remote administration, the central data center needs to be accessible from the branch servers.
- Gold Images are created in the central data center or the branch, and are either checked out to the branch or assigned a Desktop Policy with the deployment mode set to the Branch.
- Checking the image out to the branch gives the branch permission to make changes. When the Gold Image is checked in, the changes are saved to the data center.
- User access and session settings are assigned to the Gold Image from the data center.
- On the Cloud Branch server, the synchronization daemon contacts the VERDE Server to check for policy and session settings updates and synchronize Gold Images that are not checked out to the branch. Synchronization is two-way.

Note: If a user logs in from a location other than the branch, the user will be able to launch the session but will not recover his/her documents from the previous connections.

CHAPTER 3

Virtual Desktop Networking

This chapter discusses the following.

VERDE supports two networking options. If no configuration is done, virtual machines use NAT. Once networking is configured, settings are applied to Gold Images and guest sessions.

Bridged networking now enables Virtual Local Area Network (VLAN) tagging and port bonding, which are also configured in the VERDE Menu.

NAT NETWORKING

NAT networking provides a platform to deliver services securely, without exposing the virtual machine to the network at large or requiring a unique IP address across the subnet. In this mode, the virtual machine does receive an IP address, but that address is visible only to the host server and it is managed automatically by VERDE. Virtual machines do not receive inbound network connections when using NAT networking, which increases the level of security and diminished the need for firewalls inside a guest image. However, outbound traffic has access to all routes on the host.

NAT uses two connection interfaces.

- The primary interface is used for guest-to-host and host-to-guest services and is configured on the private interface, such as `10.0.2.x`.
- The secondary network interface uses DNS to route to the external networks connected to the host. By default, a virtual subnet of `192.168.84.x (netmask 255.255.255.0)` is assigned.

This interface should not be reconfigured unless one of the following is true:

- The subnet needs to be changed.
- The interface is placed on a VLAN.
- The interface is disabled.

Bridged Networking

Bridged networking enables full access to a physical network from a virtual machine. Use bridged networking to assign one or more network interfaces to guest session traffic. Bridged networking provides the following:

- Virtual machines have full access to a specific host-attached network, allowing advanced functions such as network share browsing.
- Virtual machines can export shares or allow inbound connections from other clients or virtual machines.
- Virtual machines must receive a unique IP address from a DHCP server, or configure one statically. This IP address must be unique in the subnet.
- VLAN tagging.

As with NAT, bridged networking uses two connection interfaces:

- The primary interface is used for guest-to-host and host-to-guest services, and is configured on a private subnet, such as **10.0.2.x**.
- The secondary interface binds to a physical or logical Ethernet interface on the host and maintains real network parameters (IP address, netmask).

To set up multiple interfaces for bridging without bonded ports or VLAN networking, use the VERDE Menu.

Open vSwitch Networking

Open vSwitch is a multilayer software switch that supports standard management interfaces and is designed for virtual environments. Open vSwitch is a type of bridged networking that enables VERDE to use VLAN tagging and port bonding to enhance security and increase network bandwidth. When configured, it replaces the standard Linux bridge networking.

Open vSwitch functions as a virtual networking switch. When configured with VERDE, the following features are available:

- Standard VLAN model with trunk and access ports.
- NIC bonding.
- Per session bandwidth controls through Session Settings.

Note: If configuring multiple VLAN host interfaces, one interface must have a static IP address. Multiple DHCP interfaces without a static IP interface are not supported. An interface with a static IP address is needed to determine the default route.

BONDED PORTS

One or more network interfaces can be bonded together to act as one physical interface. Interfaces can be bonded to increase networking speed or as a failover mechanism. Once a single network interface is configured, additional networks are configured as "slaves" to the first network bridge.

Bonded interfaces are represented by a unique port on the network device called the trunk. This port passes tagged or untagged packets from the Open vSwitch on to the physical networks.

VLAN TAGGING

A VLAN enables one or more virtual networks to travel across a physical interface. Each Ethernet packet contains a field called VLAN tag that, if configured, determines the virtual network on which it will travel. The tag, assigned by the internal Open vSwitch, is used to appropriately route the packet and is removed once the packet reaches the external destination switch. See the standard developed by **IEEE 802.1** for more information.

VLANs are set on the host and are assigned to guests through Session Settings.

- VLAN assignments for guests are set in Session Settings. The interface name of the network created in VERDE Menu (NETWORK1, or NETWORK2 for example) is defined there. The VLAN number is also defined in Session Settings.
- Server interfaces (storage NFS connection or User Console for example) are assigned a VLAN tag in the VERDE menu.

Firewall Considerations For Non-Bare Metal VERDE Servers

To permanently disable the iptables firewall, enter the commands in the table below as root:

Table 3-1 Commands for Disabling the iptables Firewall

Action	Command
Stops VERDE Services.	`service VERDE stop`
Turns off iptables.	`service iptables stop`
Turns off iptables at each reboot. This will disable them from coming on again.	`chkconfig iptables off`
Restarts VERDE.	`service VERDE start`

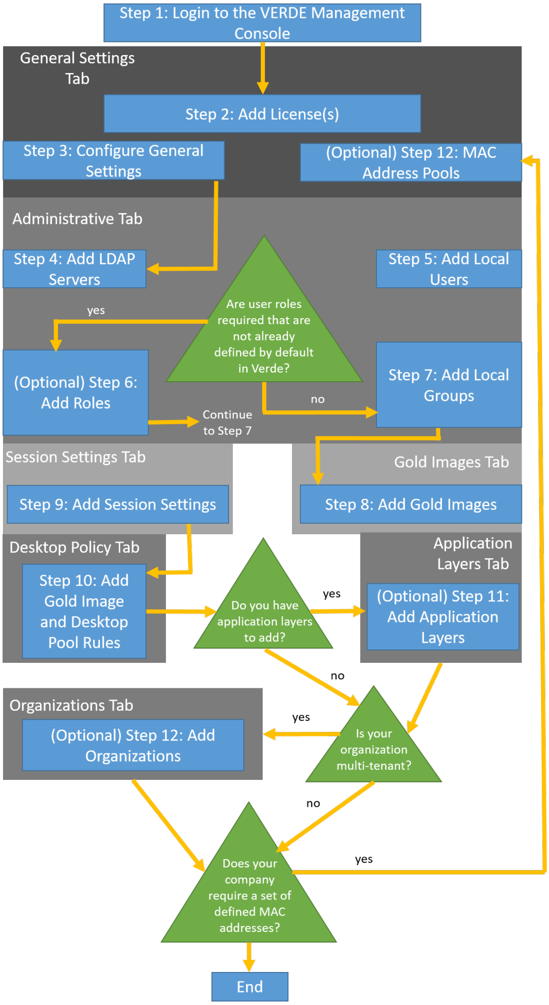
CHAPTER 4

VERDE Management Console

This chapter discusses the following.

The VERDE environment and virtual desktop sessions are managed from the VERDE Management Console, which is accessed from a standard web browser. You must have the correct privileges in order to access the console.

As your VERDE experience grows, the actions you'll be performing on the console and the sequence by which you'll be performing them will change, but if you're accessing the VERDE Management Console for the first time, the order for which you'll be performing tasks will look similar to the chart on the following page.


Step 1: Login to the VERDE Management Console
General Settings Tab
Step 2: Add License(s)
Step 3: Configure General Settings
(Optional) Step 12: MAC Address Pools
Administrative Tab
Step 4: Add LDAP Servers
Are user roles required that are not already defined by default in Verde?
Step 5: Add Local Users
yes
(Optional) Step 6: Add Roles
no
Step 7: Add Local Groups
Continue to Step 7
Session Settings Tab
Gold Images Tab
Step 9: Add Session Settings
Step 8: Add Gold Images
Desktop Policy Tab
Application Layers Tab
Step 10: Add Gold Image and Desktop Pool Rules
Do you have application layers to add?
yes
(Optional) Step 11: Add Application Layers
no
Organizations Tab
yes
(Optional) Step 12: Add Organizations
Is your organization multi-tenant?
no
Does your company require a set of defined MAC addresses?
yes
End

Starting the VERDE Management Console

Launch the VERDE Management Console from a browser with one of the following:

```
https://<server-name-or-IP>:8443/mc
```

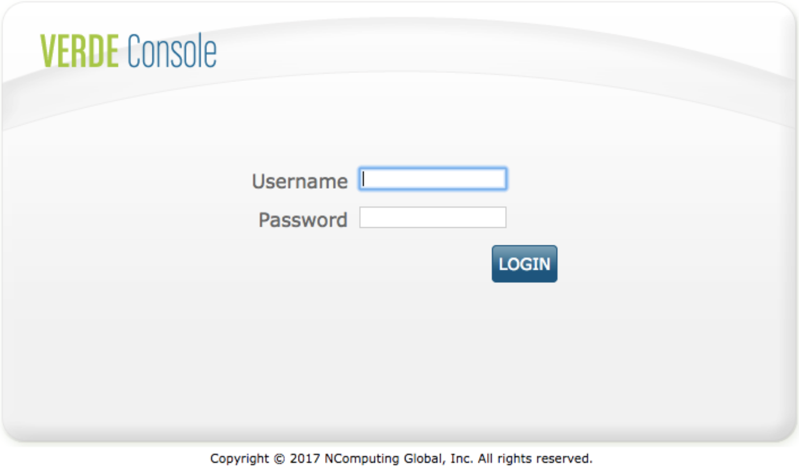
or

```
http://<server-name-or-IP>:8080/mc
```

Port 8443 is the default port. If VERDE was configured with a different port, enter the port defined during the VERDE post installation configuration and open this port in the server firewall configuration.

Note: If a bare metal install was performed, then the management console and user console can be accessed by ports 443 and 80. If you would prefer to restrict bare metal access to these ports, you can block them via iptables or an ACL on the switch.

Log into the VERDE Management Console using the console administrator ID.

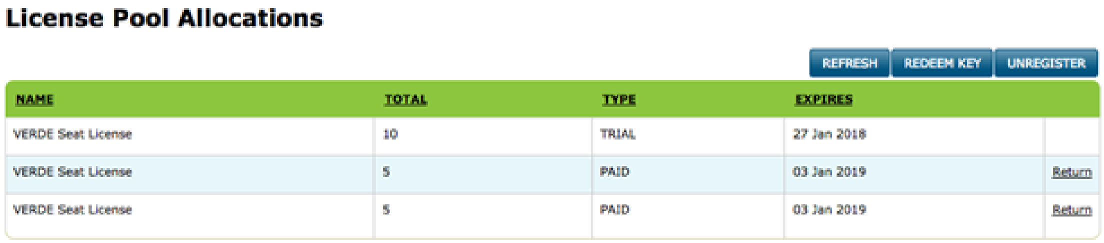

VERDE Console
Username
Password
LOGIN
Copyright © 2017 NComputing Global, Inc. All rights reserved.

Setting General Configuration Parameters

After you have signed into the VERDE Management Console, look on the left of the screen where the **General Settings** tab is displayed. Under this tab, you'll perform the first steps needed to get VERDE off and running.

ADDING VERDE LICENSES

In VERDE 8.2 a new licensing model is being introduced to improve the security of licenses and make it easier for customers and partners to manage license keys.



License Pool Allocations

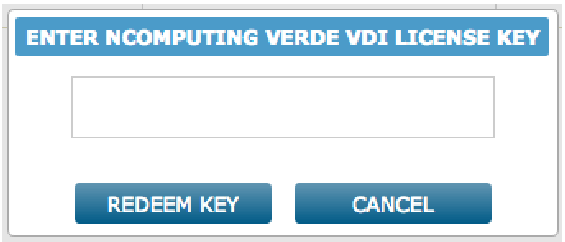
NAME	TOTAL	TYPE	EXPIRES	
VERDE Seat License	10	TRIAL	27 Jan 2018	
VERDE Seat License	5	PAID	03 Jan 2019	Return
VERDE Seat License	5	PAID	03 Jan 2019	Return

The registration and licensing for VERDE 8.2 follows the techniques implemented in NComputings management portal for vSpace Pro. In order to acquire a VERDE license key, the administrator must have or create a registered user account in the NComputing Management portal. This is a free account and can be obtained by registering a username, domain, and password at:

https://www.ncomputing.com/en/user/login?destination=frontpage-en

Alternatively, the user can create an account or login to the management portal directly from within VERDE during the installation process.

During VERDE installation the administrator will be asked to redeem and download one or more license keys. VERDE can hold multiple license keys with different numbers of seats and different expiration dates. All licenses installed in VERDE that are not expired will be aggregated and used as the total number of concurrent user sessions ("seats") allowed for an individual VERDE instance (single server or cluster). If a customer had multiple VERDE instances licensed seat can be allocated, reallocated and redeemed for use on different VERDE instances.

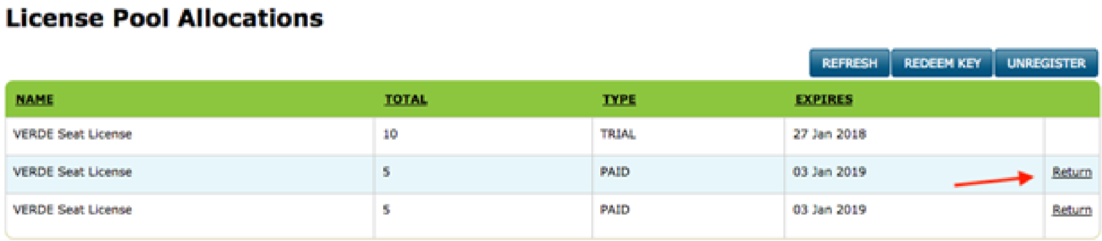


A trial license for VERDE seats is automatically generated by the Management Portal upon registration. Trial licenses permit full VERDE functionality – no limitations. The trial license parameters (i.e., quantity and term) is defined in the Management Portal.

A license key for additional seats/term can be redeemed in the Management Portal and allocated to registered VERDE installations. It is not necessary to remove the trial license when adding purchased licenses. The trial licenses will continue to be counted in the total number of available seats until the expiration of the term of the trial.

Once a license key is obtained that key will be emailed to the person who purchased the key and that key will be used in the VERDE license management tab to redeem it. Once redeemed, the purchased seats will be added to the available licensed seat count.

VERDE licenses can also be returned to the management portal as available unredeemed seats either by de-registering a server instance, or by releasing licensed seats back to the Management Portal for subsequent reallocation.



License Pool Allocations

NAME	TOTAL	TYPE	EXPIRES	
VERDE Seat License	10	TRIAL	27 Jan 2018	
VERDE Seat License	5	PAID	03 Jan 2019	Return
VERDE Seat License	5	PAID	03 Jan 2019	Return

The use of the Refresh button will retrieve and list updated licensing information from the Management Portal.

EDITING GENERAL SETTINGS

Configurationparameters for the VERDE environment and virtual sessions can be defined or adjusted after installation. From the VERDE Management Console, select **General Settings> General Settings**.

Advanced Settings

ADVANCED SETTINGS

The following advanced settings are available:

- **Dynamic Network Configuration**. Enables Dynamic Network Configuration by importing a `netcfg.csv` file.
- **Web Server Certificates**. Enables updating of signed certificates to the VERDE Server. Perform the following steps to update certificates:
    a. Select "Export CSR." A CSR is generated from `$CERT_DIR` on the VERDE Server.
    b. Outside of the VERDE Management Console, have the CSR signed with a certificate authority.
    c. In the VERDE Management Console, select "Import Certificates."
    d. In the **Import Certificates** dialog, browse to select the signed certificate file and the Root/Chain certificate file.
    e. Select "Apply Certificates to the Cluster."
    f. Restart the VERDE Server and connect with HTTPS.

BRANCH CLUSTER SETTINGS

The **Branch Cluster Settings** screen lists the branch clusters in the VERDE system and enables adding a user-friendly name to the cluster. If there are multiple branch servers in the environment, the fully-qualified domain name of the cluster master is listed. This name represents the cluster, not individual servers in the cluster.

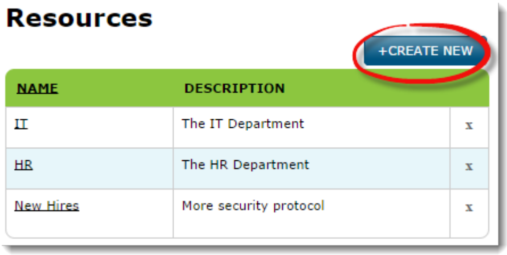
To assign a name to a cluster, select "EDIT," then enter a name, and select "Save."

Note: To delete a branch cluster, each branch server must first be deleted from the Reporting screen.

CREATE COMPUTER RESOURCES

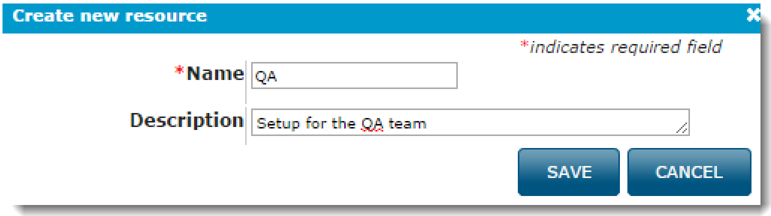
Resources are identification tags that enable resource assignment in a clustered environment. In multi-tenant environments, resource tags can be associated with specific servers to limit one or more servers to use only those hardware devices. Isolation of servers is one of the advantages of multi-tenancy. These settings are managed in the Organizations panel.

1. Select "Resources" from the **General Settings** menu.
2. The **Resources** screen will open. Select "CREATE NEW."



NAME	DESCRIPTION	
IT	The IT Department	x
HR	The HR Department	x
New Hires	More security protocol	x

3. The **Create New Resource** window will appear. Enter a name for the resource and an optional description.



*Name: QA

Description: Setup for the QA team

4. Select "SAVE" to save your new resource.

Administration

The Administration screens enable role-based user and group management, either locally or through an LDAP connection to an LDAP compliant directory structure.

ROLES AND PERMISSIONS

VERDE comes with a set of predefined roles and permissions. Existing roles cannot be edited. Multiple roles can be assigned to local users, local groups, or directory service users (by specifying user@domain), and directory service groups (by specifying the Group DN and realm). An administrative user can be assigned multiple roles.

VERDE provides the following predefined roles:

- ✓ **Management Console Master Administrator**. Has full permissions for all tasks. This is the only role that has full rights for LDAP and local user management and permission assignment.
- ✓ **Management Console User**. Can configure LDAP for the system and has full permissions for all other tasks.
- ✓ **Desktop Administrator**. Has full permissions for Gold Images, Sessions Settings, Application Layers, Desktop Policy. Read-only for all other configuration items. No Maintenance" permissions. Can manage sessions for Reports and view report data.
- ✓ **Helpdesk Administrator**. Has permission to manage sessions for Reports and has read-only permissions for all other tasks.
- ✓ **Analyst**. Has read-only permissions for all configurations, no permissions for Maintenance, and read only permissions for Reports.
- ✓ **Organization Administration**. Can perform Administration tasks for an organization.

Note: Roles and permissions are for administrative purposes. To create a user with no administrative rights, leave the **Role** field empty when creating a user.

Granular permissions are available for creating roles or editing existing roles.

Table 4-1 Roles, Permissions, And Requirements

VERDE Management Console Roles	Permissions	Requirements
Gold Images	Read-only, Operations, Owners, Full	
Application Layers	Read-only, Full	
Session Settings	Read-only, Full	
Desktop Policy		Full requires Gold Images (read-only), Session Settings (read-only), Application Layers (read-only), Desktop Pools (read-only)
Desktop Pools	Read-only, Full	
Administration		Requires Management Console Master Administrator role
General Settings	Read-only, Full	
Organizations	Read-only, Administration, Full	The Administration permission doesn't provide any permissions for the VERDE Management Console in the Global space.
Maintenance	Full	
Reports	View, Manage Servers, Manage Sessions	

Permissions are mapped to the tasks in the VERDE Management Console **Configuration** tab. Permissions include:

- **Read-only**. Allows users to view or list objects.
- **Full**. Allows users to view, list, edit create, or remove objects.
- Gold Image permissions, in addition to read-only are:
  - **Operations**. Enables creating, cloning, editing, and deleting images and performing operations on all images owned by the user with this role.

- **Owners**. Enables creating images, performing image operations on images owned managing image owners on images I already own.
- **Full.** Enables all permissions on all images.

✓ For organization roles, the following apply:

- The creator of an organization automatically becomes the first administrator for that organization, with a master administration role for that organization. Additional administrators can be defined in the organizational scope.
- Users and administrators are assigned to the organization through directory service realms.
- **Full**. Allows users to edit any organization.
- **Administration**. Enables a user to be master administrator for a specified organization.

✓ **View** permission in Reports also allows managing charts. Charts will only display the information that is available to an administrator or user.

✓ **Manage Servers**. Allows taking servers offline or online, and removes branch servers.

✓ **Manage Sessions**. Allows shutting down user sessions.

✓ **Full** permissions in General Settings enable revoking MAC addresses (from the **Reporting** tab).

CREATE VERDE USERS

The **User** screen lists individual users created for VERDE access. Local user accounts created in VERDE reside in the VERDE database. An LDAP server can also be used to manage/assign accounts. Once an account is created, the password, and group assignment can be changed by selecting the user name in the table.

To add a new administrator or user:

1. Select "CREATE NEW" and enter the name of user. This cannot be edited.
2. Select the "Local User" or "LDAP User" type. If you've selected a local user, enter and confirm a password for this account. If you chose an LDAP user type, select the **LDAP Server** in which this account resides.
3. **(Optional)** If you're adding a local user, search for and select one or more groups from the list.
4. Select "Save."

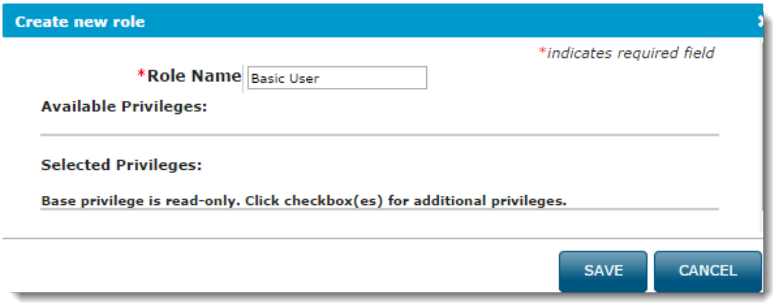
Note: A user cannot be deleted while still assigned in a Desktop Policy rule.

CREATE A ROLE

The purpose of Roles in VERDE Management Console is to expedite the process of assigning privileges to VERDE users. A Role is a predefined list of privileges that can be used to assign identical privileges to one or more users quickly and easily.

The VERDE Management Console comes with predefined Roles, but you may also create a new Role to further define application accessibility. Perform the following steps to create a Role:

1. On the **Roles** screen, select "CREATE NEW."
2. On the**Create New Role**window, enter a name in the "Role Name" field. Names are case sensitive.
3. Select the task group to assign to the role. Once the object is selected, it is added to the "Selected Privileges" list and a sub-set of privileges will be displayed.



Create new role

*indicates required field

*Role Name: Basic User

Available Privileges:

Selected Privileges:

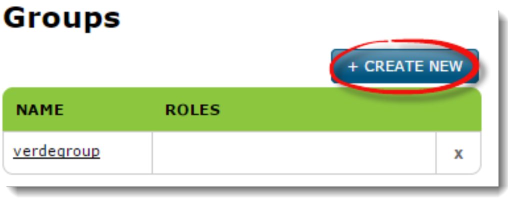
Base privilege is read-only. Click checkbox(es) for additional privileges.

4. Select the privileges for this role. See Roles and Permissions on p. 40 for more details. If no permissions are selected, read-only is assumed for an object.
5. Select "Save" to save the new role.

CREATE VERDE GROUPS

The **Groups** screen enables creating and editing groups for use in VERDE. Groups can be local VERDE groups or LDAP groups. Users are assigned to groups through the **Users** screen.

1. Select "Create New" to add a new group.



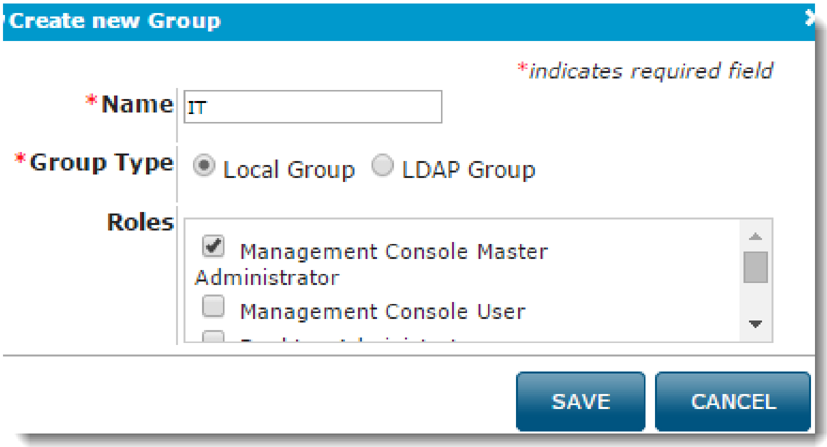
Groups

+ CREATE NEW

NAME	ROLES	
verdegroup		x

2. Enter a name for the group.
3. Select the "Local Group" or "LDAP Group" type.
4. If you selected an LDAP group, select the LDAP server in which the group resides.

Note: A group cannot be deleted if assigned in a Desktop Policy rule.



Create new Group

*indicates required field

*Name IT

*Group Type ● Local Group ○ LDAP Group

Roles
☑ Management Console Master Administrator
□ Management Console User
□ Desktop Administrator

Managing Directory Users and Groups

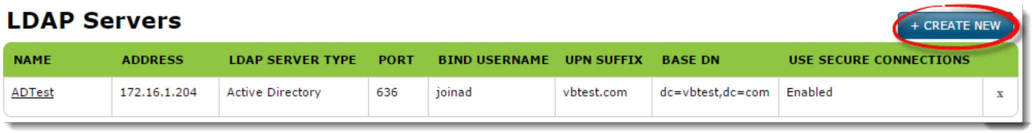
Use directory services with VERDE dynamic virtual desktops by configuring VERDE to connect to any LDAP-compliant directory. There are two connectors provided:

- Optimized connector for Active Directory. To join a virtual desktop to Active Directory, the host server must have DNS set to the address of the Domain Controller.
- LDAP connector that works with other directories such as OpenLDAP, Novell eDirectory, and IBM Tivoli DS. Once the LDAP connection is configured in the VERDE Management Console, session settings are used to assign settings.

Important: The Session Settings function on the VERDE Management Console has the ability to enable Windows Guest sessions, but Linux guest sessions will require a third-party application to authenticate with a directory service. This is because Linux virtual desktops require configuring the virtual desktop itself to join a domain. Additionally, this method may not provide single sign-on (SSO), because users must authenticate to VERDE and then authenticate to their respective virtual desktops once VERDE authorizes them.

To add a new LDAP compliant directory, complete the following steps:

1. Open the **LDAP Servers** screen.
2. Select "CREATE NEW."



LDAP Servers

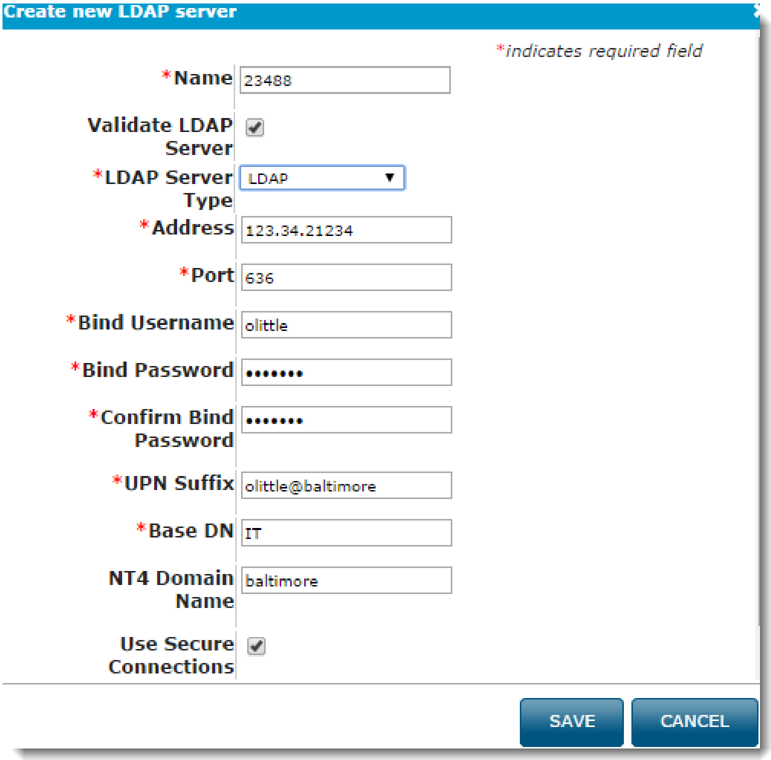
NAME	ADDRESS	LDAP SERVER TYPE	PORT	BIND USERNAME	UPN SUFFIX	BASE DN	USE SECURE CONNECTIONS	
ADTest	172.16.1.204	Active Directory	636	joinad	vbtest.com	dc=vbtest,dc=com	Enabled	x

3. A new window will appear. In the field beside "Name," enter a name for this connection. Names are case sensitive and cannot be changed once added. A directory user is represented in VERDE in the form of `<user>@<name>` where `<name>` refers to the name listed here for this directory. This is the format that is used for VERDE Management Console login, Desktop Policy, and Session Settings.

   Directory groups are represented as `<group>@<name>`. In Desktop Policy, the group is specified as `%<group>@<name>`. The name must be unique so that users are correctly identified. Note that the UPN Suffix can be repeated across multiple LDAP specifications VERDE. This enables creation of different connectors and Desktop Policies for different OUs within the same directory.

4. Use the "Validate LDAP Server" option (enabled by default) to confirm that the connection information is valid. Do not select this option if only a branch server is connected to the LDAP server.
5. Select "LDAP" or "Active Directory."

6. Enter the information listed in the LDAP Settings table to define a connection.



Create new LDAP server

*indicates required field

*Name	23488
Validate LDAP Server	☑
*LDAP Server Type	LDAP ▼
*Address	123.34.21234
*Port	636
*Bind Username	olittle
*Bind Password	•••••••
*Confirm Bind Password	•••••••
*UPN Suffix	olittle@baltimore
*Base DN	IT
NT4 Domain Name	baltimore
Use Secure Connections	☑

7. Save the settings. You'll see the new LDAP server on the **LDAP Servers** screen. Users and groups can be assigned to the server through a Desktop Policy.

Table 4-2 LDAP Settings

Setting	Description
Address	The host name or IP address of the directory server. The VERDE cluster master uses this address to access the server. Multiple addresses can be entered, separated by comma. For example, 132.16.1.204, vbad.NComputing.com. When setting up the LDAP connection, VERDE will try to bind to all the addresses listed in order until an available server is found that authenticates the admin user and can read the groups for that user.
Port	The LDAP server listening port. The secure port is recommended. The default SSL port is 636. The non-secure port is 389.
Bind Username	The user belonging to this directory that has permissions to view the entire directory (or OU) as specified in the LDAP connector. For OpenLDAP, this username is represented as a distinguished name (DN), such as cn=administrator, dc=group, dc=coompany, dc=com. Confirm that the user has permission to do the following: Search the directory under the subtree specified by the Base DN to: look up specific user, look up specific group, look up groups for given user. Change account passwords.
Bind Password	The bind username account password.
Confirm Bind Password	Confirm the password.
Base DN	The base distinguished name (DN) which is a unique identifier used to limit the search space. For example, to limit the search to the technical sales group, enter OU=tecchnical,DC=sales,DC=com. The search is limited to the technical OU (Group), rather than the whole directory tree. To locate these settings on a Windows Server (2003 and 2008), run the dsquery command, for example: $ dsquery user -name administrator "CN=administrator, CN=Users, DC=sales, DC=com." This lists a DN for administrator. A base DN can be constructed as DC=sales, DC=com. This is field is required for OpenLDAP. For eDirectory, the base DN is entered as o=company. An administrative DN may be cn=administrator, o=company
Use Secure Connections	If the port entered is an SSL port, select this check box.

LDAP has additional settings on the **Advanced Settings** tab. Use the listed default settings, or edit the settings to your needs.

- **Username Attribute**. Specifies the LDAP attribute name that defines the username.
- **Group Attribute**. Specifies the LDAP attribute name that defines a group.
- **Group Entry ID**. Specifies the LDAP attribute on a group that identifies all members belonging to that group.

Table 4-3 Active Directory Settings

Setting	Description
Address	The host name or IP address of the directory server. The VERDE cluster master uses this address to access the server.
Port	The LDAP server listening port. The secure port is recommended. The default SSL port 636. The non-secure port is 389.
Blind Username	The user belonging to this directory that has permissions to view the entire directory (or OU) as specified in the LDAP connector. For Active Directory, this is a name, such as administrator. Confirm the user has permission to do the following: search the directory under the subtree specified by the Base DN to: look up specific user, specific group, and groups for the given user. Change account passwords.
Blind Password	The bind distinguished name (DN) account password.
Confirm Blind Password	Confirm the password.
UPN Suffix	The User Principal Name (UPN) suffix, without the (@) symbol. For Active Directory, enter in format dictated by the directory structure, such as sales.-com.
Base DN	The base distinguished name (DN) which is a unique identifier used to limit the search space. For example, to limit the search to the technical sales group, enter OU=technical,DC=sales,DC=com. The search is limited to the technical OU (Group), rather than the whole directory tree. To locate these settings on a Windows Server (2003 and 2008), run the dsquery command, for example: $ dsquery user -name administrator "CN=a-administrator,CN=Users,DC=sales,DC=com" This lists a DN for administrator. A base DN can be constructed as DC=sales, DC=com. This is field is optional for Active Directory.
NT4 Domain Name	Windows NT 4.0-style domains do not support DNS naming, and require a unique (for that network) NetBIOS name assigned for the domain. If the domain intends to support clients for Windows NT 4.0-style domains, enter a NetBIOS name.
Use Secure Connections	If the port entered is an SSL port, select this check box.

Gold Images Overview

After you've adjusted user, role, and group information, you're ready to navigate to the Gold Images screen and begin adding and managing Gold Images. Because this step is more involved the others—and will vary depending on the type of Gold Image you're wishing to install—we've dedicated three separate sections for addressing the various tasks required for maintaining Gold Images.

If you would like to take a detour from the VERDE Management Console chapter to learn more about Gold Images, browse the list below and navigate to the topic that best fits the information you're interested in:

- Installing a Gold Image Virtual Machine. See Installing a Gold Image Virtual Machine on p. 80 for more details.
- Creating a New Gold Image. See Gold Images on p. 83 for more details.
- Editing a Gold Image. See Making Changes to a Gold Image on p. 102 for more details.
- Upgrading and Importing a Gold Image. See Upgrading and Importing Gold Images on p. 108 for more details.
- Upgrading Gold Image Guest Drivers. See Upgrading Gold Image Guest Drivers on p. 106 for more details.
- Provisioning a Gold Image Virtual Machine. See Provisioning a Gold Image Virtual Machine on p. 129 for more details.
- Configuring the Gold Image. See Configuring the Gold Image on p. 109 for more details.

Managing Session Settings

Session settings manage the environment for virtual sessions in terms of system resources, networking, access to peripherals, disconnected mode, and USB support. Settings can be assigned to a Gold Image as the default environment for that image, or they can be used to customize the environment for a specific rule in the **Desktop Policies** screen.

Some important factors to consider:

- The RAM and Max Size User Image must be exactly the same in both the session settings used to create the Gold Image and in the session settings applied to deploy the Gold Image to a user or group (**Desktop Policy** screen). If these values are different, there may be problems the first time a user tries to log in to a guest session.
- Session settings specified on the **Desktop Policy** screen override **Gold Images** screen settings, and each of them overrides the Default settings.
- The Default session settings object contains default settings for a dynamic session. Other session settings inherit the values from the default, unless overridden. If a default setting is changed, the setting is reflected in all other session settings, unless specifically overwritten.

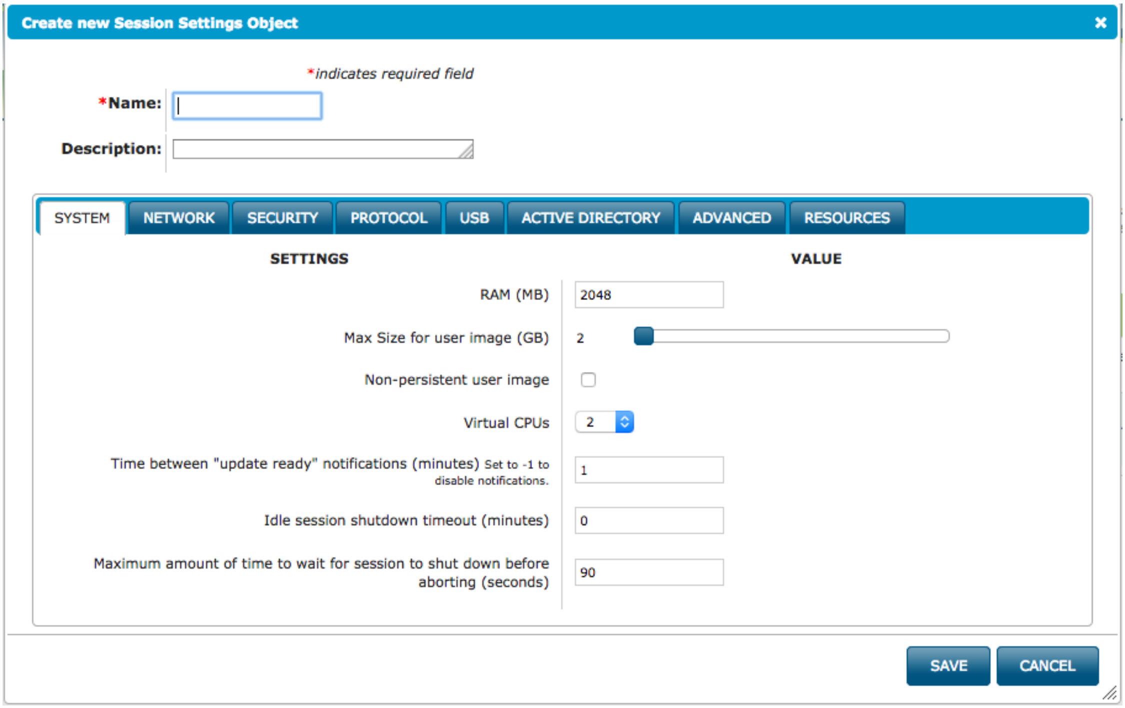
SYSTEM SESSION SETTINGS

System session settings define the user’s guest session experience once applied to a Gold Image.

Set or change the following values:

- ✓ **RAM (MB)**. The amount of RAM allocated to the guest session is in 4 MB increments. The guest default is 2028 MB.
- ✓ **Maximum Size for user image (MB)**. The maximum guest virtual D: drive (user data) volume size, in GB. The maximum value is 256 GB. The default is 2 GB. **Note:** For Linux guests, the maximum user image size is 16384 MB (16 GB).
- ✓ **Non-persistent user image**. By default, user images persist. To delete user images after each session, check the box.
- ✓ **Virtual CPUs**. The number of virtual CPU’s available for a guest operating system. Valid values are 1, 2, 4, 8, 12, and 16. Important: Windows Gold Images need to be installed or updated with the necessary drivers to support multiple virtual CPUs. Assign the highest number of CPUs to the Gold Image, check it out, let Windows install the correct drivers, restart the image, and check it back into the VERDE Management Console. See Upgrading Gold Image Guest Drivers on p. 106 for more details. Additionally, Ubuntu Gold Images should not be assigned to more than one virtual CPU during a Gold Image installation. Multiple CPUs cause file copy and reboot issues.

- ✓ **Idle session shutdown timeout (minutes)**. The amount of time allowed for a session to be disconnected before it is shutdown.
- ✓ **Maximum amount of time to wait for session to shut down before aborting (seconds)**. The amount of time allowed for a session to attempt to shutdown before it is aborted.



Create new Session Settings Object

*indicates required field

*Name:

Description:

SETTINGS	VALUE
RAM (MB)	2048
Max Size for user image (GB)	2
Non-persistent user image	□
Virtual CPUs	2
Time between "update ready" notifications (minutes) Set to -1 to disable notifications.	1
Idle session shutdown timeout (minutes)	0
Maximum amount of time to wait for session to shut down before aborting (seconds)	90

NETWORK SESSION SETTINGS

Network settings define the networking type for a guest session. NAT networking is the default setting.

Note: Changes to Network Settings previously applied to Gold Images will not take effect until the image is shut down and restarted. See Installing a Gold Image Virtual Machine on p. 80 for more details.

Set or change the following values:

- **Network Type**. The type of networking to present to the virtual machine environment. Choices are NAT or Bridged.

  If Open vSwitch networking is configured, choose Bridged.

  Note: The Gold Image must be started at least one time with NAT networking configured. Following this process ensures the necessary drivers were installed and configured successfully, before being inherited by the guest session.

- **Bridge Interface**. The host network device to which the virtual machine is bridged (for example, `NETWORK0`). If multiple networks are defined, this field becomes a drop-down list. The host networking adapter in General Settings must also be configured to allow bridging.
- **VLAN**. If VLAN networking is configured, enter the VLAN tag to use for guest sessions.
- **MAC Address Pool**. If the session will use a pool of MAC addresses, select a pool from the list.
- **Return MAC addresses to pool when sessions end**. To return a MAC address to the pool when a guest session ends, select this option.
- **Limit Virtual Network Bandwidth**. Limits the upstream traffic from the virtual desktop to the network on which it is bridged. Downstream traffic must be limited at the switch or firewall. This prevents individual users from consuming large amounts of upstream traffic on the switch, such as uploading or streaming from the virtual desktop.

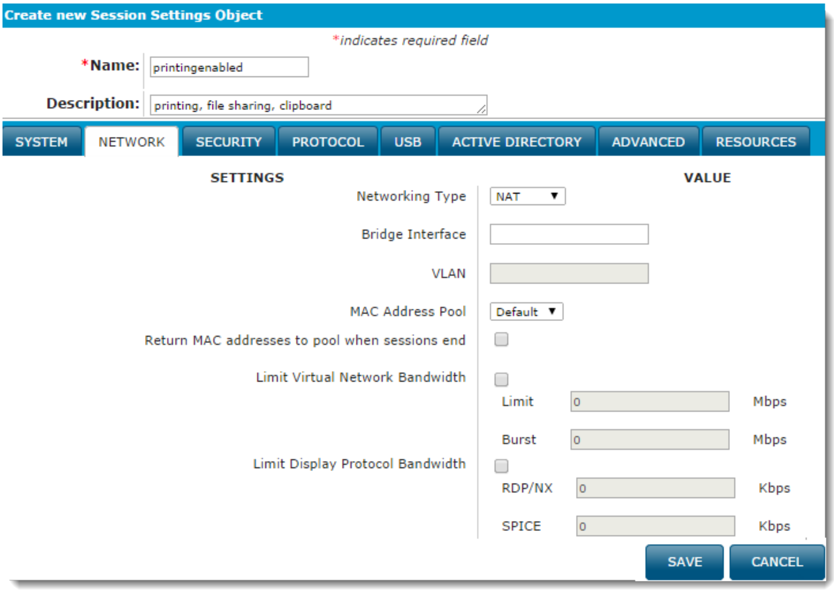
  A burst rate can be set to expand the resource limit if needed. For example, if the interface that the session is using has spare capacity, the session bandwidth would be allowed to expand to a specific maximum rate that is higher than the set limit.

  Note: No single socket for any protocol will exceed the bandwidth assigned in Network Session Settings.

- **Limit Display Protocol Bandwidth**. VERDE limits the traffic in the direction of the virtual desktop to the client. Graphics coming from the virtual desktop are affected by this limit. Data flowing upstream (from the client to the virtual desktop) is not limited by VERDE.

- For RDP, this also includes USB traffic. RDP uses only one socket for all traffic.
- For SPICE, there are multiple sockets for the audio and graphics, plus the USB device socket (s), one per device. Generally, SPICE traffic only flows on one to two sockets at a given time. However, with multimedia, the limit will most likely be exceeded because several sockets may be transmitting at once.

Note: No single socket for any protocol will exceed the bandwidth assigned in Network Session Settings.



Create new Session Settings Object

*indicates required field

*Name: printingenabled

Description: printing, file sharing, clipboard

SETTINGS	VALUE
Networking Type	NAT ▼
Bridge Interface	
VLAN	
MAC Address Pool	Default ▼
Return MAC addresses to pool when sessions end	□
Limit Virtual Network Bandwidth	□ Limit 0 Mbps Burst 0 Mbps
Limit Display Protocol Bandwidth	□ RDP/NX 0 Kbps SPICE 0 Kbps

SECURITY SESSION SETTINGS

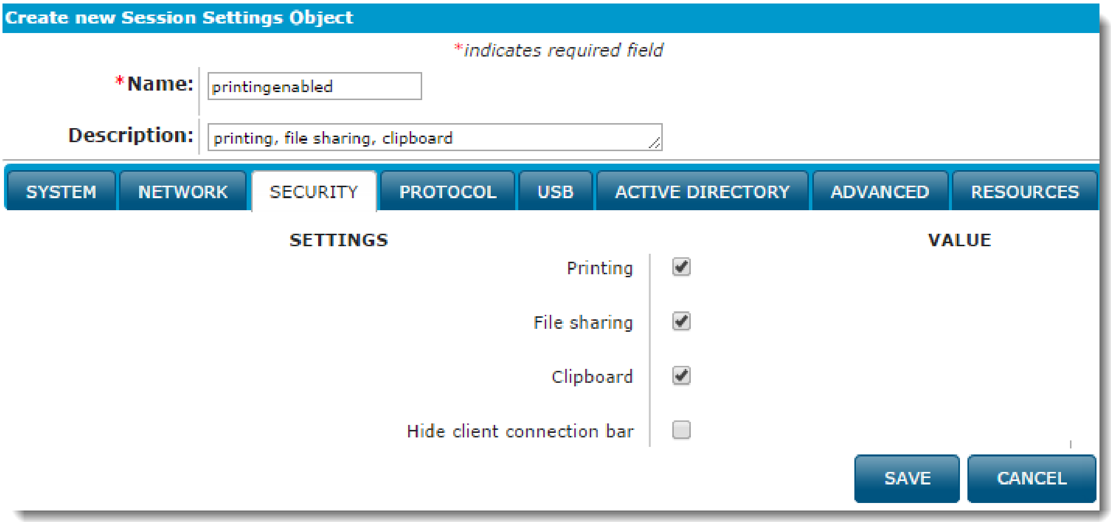
Security settings define the guest session’s printing, file sharing, and the clipboard for SPICE and RDP protocols.

The following options are available.

- **Printing**. This enables printing to a default host or client printer from a virtual machine.

  Note: If not enabled, a Save As dialog is displayed to the user instead of Print. The user can save the document to a file, but cannot print it.

- **File Sharing**. This parameter defines shared folders on the host only. VDI clients can access local folders if those folders are shared on the client.
- **Clipboard**. Allow cut/copy and paste between guest and host applications, or between guest and client applications.



Create new Session Settings Object

*indicates required field

*Name: printingenabled

Description: printing, file sharing, clipboard

SETTINGS	VALUE
Printing	☑
File sharing	☑
Clipboard	☑
Hide client connection bar	☐

PROTOCOL SESSION SETTINGS

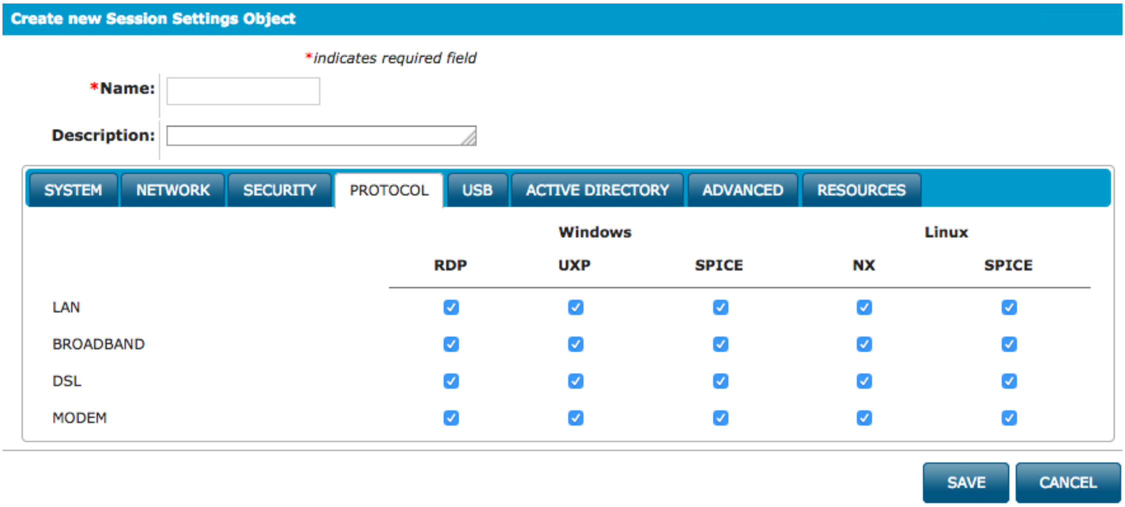
Protocol settings specify which network protocols are available for the user accessing the desktop session. Depending on the end user's location and system/infrastructure, protocols may be restricted for performance reasons. Each connection requires RDP and/or SPICE for Windows sessions, and SPICE for Linux sessions. These settings determine the choices available to a user from the VERDE User Console. If only SPICE options are selected, the VERDE User Console will not display a protocol choice.

Important: SPICE requires more resources to manage high definition video and may not be appropriate for all networks.

The different available connections include:

- **LAN**. Uses a LAN connection for client sessions.
- **Broadband**. Uses a broadband connection for client sessions.
- **DSL**. Uses a DSL connection for client sessions.
- **Modem**. Uses a modem connection for client sessions.

Important: Confirm the client machine and Gold Image are configured to support the selected protocol.



Create new Session Settings Object

**indicates required field*

***Name:**

Description:

	Windows			Linux	
	RDP	UXP	SPICE	NX	SPICE
LAN	☑	☑	☑	☑	☑
BROADBAND	☑	☑	☑	☑	☑
DSL	☑	☑	☑	☑	☑
MODEM	☑	☑	☑	☑	☑

USB SESSION SETTINGS

USB settings enable the guest operating system to access the USB devices that are plugged into the client. You can choose to support all devices except human interface devices (HID), or you can specify certain ones.

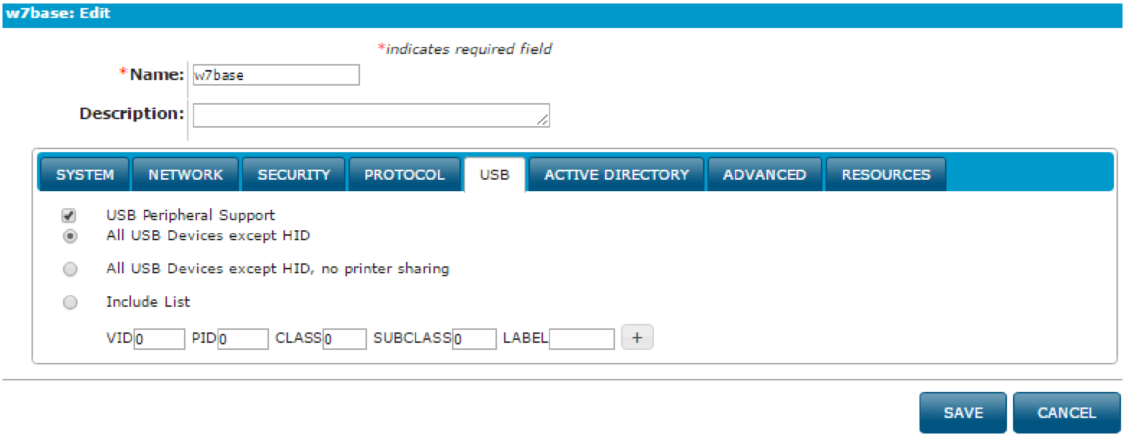
Note: Either the client or the guest can control these USB devices, but not both. However, human interface devices (HID) such as a mouse and keyboard are controlled by the client and are available for use by both the client and the guest virtual machine.

To enable composite USB devices:

1. List device in the "include" list by its USB device class code, including the vendor ID and product ID.
2. Select "Add **+**" to add entries to the list.

   Note: For information about USB device class codes, visit the USB developer **site**.

3. Enter an optional name in the "Label" field. The following options are available.
   - **USB Peripheral Support**. Allows all USB devices to connect to the client through the guest session.
   - **All USB Devices except HID**. Allows all USB devices to connect to the client through the guest session (except a human interface device).
   - **Include List. Allows specified USB devices**. To specify individual devices and all other non-HID devices, add a final row with values of 0000.



w7base: Edit

*indicates required field

*Name: w7base

Description:

☑ USB Peripheral Support

● All USB Devices except HID

○ All USB Devices except HID, no printer sharing

○ Include List

VID 0 PID 0 CLASS 0 SUBCLASS 0 LABEL

ACTIVE DIRECTORY SESSION SETTINGS

Define session settings for guest sessions to authenticate with the Active Directory domain. Configure the settings listed in the table below.

Table 4-4 Active Directory Settings

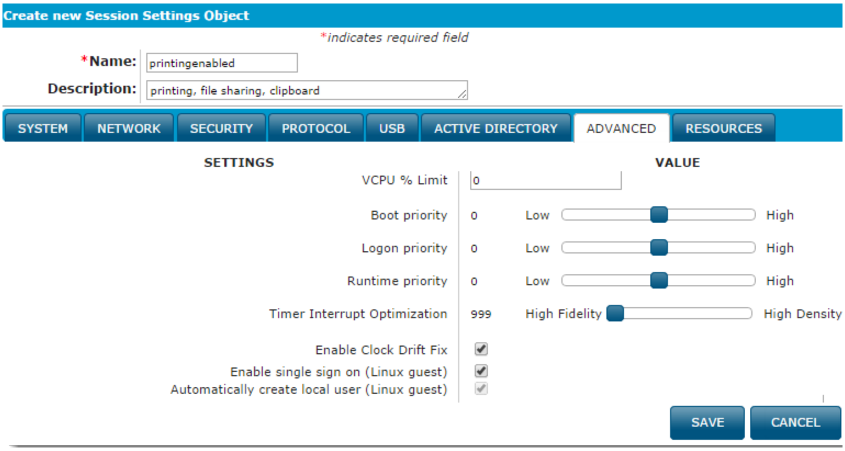
Active Directory Setting	Description
Desktop Name Prefix	Active Directory requires a computer name to access the domain. Guest sessions will access the domain with this name. The name is the prefix plus a sequence number assigned by the system.
AD Domain Name	The fully qualified name of the Active Directory domain.
Optional: AD Organizational Unit	To limit the directory search to a specific organizational unit, enter the OU. This prevents a search through the entire directory tree. If there are multiple or nested organizational units, confirm they are listed in order of inner unit to outer. For example, a single layer would be listed as: `OU=test, DC=example, DC=com`. A nested unit software inside the top unit test, would be listed as: `OU=software,OU=test,DC=example,DC=com`
AD Administrator User Name	Enter the fully qualified Active Directory administrator user name. For example: *username@domain.example.com*
AD Administrator Password and Confirm Password	Enter and confirm the administrative account password.

ADVANCED SETTINGS

Sessions can be put into priority groups where CPU, login, and runtime can be governed. For example, system priority can be given to users who need more resources during login than during the actual running of a session. Confirm overall use and system planning information is defined before adjusting these settings.

Setting	Description
VCPU % Limit	Sets the maximum percentage of CPU that a session can consume. Values are per virtual CPU. For example, if a guest has one virtual CPU, a 30% value would mean that it never uses more than 30% of a single host CPU thread. If the guest has two virtual CPUs, 30% means 60% of host. A value of 0 is unlimited.
Boot priority	Sets the session priority from early boot to the start of the guest service agent.
Logon priority	Sets the session priority from the start of the guest service agent to start of the guest user agent.
Runtime Priority	Sets the session priority from start of the guest user agent and continues while the session is connected.
Timer Interrupt Optimization	Sets the rate at which interrupts can occur within a session. This setting is used for sessions that need resources for multi-media use.
Enable Clock Drift Fix	The virtual machine synchronizes with the server every 8 seconds. Enable this for more frequent synchronization.
Automatically create local user	Creates a local VERDE account for a user that logs into the VERDE User Console or VERDE Client to launch a Linux session.
Enable single sign on (Linux guest)	Leave this setting checked on.

See example screenshot on next page.



Create new Session Settings Object

*indicates required field

*Name: printingenabled

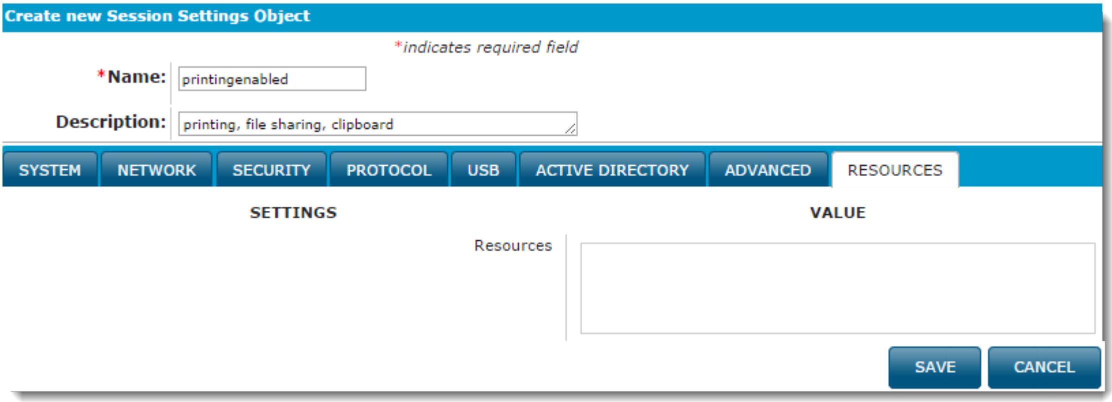
Description: printing, file sharing, clipboard

SETTINGS	VALUE
VCPU % Limit	0
Boot priority	0 Low High
Logon priority	0 Low High
Runtime priority	0 Low High
Timer Interrupt Optimization	999 High Fidelity High Density
Enable Clock Drift Fix	☑
Enable single sign on (Linux guest)	☑
Automatically create local user (Linux guest)	☑

RESOURCE SETTINGS

Assign resource tags to sessions to confirm that those sessions run on a particular server. They are simply identification tags that enable resource assignment in a clustered environment. Resource tags are created under General Settings, associated with servers in Computer Resources, and assigned to guest sessions through Session Settings. Perform the following to assign resource tags to sessions:

On the **Resources** tab, select one or more resources.



Create new Session Settings Object

*indicates required field

*Name: printingenabled

Description: printing, file sharing, clipboard

SETTINGS	VALUE
Resources	

VERDE Virtual Application Layers

Virtualized application layers provide application distribution to end users with Gold Images. Each image contains the basic application requirements of the organization. Specific applications can be deployed to each group of users.

Application layers have the following characteristics:

- The application layers are compatible with Windows applications.
- The application layers work for all Windows User Mode applications except for "Kernel mode applications" that require device drivers.
- Application layers are published to the end users or groups using the provisioning rules from the VERDE Management Console.
- The end user sees one composite desktop which includes the Gold Image and the blended application layers.
- Applications are updated the same way Gold Images are updated.

VERDE provides a differential update mechanism for the application layers in disconnected mode, such as in a Cloud Branch location. When an application layer is updated, users have an option to reload the new application layer without having to restart the session.

APPLICATION LAYER WORKFLOW

Build the application package on a workstation or virtual machine using a third-party tool application package building tool such as ThinApp, SPOON, ZENworks, Cameyo, or InstallFree.

1. Upload the application package to the VERDE Server from the VERDE Management Console.
2. Publish the application.
3. Deploy the application to users.

Note: Currently, only `.exe` and `.msi` file types with less than 2 GB each can be installed. The `.DAT` file format is not supported.

UPLOADING THE VIRTUAL APPLICATION

After the virtual application package has been build, upload and import it in the VERDE Management Console.

1. On the **Application Layer** screen, select "CREATE NEW" in the upper right corner. The **Import Application Layer** dialog will open.
2. Enter the application name, Revision Tag, and select the target operating system(s). Application names are case sensitive.
3. Select "Upload."
4. The **Upload** dialogue window will open. Browse for the file you wish to upload. The file must have a.msi or .exe extension. Choose the correct file and select "Open."
5. When the upload is complete, select "Import." The new application will now be listed in the **Application Layer** screen.
6. Select "STAGE ." The application will be in an intermediate/temporary status that can be used during a test phase.
7. Select "PUBLISH" to make the application available for deployment.

DEPLOYING VIRTUAL APPLICATIONS

The new application package has been imported to the VERDE Server and is ready to be deployed to users and groups. Open the **Desktop Policy** screen, and perform one of the following tasks:

- Add a new rule.
- Edit an existing rule.
- Add an Image to an existing rule.

The **Desktop Policy** dialog displays the **Application Layer** tab.

1. In the **Application Layer** tab, select the application to deploy or use the search option to find an application. The applications listed in the Search Results depend on the OS of the Gold Image selected search parameters (name and/or revision tag).
2. In **Search Results**, select the application to be deployed.
3. Select the deployment type:
   - **Latest**. Applies the latest version of the application.
   - **Staging**. Uses the application for testing purposes.
   - **Version**. Enables selection of a specific version of the application.
4. Select "UPDATE."

INSTALLING THE VIRTUAL APPLICATION IN THE GUEST

The application package can be installed inside the guest image when a user launches a session. Depending on how the application package was generated, the application may install automatically, or may be available in `\\host\apps`, and is installed by the VERDE user.

If application packages were created with VMWare's ThinApp, the `ThinReg.exe` must be installed in the Gold Image to `ProgramFiles\VMWare\VMWare ThinApp\ThinReg.exe`. The ThinApp application requires this to install the application package in the Gold Image.

Application packages created with Cameyo require no additional licensing or installation inside the Gold Image. The `.exe` file is available in the `\\host\apps` local, non-persistent drive.

Organization Overview

Organizations offer the ability to assign resources from a single infrastructure to physical or departmental locations, while providing the granularity required to manage each organization separately. Organizations provide management benefits for:

- **Departmentalized IT services in a single enterprise**. Different organizations (Marketing, Engineering, Sales), geographies, and business units may have their own set of users and requirements. IT services can create organizations based on functional or geographical business requirements.
- **Managed service providers (MSPs) with multiple customers and solution sets**. For security, manageability, and licensing reasons, customer deployments must be managed separately. Separate administration, separate physical VDI servers, and separate logical networks can be managed and maintained with organizations. Services can be offered as:
  - **Private Desktop Cloud**. Servers are assigned to organizations and each organization can manage its own desktops and policies through delegated administration functions.
  - **Desktop as a Service (Public or Private Cloud)**. Service provider provisions desktops directly to organizations and performs all management on their behalf, while organizations get personalized SLAs and VERDE User Console portal.

Managed service providers should understand the licensing restrictions of each Windows operating system offered. Certain license types are required for service providers and virtual desktops depending on how infrastructure resources are assigned. See the Microsoft **site** for details.

ORGANIZATION MANAGEMENT

Organizations can be managed in several ways, but some general rules apply:

- Each organization manages its own set of Gold Images and Application Layers. For MSPs, the organizational administrator can be part of the MSP staff, or the customer's IT staff, depending on the service model.
- Each organization must be assigned to one or more servers to run guest sessions, including the global (first created after installation) organization.
- The creator of an organization automatically becomes the first administrator for that organization, with a master administrator role for that organization. Additional administrators can be defined for the organization. An administrator can be limited to manage one or more organizations.
- A Management Console Master Administrator can manage all settings in all organizations, including defining new organizations and delegating administrative privileges to manage organizations.
- Each organization has full control over the assignment of Gold Images to users.
- Each organization controls Session Settings relevant to its users' sessions.

- An organizational administrator can create an image by cloning a Gold Image that was created at the global level in the VERDE Management Console.
- An organizational administrator can provision Gold Images, Application Layers, and Session Settings all created at the global level to end users.

Note: All organizations, including the global organization, must have server resources assigned before running desktop sessions.

USER SEPARATION

User separation is achieved by defining different authentication realms (LDAP directories) for different organizations. To achieve the same for users belonging to different units within the same organization, VERDE enables the administrator to specify multiple authentication providers (LDAP connectors) to the same directory but differentiated by the Base DNs.

Note: Local users cannot be created within a tenant organization. New users must be LDAP users.

NETWORK SEPARATION

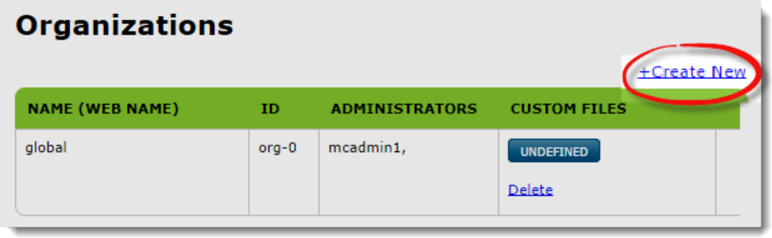
Organizations rely on the resources in a single enterprise. To ensure the security of organizational access and user data, networks and resources can be defined and allocated in the following ways:

- Network separation can be achieved through VLANs, or each server can have its own network configuration where networks on the host are on different physical topologies.
- Resource separation is achieved through the ability to designate different servers for different organizations.

CREATE NEW ORGANIZATION

Perform the following steps to create an organization:

1. From the **Organizations** screen, select "CREATE NEW."



Organizations

NAME (WEB NAME)	ID	ADMINISTRATORS	CUSTOM FILES
global	org-0	mcadmin1,	UNDEFINED Delete

2. The **Create New Organization** window will open. Enter a unique name for this organization. Names are case sensitive.
3. Assign a URL for users in this organization to access the VERDE User Console.
4. Select a MAC Address Pool.
5. Enter information in each tab:
   - **Administrators**. Search for and select the administrators to manage tasks within this organization.
   - **Resource Allocation**. Select the network type and interfaces that this organization will use. If VLAN tags are configured, enter a range that this organization can use. These settings define limitations or constraints on what will appear in Session Settings for this organization.
   - **Resource Limitations**. Specify the amount of memory, user image size (maximum is 256 GB), and CPUs each session is allocated in this organization. These settings define limitations or constraints on what will appear in Session Settings for this organization.
   - **License Utilization**. Specify the number of concurrent sessions allowed for this organization. This will be a subset of the total licenses entered in General Settings.
   - **Branch**. If this organization is a branch location, enable this deployment mode.
   - **Global View**. To allow this organization to have a global view of the VERDE Management Console and other organizations, enable global objects.

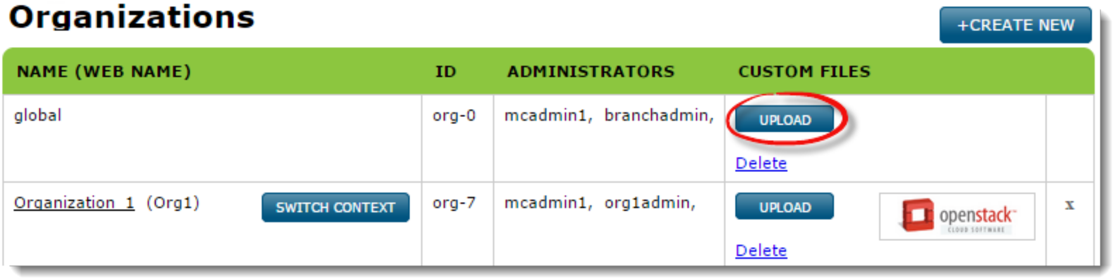
DELETING AN ORGANIZATION

Organizations must be deleted manually. If there is a possibility that the organization needs to be recreated with the same name, it will have a different identifier in the system. See the **VERDE Troubleshooting Guide** for details about deleting organization files from shared storage.

UPLOAD AN ORGANIZATION'S LOGO

A logo can be added for each organization that will replace the NComputing Global, Inc. logo in the VERDE Management Console interface and on the VERDE User Console **Login** screen. The file should be in .png format and 120 x 39 pixels in size.

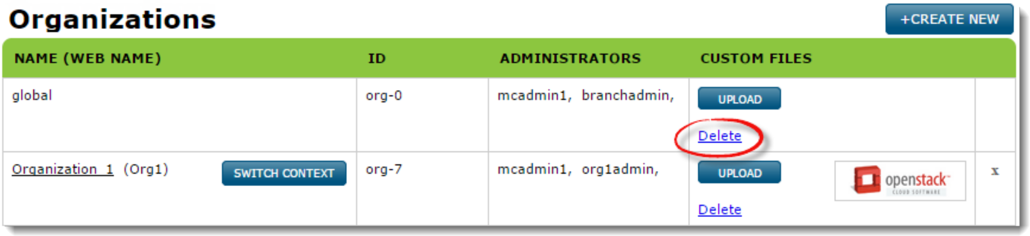
On the **Organizations** screen, select "UPLOAD" beside an Organization on the list. Locate and upload the logo file. After the file is uploaded, it will appear on the screen; however, you'll need to navigate away from the screen in order for the image to appear as the new logo.



NAME (WEB NAME)	ID	ADMINISTRATORS	CUSTOM FILES	
global	org-0	mcadmin1, branchadmin,	UPLOAD Delete	
Organization 1 (Org1) SWITCH CONTEXT	org-7	mcadmin1, org1admin,	UPLOAD Delete openstack CLOUD SOFTWARE	x

DELETING AN ORGANIZATION FILE

1. On the **Organizations** screen, select "Delete" under the "Custom Files" column in that organization's row.

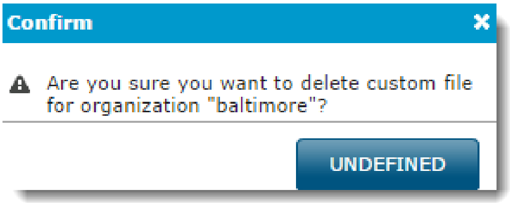


Organizations

+CREATE NEW

NAME (WEB NAME)	ID	ADMINISTRATORS	CUSTOM FILES		
global	org-0	mcadmin1, branchadmin,	UPLOAD Delete		
Organization 1 (Org1) SWITCH CONTEXT	org-7	mcadmin1, org1admin,	UPLOAD Delete	openstack	x

2. A confirmation message will display. Select "Undefined" to continue with the deletion of the file.



Confirm

Are you sure you want to delete custom file for organization "baltimore"?

Assign MAC Address Pools

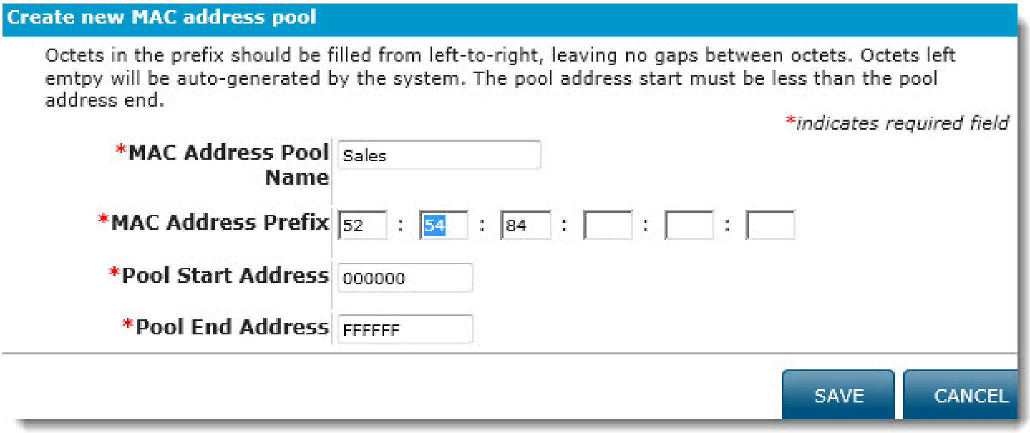
Highly secure environments may require a defined set of MAC addresses to enable virtual sessions to access the network. When a MAC address pool is assigned through Session Settings, unused MAC addresses can be returned to the pool when a guest session ends.

Note: VERDE uses the Default pool for all images. Any changes to the Default settings will be inherited by all images.

If MAC address pools conflict with other addresses on the network, VERDE will not detect conflicts.

The use of a MAC Address can be revoked through the Reporting screens. See User Session Reporting on p. 154 for more details.

1. On the **MAC Address Pools** screen, select "CREATE NEW." Enter settings for this pool.



Create new MAC address pool

Octets in the prefix should be filled from left-to-right, leaving no gaps between octets. Octets left emtpy will be auto-generated by the system. The pool address start must be less than the pool address end.

*indicates required field

***MAC Address Pool Name**	Sales
***MAC Address Prefix**	52 : 54 : 84 : : :
***Pool Start Address**	000000
***Pool End Address**	FFFFFF

2. Enter a name for this pool. Keep in mind that names are case sensitive.
3. Set a prefix for the range of addresses in the "MAC Address Prefix" fields, if desired. The prefix helps ensure uniqueness in a cluster. Enter values for one or more octets from left to right. The fields that are left empty are populated by the range defined in the start and end fields.
4. Enter the range for the MAC address pool in the "Pool Start Address" and "Pool End Address" fields. If a prefix is defined, enter the remaining octet values in these fields. Confirm that the start value is less than the end value.
5. Select "Save." The pool is assigned through Network Session Settings.See Managing Session Settings on p. 51 for more details.

Managing Desktop Pools

Desktop pools are anonymous non-persistent virtual machines that are assigned desktop policies and users. They are a great way to maintain guest sessions that need to be readily available at all time. They are assigned to users who need consistent access to a set of non-persistent desktop sessions that are up and running.

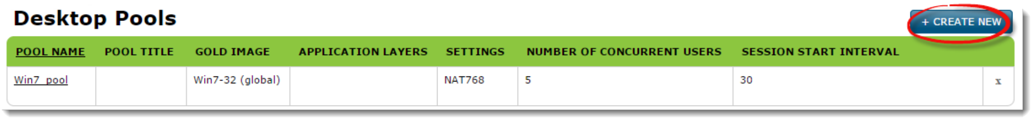
Important: Due to the non-persistent state of the desktop pools, native profile management will not work in this case. Use a profile management tool such as Windows Roaming Profiles to enable any type of user persistency.

Confirm network resources can manage the number of created pools and sessions. Start with a smaller pool and add sessions as needed. If there are not enough resources to run desktop pool sessions, the desktop pool will not start.

- If a user disconnects or logs out of a session and reconnects within five minutes, the user is reconnected to the original session.
- If a user disconnects for more than five minutes, the session is terminated. When the user logs in again, a new session is created.
- To temporarily disable the desktop pools, set the concurrent users to zero.

CREATING A NEW DESKTOP POOL

1. On the **Desktop Pools** screen, select "Create New."

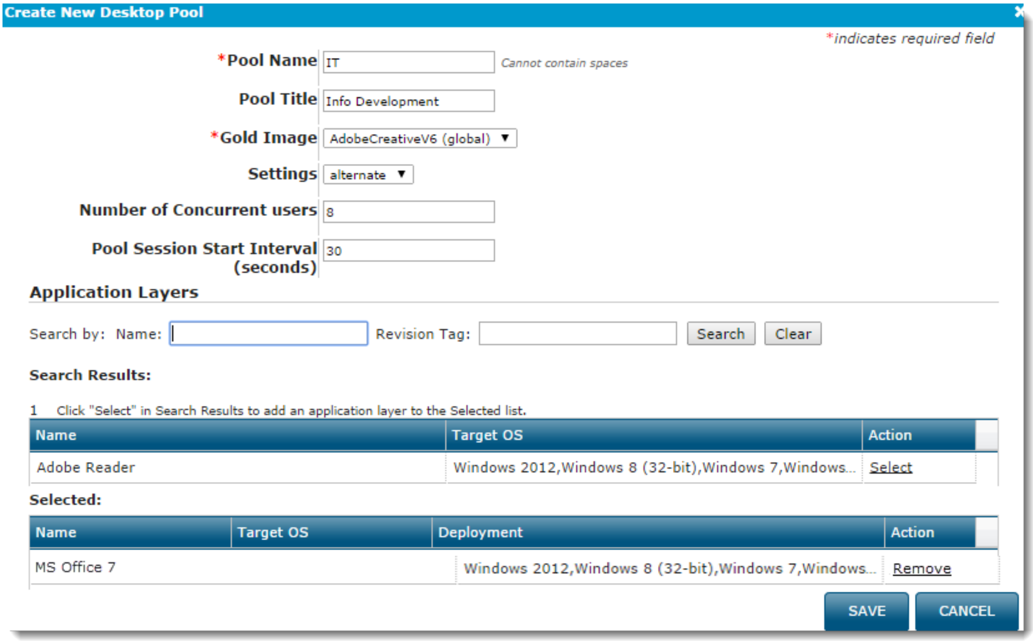


Desktop Pools

POOL NAME	POOL TITLE	GOLD IMAGE	APPLICATION LAYERS	SETTINGS	NUMBER OF CONCURRENT USERS	SESSION START INTERVAL	
Win7_pool		Win7-32 (global)		NAT768	5	30	x

2. Define the following settings:
    - **Pool Name**. Alphanumeric desktop pool name. This name cannot contain spaces.
    - **Pool Title**. Short description for the desktop pool.
    - **Gold Image**. The Gold Image that will launch the desktop pool sessions.
    - **Settings**. The Session Settings to assign to these guest sessions.
    - **Number of Concurrent Users**. The number of users that can run sessions at the same time. The number must be supported by the environment and resources available.
    - **Pool Session Start Interval**. The delay time in seconds that each session in the pool can start. If a pool is assigned to a group of users that typically start their sessions at the same time, this prevents a boot storm from occurring.

3. Search for and select any Application Layers. (For more information about Application Layers, see VERDE Virtual Application Layers on pg. 61.)
4. Select "Save" to save the new desktop pool.



Create New Desktop Pool

*indicates required field

*Pool Name: IT — Cannot contain spaces

Pool Title: Info Development

*Gold Image: AdobeCreativeV6 (global) ▼

Settings: alternate ▼

Number of Concurrent users: 8

Pool Session Start Interval (seconds): 30

Application Layers

Search by: Name: Revision Tag:

Search Results:

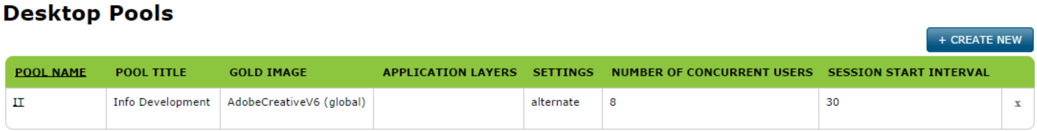
1 Click "Select" in Search Results to add an application layer to the Selected list.

Name	Target OS	Action
Adobe Reader	Windows 2012,Windows 8 (32-bit),Windows 7,Windows...	Select

Selected:

Name	Target OS	Deployment	Action
MS Office 7		Windows 2012,Windows 8 (32-bit),Windows 7,Windows...	Remove

5. The new pool will now be available on the **Desktop Pool** screen once it has been assigned to a desktop policy. Assign a pool through a rule in Policies. See Managing Desktop Policy on p. 72 for more details.



Desktop Pools

POOL NAME	POOL TITLE	GOLD IMAGE	APPLICATION LAYERS	SETTINGS	NUMBER OF CONCURRENT USERS	SESSION START INTERVAL	
IT	Info Development	AdobeCreativeV6 (global)		alternate	8	30	x

Managing Desktop Policy

Under the **Configuration** tab, select "Desktop Policy" to manage the policies that determine the users, groups, applications, and deployment specifics that are associated with a Gold Image.

- Rules are listed in the order they were created.
- To change the order in which rules are processed, change the number to the left of the rule.
- To edit the list of users and groups for a rule, select the link in the "USER/GROUP" column.
- List entries are separated by commas.
- Group names are preceded by "%."

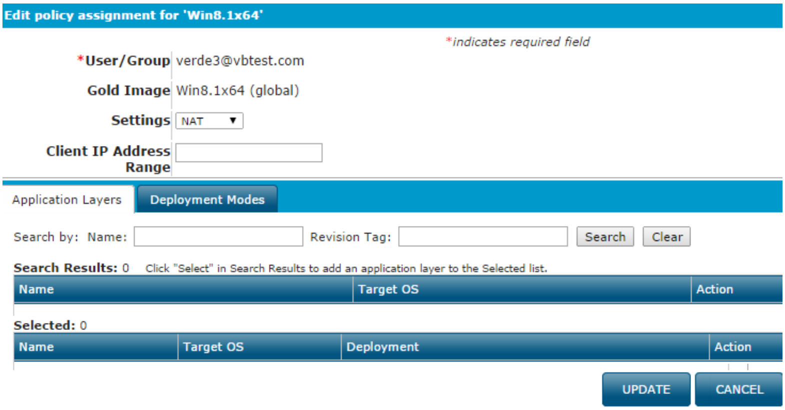
CREATING A RULE FOR A GOLD IMAGE

If assigning the rule to a Gold Image, the following information is defined:

- **Application Layers**.Used to deploy virtual applications. See VERDE Virtual Application Layers on p. 61 for more details.
- **Deployment Modes**. Defines the deployment modes and the desktop type for the specified Desktop Policy. The preferred deployment type is "Dynamic" with "Normal Session Lifetime." See Deployment Mode, Type, and Active Directory on p. 132 for more details..

To create a new rule, follow the steps listed below:

1. If created, select a "Gold Image" from the drop-down list. Rules can be created and later assigned to a Gold Image. This creates a Skip rule for the specified user or group. The rule is listed with **Stop Matching**, which keeps the policy from matching items beyond that point. For example, create a skip rule to stop the provisioning of desktops to a user or group.
2. Select a session setting from the "Settings" drop-down list. Default is the only setting available after installation. Additional settings can be created. The Default setting is used if no option is chosen.
3. If it is necessary to restrict access to the Gold Image based on client location or IP address, define a range of addresses in the "Client Address Range" field. The format should be `aa.bb.cc.dd/n` where "n" is a number between 32 and 1. For example, `170.17.0.0/16`. See screenshot on next page.



Edit policy assignment for 'Win8.1x64'

*indicates required field

*User/Group	verde3@vbtest.com
Gold Image	Win8.1x64 (global)
Settings	NAT ▾
Client IP Address Range	

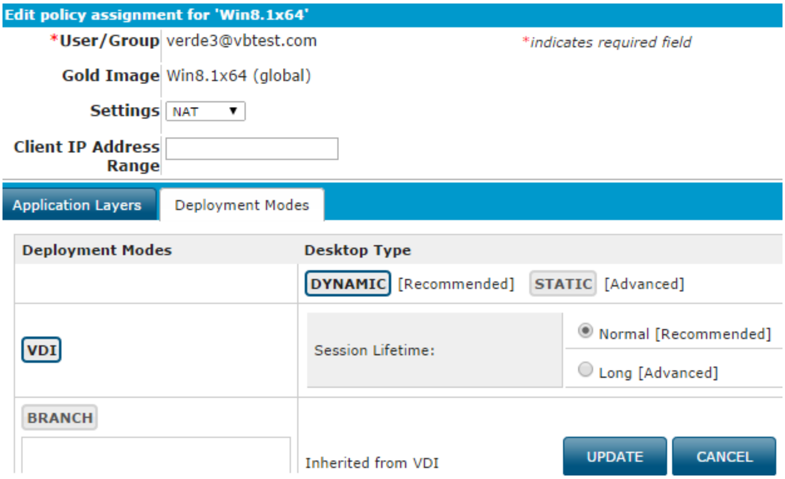
Search Results: 0 Click "Select" in Search Results to add an application layer to the Selected list.

Name	Target OS	Action

Selected: 0

Name	Target OS	Deployment	Action

4. Select **Deployment Modes** to assign modes to this user or group for the selected Gold Image.



Edit policy assignment for 'Win8.1x64'

*indicates required field

*User/Group	verde3@vbtest.com
Gold Image	Win8.1x64 (global)
Settings	NAT ▾
Client IP Address Range	

Deployment Modes	Desktop Type
	DYNAMIC [Recommended] STATIC [Advanced]
VDI	Session Lifetime: ● Normal [Recommended] ○ Long [Advanced]
BRANCH	Inherited from VDI

5. On the **Deployment Modes** tab, select "VDI" and "Normal."
6. Select the mode or modes for these guest sessions. Refer to the Gold Image Deployment Modes Table on the next page to review the different modes available and their descriptions.
7. Select the "Desktop Type" for the corresponding Deployment Mode. (Each type is described in the dialog. Refer to the Gold Image Deployment Types Table on the next page to review the different types available and their descriptions.) Finally, save the new rule.

Table 4-5 Gold Image Deployment Modes

Deployment Mode	Description
VDI	Deployed from the VDI server.
BRANCH	Deployed and synchronized to the listed branches.

Table 4-6 Gold Image Deployment Types

Deployment Type	Description
Normal	Users receive a fresh copy of the Gold Image each time the session is launched. Changes to the system are lost after every shutdown.
Long	User changes to the Gold Image are preserved until the Gold Image is updated.
Static	User changes to the Gold Image persist after the session shuts down. The user is responsible for all changes to the system areas. Users do not get any Gold Image changes, as with dynamic desktops. Gold Images that are static should not be joined to the Active Directory.

CREATING A RULE FOR A DESKTOP POOL

If assigning the Desktop Policy rule to a Desktop Pool, perform the following steps:

1. Select the Desktop Pool. See Managing Desktop Pools on p. 70 for more details.
2. Select **Enable VDI in Data Center** to have guest sessions run in the data center. If this option is not selected, desktop pools will only run on the selected branch nodes.
3. To apply the desktop pool to a branch server, select one from the **Branch** list.
4. If it is necessary to restrict access to the Gold Image based on client IP address, define an address with a fixed set of bits that should be matched in the "Client Address Range" field. The format should be aa.bb.cc.dd/n where n is a fixed number of bits (between 32 and 1) in the specified address. For example, `170.17.0.0/24`, states that the system should match the first 24 bits of the IP address (170.17.0.x). Any client with an address that matches the first 24 bits will be included in the range.
5. Once the rule is assigned to a desktop pool, the number of sessions defined in the pool (number of concurrent users) is started. This is shown on the **Live Sessions Reporting** screen. See Managing Session Settings on p. 51 for more details. If the Desktop Pool is edited and the number of concurrent sessions is changed, the number of running pool instances will change.

Note: Once assigned to a Branch Server, a Gold Image will obtain a MAC address from the MAC address pool if the image is installed prior to the synchronization interval. The Branch Server must synchronize with the data center to receive the pool assignment.

Adding Multiple Gold Images to a User/Group

Multiple Gold Images and desktop pools can be assigned to a user/group.

1. Select "Add" on the upper right side of the row that corresponds to the User/Group.
2. Select the "Gold Image" Assignment Type.
3. Select the additional image from the **Gold Image** menu.
4. Define any additional settings.

Editing a Desktop Policy Rule

The rules assigned to users and groups can be updated by editing the Desktop Policy.

1. Select the "Edit" link.
2. Make necessary changes.
3. Select "UPDATE."

> **Note:** It is not possible to change the user data space (D: drive) by changing session settings on this screen. Even if a setting rule with a larger space is assigned, it will have no effect. This setting will be taken into account when the session is launched for the first time.

4. If the "Session Settings" field is empty, the session will inherit the session settings of the Gold Image, as defined in the Gold Images screen. See Managing Session Settings on p. 51 for more details.

Removing a Gold Image or Desktop Pool from a User/Group

To remove access to a Gold Image from a user/group:

1. Open the **Desktop Policy** screen.
2. Select "Remove" for the corresponding image.

Removing a Rule

To remove a rule for a user/group:

1. Open the **Desktop Policy** screen.
2. Select the "Delete" icon (right) for the rule.

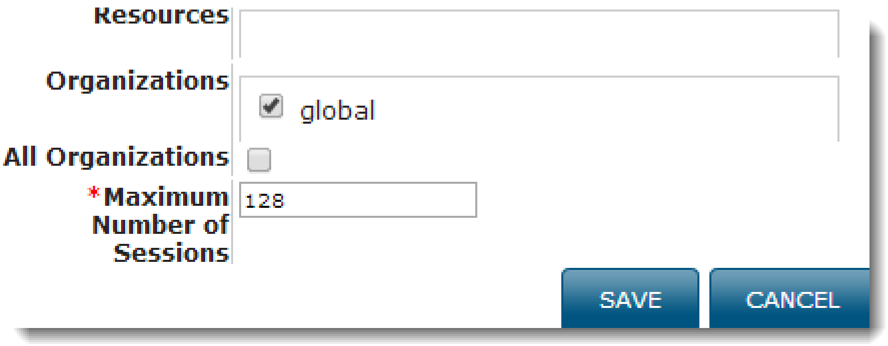
Computer Resources

Resource tags are created under the **Configuration** tab and are associated with servers on the **Server** screen (under the **Administration** tab), and with sessions in **Session Settings**. When a tag is associated with a Session Setting, desktops that use that Session Setting will only run on servers with which the tag is associated. For each server in the cluster, the following can be configured:

- Organizations can be assigned to one or more servers.
- Resource tags associated with this server. Tags are created for each server in General Settings and assigned through Session Settings. When a tag is assigned, sessions will only run on the associated server.
- Maximum number of sessions the server can run.

EDIT A COMPUTER RESOURCE

1. Select "Edit" beside the computer resource that you wish to edit. Type a name for the resource in the field beside "Resource."
2. Next to "Organization," check the organizations that are related to the resource. You can also select the box beside "All Organizations" to make it a universal resource.
3. Beside "Maximum Number of Sessions," type the limit of sessions that can be run at one time using this resource.
4. Select "Save" to save your changes.



Resources

Organizations ☑ global

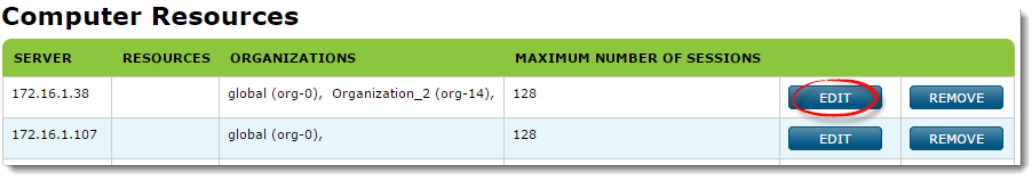
All Organizations □

*Maximum Number of Sessions 128

EDIT SERVER RESOURCES

Resource tags are created under General Settings, associated with servers in Computer Resources, and assigned to guest sessions through Session Settings. To assign organizations to a server, perform the following steps:

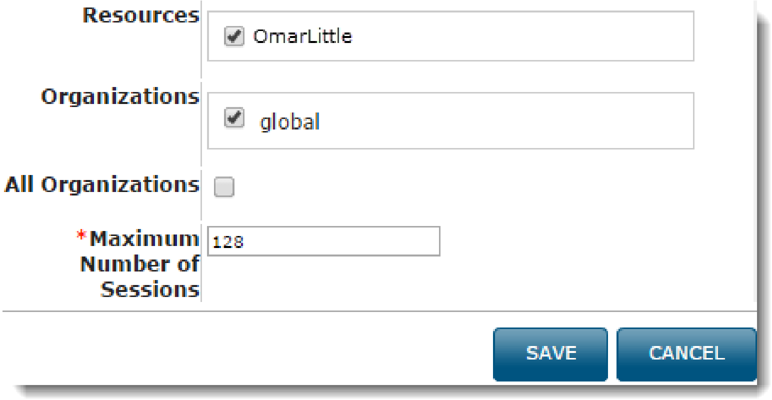
1. On the **Computer Resources** screen, select a server and select "EDIT."



Computer Resources

SERVER	RESOURCES	ORGANIZATIONS	MAXIMUM NUMBER OF SESSIONS		
172.16.1.38		global (org-0), Organization_2 (org-14),	128	EDIT	REMOVE
172.16.1.107		global (org-0),	128	EDIT	REMOVE

2. Select the resource tags to assign to this server.
3. Select the organizations that will use this server.
4. Enter the maximum number of sessions that can run on this server.



Resources	☑ OmarLittle
Organizations	☑ global
All Organizations	☐
*Maximum Number of Sessions	128

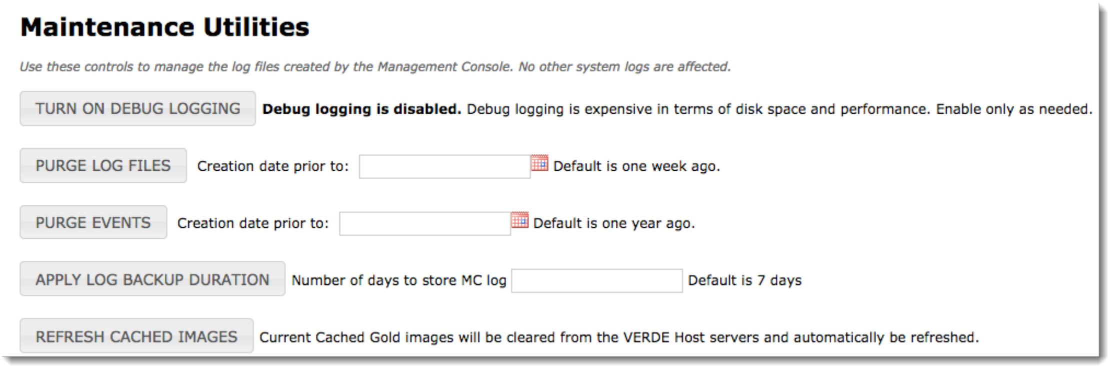
5. Select "Save."

Note: All organizations, including the global organization, must have servers assigned before desktop sessions can be run.

Managing Debug Logs and Events

In the Maintenance section of the VERDE Management Console, the following tasks can be performed:

- Enable or disable logging Debug mode.
- Purge log files for a specified time range.
- Purge system events for a specified time range.
- Apply Log Backup Duration.
- Refresh Cached Images.



Maintenance Utilities

Use these controls to manage the log files created by the Management Console. No other system logs are affected.

TURN ON DEBUG LOGGING **Debug logging is disabled.** Debug logging is expensive in terms of disk space and performance. Enable only as needed.

PURGE LOG FILES Creation date prior to: Default is one week ago.

PURGE EVENTS Creation date prior to: Default is one year ago.

APPLY LOG BACKUP DURATION Number of days to store MC log Default is 7 days

REFRESH CACHED IMAGES Current Cached Gold images will be cleared from the VERDE Host servers and automatically be refreshed.

CHAPTER 5

Installing a Gold Image Virtual Machine

This chapter discusses the following.

Gold Images are operating system images for user desktops. Gold images are created for Windows Server 2008 R2, Windows Server 2012 R2, Windows 7, 8.1, and 10, or Linux from a bootable CD, DVD, or .iso image on a CD or DVD that is accessible to the VERDE Server.

WINDOWS GOLD IMAGE CONSIDERATIONS

The following should be considered when creating and using Gold Images:

- Windows 7, 8.1, and 10, as well as Windows Servers 2008 R2, 2012 R2, and 2016, use the same user state separation, which means users must log out of their session in order for their session changes to be continued. By default, user documents are written synchronously.
- Users must never make changes to the network settings for the first "Local Area Network Connection;" it is configured during the Gold Image creation and should not be changed.
- The program `vbverdeuser_bootstrap.exe` in the Windows **Start** folder must not be deleted. It is present in the "All Users Startup folder." This program starts the user portion of the guest session.
- RDP is enabled by default in Windows 7 and 10 guests and Windows 2008 Server R2, Windows 2012 Server R2, and Windows Server 2016.
- If assigning Session Settings to a Gold Image that enable multiple CPUs, confirm that the Gold Image is installed with at least the same number of virtual CPUs that will be assigned.
- If Windows Gold Images are created on Intel servers and are run on AMD Branch servers (or created on AMD and run on Intel), Windows will boot twice after an initial start up, an upgrade, or each time it boots if in Normal Life deployment mode. This occurs if the images are not joined to Active Directory through Session Settings. If the image is joined to Active Directory through Session Settings, Windows will not need an additional reboot.

VERDE Client Software Tools are used to upgrade Gold Images created with an earlier version of VERDE and to complete the Gold Image post-installation. See Upgrading and Importing Gold Images on p. 108 for more details. Windows tools are provided for both 32- and 64-bit.

WINDOWS RDP ACCESS AND GROUP POLICY

Using Restricted Groups group policy to set membership of the Remote Desktop Users local group can cause problems with VERDE's ability to add the user through the VERDE Management Console. If using the Remote Desktop Users Group Policy, confirm that all users connecting to a Windows session through RDP are members of the group, or are not restricted by settings in the Group Policy Object.

Branch Servers and Gold Images

Gold Images can be created, checked out, checked in, and updated at a branch location. If changes are made to an image at a branch location, changes are synchronized with the master image in the data center when the image is checked in. The VERDE Management Console maintains history and location of each Gold Image.

Cloning or importing Gold Images cannot be done from a branch. The username and password specified for Branch synchronization must be a Master Console Master Administrator in global space.

SINGLE SIGN-ON AND ACTIVE DIRECTORY IN A GOLD IMAGE

If you are joining a Linux virtual desktop to Active Directory, Single Sign-on (SSO) can be used to log into both the VERDE User Console and the virtual machine itself. Once joined, these credentials are passed to the virtual machine automatically when using the VERDE User Console.

Linux client support for SSO requires installing a third-party application, such as Centrify, in the Gold Image.

Windows desktops should NOT be joined to the Active Directory through the Gold Image. Use the VERDE Management Console Session Settings to join desktops to a domain.

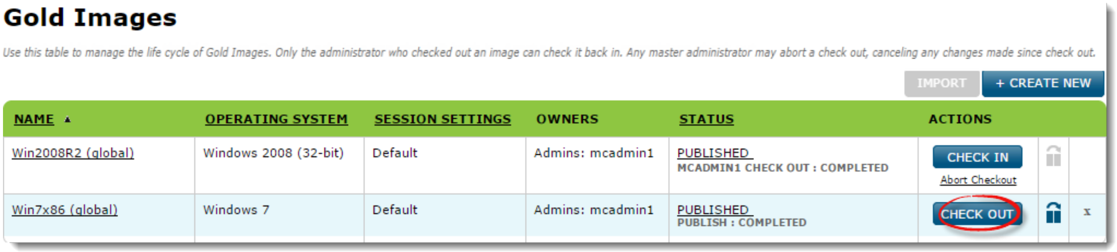
Single Sign-On capability is established with the installation of the VERDE Client Software Tools on the client. The following table lists the operating systems and communications protocols available for SSO.

Table 5-1 SSO Supported Protocols Table

Guest Operating System	SSO Supported Protocols		
	RDP	SPICE	UXP
Windows	✓	✓	✓
Red Hat/CentOS 6.x , 7.x (64-bit)	✗	✓	✗
Ubuntu 12.x, 14.x, and 16.x (64-bit)	✗	✓	✗

Gold Images

The **Gold Images** screen enables the creation and management of Gold Images. A table displays the list of existing Gold Images and the status for each one. The name, operating system, virtual session settings, owner, status (New, New Install Complete, or Published), and actions that can be performed for each Gold Image are listed.



Gold Images

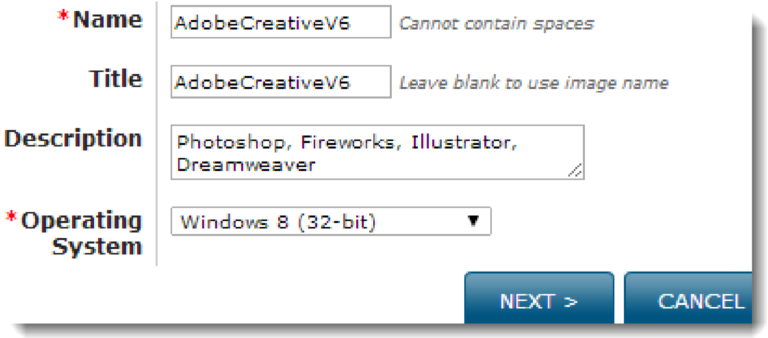
Use this table to manage the life cycle of Gold Images. Only the administrator who checked out an image can check it back in. Any master administrator may abort a check out, canceling any changes made since check out.

NAME ▲	OPERATING SYSTEM	SESSION SETTINGS	OWNERS	STATUS	ACTIONS		
Win2008R2 (global)	Windows 2008 (32-bit)	Default	Admins: mcadmin1	PUBLISHED MCADMIN1 CHECK OUT : COMPLETED	CHECK IN Abort Checkout	🔓	
Win7x86 (global)	Windows 7	Default	Admins: mcadmin1	PUBLISHED PUBLISH : COMPLETED	CHECK OUT	🔒	x

CREATING A NEW GOLD IMAGE

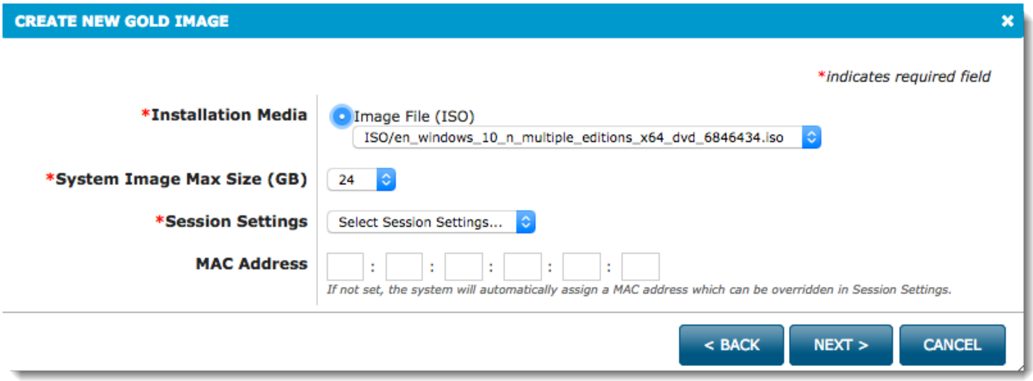
Gold Images are created and managed from the **Configuration** tab of the VERDE Management Console.

1. To create a new Gold Image, select "CREATE NEW."
2. Enter the Gold Image name with no spaces or commas in the field provided.
3. (Optional) Enter the Gold Image title and description. The title is displayed to end users who access this image through the VERDE login screen on the user console or VERDE client. If you leave this field blank, the system will automatically use the image name as the title.
4. Choose the operating system from the drop-down list and select "Next" to continue to the next step.



*Name	AdobeCreativeV6	*Cannot contain spaces*
Title	AdobeCreativeV6	*Leave blank to use image name*
Description	Photoshop, Fireworks, Illustrator, Dreamweaver	
*Operating System	Windows 8 (32-bit) ▼	

5. Beside "Installation Media," select the method for which you will be using to install the Gold Image. Your options include: PXE (Linux only), CD/DVD Drive, or Image File.



CREATE NEW GOLD IMAGE

*indicates required field

*Installation Media ● Image File (ISO) ISO/en_windows_10_n_multiple_editions_x64_dvd_6846434.iso

*System Image Max Size (GB) 24

*Session Settings Select Session Settings...

MAC Address _ : _ : _ : _ : _ : _

If not set, the system will automatically assign a MAC address which can be overridden in Session Settings.

6. Beside "System Image Max Size (GB)," select the maximum amount allowed for the guest's virtual C: (system) drive volume size from the drop-down list. The table below lists the different operating systems and their maximum image size.

   Maximum Image Size

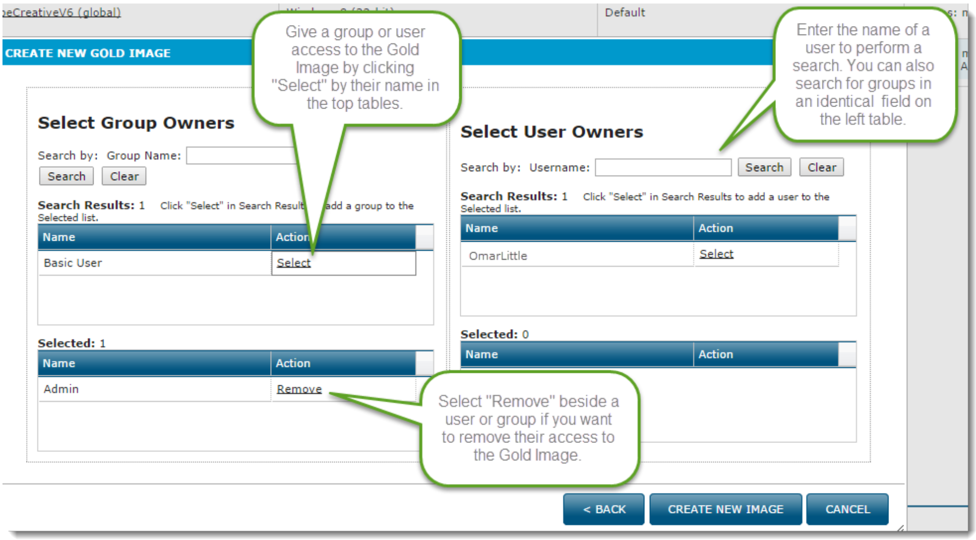
Table 5-2 Maximum Image Size

Operating System	Default Image Max Size
Linux	12 GB
Windows Servers 2008 R2, 2012 R2, and 2016 Windows 7, 8.1, and 10	24 GB

7. In the drop-down beside "Session Settings," select the setting you wish to apply to the Gold Image.
8. Select "NEXT."
9. A new dialogue window will open that will allow you to select groups or users that will have access to this image. Groups and users are broken up into two panels. The actions listed below are relevant for both panels:
   - **Perform a search for groups or users**. Type the name of a group or user in the field beside "Search by," then click "Search." The search results will appear in the table below.
   - **Add access**. Choose "Select" beside the group or user name. Observe that the group or user will then be visible in the "Selected" tables.

- **Remove access**. In the "Selected" table, click "Remove" by the name of the group or user.

Important: The accounts selected must have the Gold Images ownership permission. If an account is not selected, ownership of the image is assigned to the creator of the image.



Select Group Owners

Search by: Group Name:

Search Results: 1 Click "Select" in Search Result add a group to the Selected list.

Name	Action
Basic User	Select

Selected: 1

Name	Action
Admin	Remove

Select User Owners

Search by: Username:

Search Results: 1 Click "Select" in Search Results to add a user to the Selected list.

Name	Action
OmarLittle	Select

Selected: 0

Name	Action

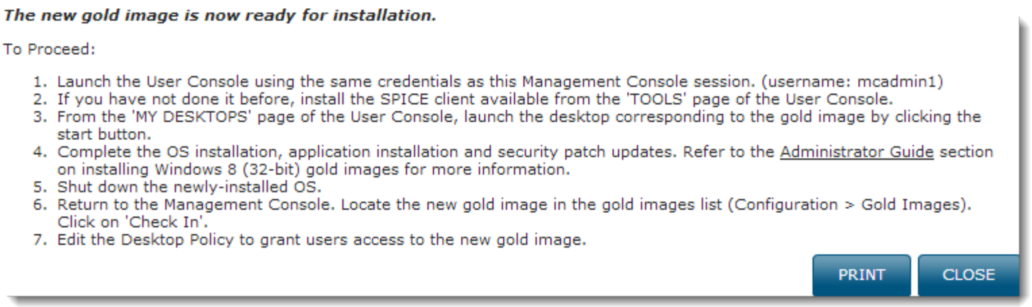
Give a group or user access to the Gold Image by clicking "Select" by their name in the top tables.

Enter the name of a user to perform a search. You can also search for groups in an identical field on the left table.

Select "Remove" beside a user or group if you want to remove their access to the Gold Image.

10. Select "CREATE NEW IMAGE."
11. A notification displays instructions for installing the Gold Image. Read the instructions, then select "CLOSE." The structure of the Gold Image has now been created on the server. The image is listed

with the status "New" until the operating system is installed and the Gold Image is published.



The new gold image is now ready for installation.

To Proceed:

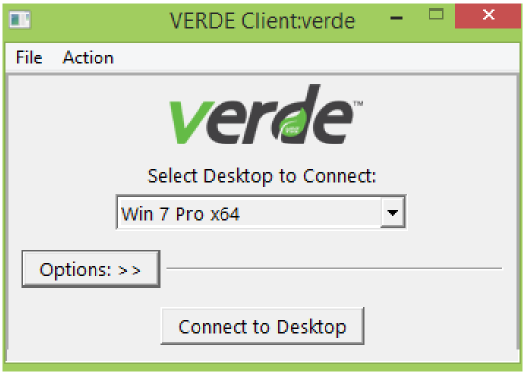
1. Launch the User Console using the same credentials as this Management Console session. (username: mcadmin1)
2. If you have not done it before, install the SPICE client available from the 'TOOLS' page of the User Console.
3. From the 'MY DESKTOPS' page of the User Console, launch the desktop corresponding to the gold image by clicking the start button.
4. Complete the OS installation, application installation and security patch updates. Refer to the Administrator Guide section on installing Windows 8 (32-bit) gold images for more information.
5. Shut down the newly-installed OS.
6. Return to the Management Console. Locate the new gold image in the gold images list (Configuration > Gold Images). Click on 'Check In'.
7. Edit the Desktop Policy to grant users access to the new gold image.

Preparing to Install a Gold Image Operating System

Installing a Gold Image requires VERDE Guest Drivers and Tools to run correctly. Install these from the VERDE Client. The VERDE Client will run a system check and prompt for an Installation or upgrade of Client Software Tools.

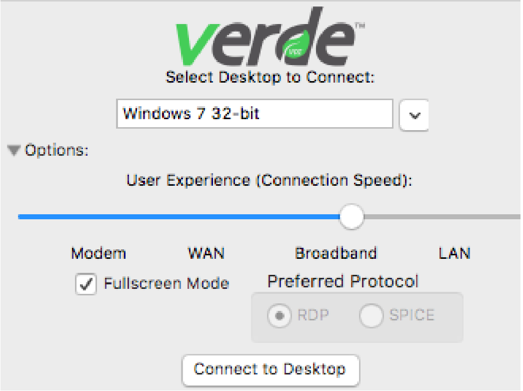
1. Login to the VERDE User Console to download the client:

```
http://<server-name-or-IP>:8443/
```



Select Desktop to Connect: Win 7 Pro x64

2. If necessary, select "Options" to choose connection speed or to run the VERDE session in full-screen mode. The User Console displays the New Image that was just created in the VERDE Management Console.



Select Desktop to Connect: Windows 7 32-bit

User Experience (Connection Speed): Broadband

☑ Fullscreen Mode

Preferred Protocol: ● RDP ○ SPICE

Installing a Windows Server 2008 R2 Gold Image

The options for installing Windows 2008 Server R2 are standard. Windows Server 2008 R2 Datacenter Edition (Full installation) is supported with the Desktop Experience feature enabled. Do not disable this feature during installation.

1. When prompted, choose the Installation Language, Time and currency format, and Keyboard or input method.
2. Select "Install Now."
3. Select the operating system type, "Windows Server 2008 R2 Datacenter (Full Installation)."
4. Accept the license terms.
5. When prompted for an installation type, select "Custom (advanced)." Do not select to upgrade.
6. At the following prompt, always select "Disk 0 Unallocated Space."
7. When prompted, enter a password for the Administrator account.
8. Configure the system. Change the computer name.

After the image has been installed, follow these steps to ensure remote access from other computers is enabled:

1. Navigate to the Windows "Start" menu and right-click on "Computer."
2. Select "Properties." The **System** window will open.
3. On the left panel, select the "Remote Settings" option. The **System Properties** window will open.
4. In the **Remote Desktop** section, select the "Allow connections from computers running any version of Remote Desktop (less secure)" option.
5. Select "Apply" to save your changes.

Note: After installing the base Windows 2008 Server R2 Guest OS, and before you run the post installation script (FinishWindowsInstall) described in "Run the VERDE Post Installation Script," you need to install the Microsoft security update KB 3033929 available from: **https://technet.microsoft.com/en-us/library/security/3033929.aspx**.

ENABLE WINDOWS SERVER 2008 R2 DATA CENTER DESKTOP EXPERIENCE

The Desktop Experience feature must be enabled after a Windows Server 2008 R2 Data Center installation. Perform the following steps to enable the Desktop Experience feature:

1. In the **Server Configuration** window, select "Add Features."
2. In the **Select Features** window, select "Desktop Experience."
3. If any other features are required, a prompt lists them.
4. In the **Add Features** window, select "Add Required Features."

5. In the **Select Features** window, the "Desktop Experience" check box is selected in addition to the other required features.
6. Select "**Next**."
7. Finish the installation and restart the server.
8. Continue with configuring the Gold Image. See Configuring the Gold Image on p. 109 for more details.

RUN THE VERDE POST INSTALLATION SCRIPT

1. Login to the desktop session and select **Start** > **Computer**.
2. In the right pane, select the VERDE CD (CD Drive with the VERDE icon).

   Run the post-installation script to configure VERDE components and make the Gold Image operational.
3. Double-select "FinishWindowsInstall." Follow the on-screen prompts to install the VERDE VDI User Tools. Several software driver packages will install.
4. When the installation is complete, Windows will shut down.
5. Log into the VERDE User Console as an administrator and launch the desktop.
6. Select **Start** > **Computer**. Go to **Control Panel** > **System and Security** > **Windows Update**.
7. Immediately install all Windows updates.
8. Select "Install updates" and follow the prompts to complete the installation
9. Select **Start** > **Computer**. Go to **Control Panel** > **System and Security** > **Windows Firewall**.
10. On the left navigation pane, click on **Advanced Settings**.
11. Click on **Windows Firewall Properties**.
12. Under the **Domain Profile, Private Profile, and Public Profile** tabs, change the **Firewall State** to **Off**.
13. Follow the steps outlined in Windows Activation Tasks on p. 111.
14. When this phase is complete, the status of the Gold Image is "NEW" in the VERDE Management Console.
15. Select "CHECK IN" to make the image available for deployment.

Installing Windows Server 2012 Gold Image

The options for installing Windows Server 2012 R2 are standard. Windows Server 2012 R2 Datacenter Edition (Full installation) is supported with the Desktop Experience feature enabled. Do not disable this feature during installation.

1. When prompted, choose the Installation Language, Time and currency format, and Keyboard or input method.
2. Select "Install Now."
3. Select the operating system type, "Windows Server 2012 R2 Datacenter (Full Installation)."
4. Accept the license terms.
5. When prompted for an installation type, select "Custom (advanced)."
6. At the following prompt, always select "Disk 0 Unallocated Space."
7. When prompted, enter a password for the Administrator account.
8. Configure the system. Change the computer name.

After the image has been installed, follow these steps to ensure remote access from other computers is enabled:

1. Navigate to the Windows "Start" menu and right-click on "Computer."
2. Select "Properties." The **System** window will open.
3. On the left panel, select the "Remote Settings" option. The **System Properties** window will open.
4. In the **Remote Desktop** section, select the "Allow connections from computers running any version of Remote Desktop (less secure)" option.
5. Select "Apply" to save your changes.

ENABLE WINDOWS SERVER 2012 R2 DATA CENTER DESKTOP EXPERIENCE

The Desktop Experience feature must be enabled after a Windows Server 2012 R2 Data Center installation. Perform the following steps to enable the Desktop Experience feature:

1. In the **Server Configuration** window, select "Add Features."
2. In the **Select Features** window, select "Desktop Experience."
3. If any other features are required, a prompt lists them.
4. In the **Add Features** window, select "Add Required Features."
5. In the **Select Features** window, select the "Desktop Experience" check box if it is not already checked.
6. Select "Next."
7. Finish the installation and restart the server.
8. Continue with configuring the Gold Image. See Configuring the Gold Image on p. 109 for more details.

RUN THE VERDE POST INSTALLATION SCRIPT

1. Login to the desktop session and select **Start** > **Computer**.
2. In the right pane, select the VERDE CD (CD Drive with the VERDE icon).

   Run the post-installation script to configure VERDE components and make the Gold Image operational.
3. Double-select "FinishWindowsInstall." Follow the on-screen prompts to install the VERDE VDI User Tools. Several software driver packages will install.
4. When the installation is complete, Windows will shut down.
5. Log into the VERDE User Console as an administrator and launch the desktop.
6. Select **Start** > **Computer**. Go to **Control Panel** > **System and Security** > **Windows Update**.
7. Immediately install all Windows updates.
8. Select "Install updates" and follow the prompts to complete the installation.
9. Follow the steps outlined in Windows Activation Tasks on p. 111.
10. When this phase is complete, the status of the Gold Image is "NEW " in the VERDE Management Console. Select "CHECK IN" to make the image available for deployment.

Installing a Windows 7 Gold Image

The options for installing Windows 7 are standard. Select the following options when prompted:

1. When prompted for installation type, select "Custom (advanced)." Do not select "Upgrade."
2. At the next prompt, always select "Disk 0 Unallocated Space." Do not select "Disk 1."
3. When prompted to enter a user name, choose a generic user name such as `verde-xxx`.
4. Choose a computer name that is unique on the network if the guest will be joined to Active Directory.
5. If using Active Directory, specify the computer name/user explicitly when logging in to the Gold Image. Avoid complicated user names and spaces.
6. When prompted, specify a password for the account.
7. If prompted to enter a product key, clear the "Automatically activate Windows when I'm online" check box. Instead, activate Windows manually. This avoids unnecessary activations (if needing to reinstall) before the activation period expires.
8. When prompted to select protection settings, select "Use recommended settings."
9. When prompted for the computer's location, select "Work network."
10. Select "Restart now" to complete the updates. Then, follow the prompts to complete the update installation. The virtual desktop will restart. Continue with configuring the Gold Image. See Configuring the Gold Image on p. 109 for more details.

After the image has been installed, follow these steps to ensure that remote access from other computers is enabled:

1. In the Windows "Start" menu, right-click on "Computer" to open the context menu.
2. Select "Properties." The **System** window opens.
3. On the left panel, select the "Remote Settings" option. The **System Properties** window opens.
4. In the **Remote Desktop** section, select the "Allow connections from computers running any version of Remote Desktop (less secure)" option.
5. Select "Apply" to save your changes.

Note: After installing the base Windows 7 (or a Windows 2008) Guest OS, you must reboot before running the FinishWindowsInstall script.

RUN THE VERDE POST INSTALLATION SCRIPT

1. Login to the desktop session and select **Start** > **Computer**.
2. In the right pane, select the VERDE CD (CD Drive with the VERDE icon).

   Run the post-installation script to configure VERDE components and make the Gold Image operational.
3. Double-select "FinishWindowsInstall." Follow the on-screen prompts to install the VERDE VDI User Tools. Several software driver packages will install.
4. When the installation is complete, Windows will shut down.
5. Log into the VERDE User Console as an administrator and launch the desktop.
6. Select **Start** > **Computer**. Go to **Control Panel** > **System and Security** > **Windows Update**.
7. Immediately install all Windows updates.
8. Select "Install updates" and follow the prompts to complete the installation.
9. Select **Start** > **Computer**.
10. Right-select "Properties."
11. Select the "(number of) days to activate. Activate Windows now" or the "Select here to activate" link at the bottom of the window.
12. Follow the prompts to complete the activation.
13. When this phase is complete, the status of the Gold Image is "NEW (INSTALL COMPLETE)" in the VERDE Management Console.
14. When the image is ready to be checked in, the Gold Image status will change to "NEW." Select "CHECK IN" to make the image available for deployment.

Installing a Windows 8.1 Gold Image

The options for installing Windows 8.1 are standard. Select the following options when prompted:

1. When prompted for installation type, select "Custom (advanced)."
2. At the following prompt, always select "Disk 0 Unallocated Space."
3. When prompted to enter a user name, choose a generic user name such as `verde-xxx`.
4. Choose a computer name that is unique on the network if the guest will be joined to Active Directory.
5. If using Active Directory, specify the computer name/user explicitly when logging in to the Gold Image. Avoid complicated user names and spaces.
6. When prompted, specify a password for the account.
7. If prompted to enter a product key, clear the "Automatically activate Windows when I'm online" checkbox. Instead, activate Windows manually. This avoids unnecessary activations (if needing to reinstall) before the activation period expires.
8. When prompted to select protection settings, select "Use recommended settings."
9. When prompted for the computer's location, select "Work network."
10. Select "Restart now" to complete the updates. Then, follow the prompts to complete the update installation. The virtual desktop will restart. Continue with configuring the Gold Image. See Configuring the Gold Image on p. 109 for more details.

After the image has been installed, follow these steps to ensure remote access from other computers is enabled:

1. Navigate to the Windows "Start" menu and right-click on "Computer."
2. Select "Properties." The **System** window will open.
3. On the left panel, select the "Remote Settings" option. The **System Properties** window will open.
4. In the **Remote Desktop** section, select the "Allow connections from computers running any version of Remote Desktop (less secure)" option.
5. Select "Apply" to save your changes.

RUN THE VERDE POST INSTALLATION SCRIPT

1. Login to the desktop session and select **Start** > **Computer**.
2. In the right pane, select the VERDE CD (CD Drive with the VERDE icon).

   Run the post-installation script to configure VERDE components and make the Gold Image operational.
3. Double-select "FinishWindowsInstall." Follow the on-screen prompts to install the VERDE VDI User Tools. Several software driver packages will install.

4. When the installation is complete, Windows will shut down.
5. Log into the VERDE User Console as an administrator and launch the desktop.
6. Select **Start** > **Computer**. Go to **Control Panel** > **System and Security** > **Windows Update**.
7. Immediately install all Windows updates.
8. Select "Install updates" and follow the prompts to complete the installation.
9. Select **Start** > **Computer**.
10. Right-select "Properties."
11. Select the "(number of) days to activate. Activate Windows now" or the "Select here to activate" link at the bottom of the window.
12. Follow the prompts to complete the activation.
13. When this phase is complete, the status of the Gold Image is "NEW (INSTALL COMPLETE)" in the VERDE Management Console.
14. When the image is ready to be checked in, the Gold Image status will change to "NEW." Select "CHECK IN" to make the image available for deployment.

Installing a Windows 10 Gold Image

The options for installing Windows 10 include additional steps to reset some of the Microsoft-enabled defaults included in a standard Windows 10 image. These steps are necessary to improve the performance of Windows 10 images running in a VDI environment. Please refer to Windows Advanced Configuration on p. 112 for more information. Select the following options when prompted:

1. When prompted for installation type, select "Custom (advanced)."
2. At the following prompt, always select "Disk 0 Unallocated Space."
3. When prompted to enter a user name, choose a generic user name such as `verde-xxx`.
4. Choose a computer name that is unique on the network if the guest will be joined to Active Directory.
5. If using Active Directory, specify the computer name/user explicitly when logging in to the Gold Image. Avoid complicated user names and spaces.
6. When prompted, specify a password for the account.
7. If prompted to enter a product key, clear the "Automatically activate Windows when I'm online" checkbox. Instead, activate Windows manually. This avoids unnecessary activations (if needing to reinstall) before the activation period expires.
8. When prompted to select protection settings, select "Use recommended settings."
9. When prompted for the computer's location, select "Work network."
10. Select "Restart now" to complete the updates. Then, follow the prompts to complete the update installation. The virtual desktop will restart. Continue with configuring the Gold Image. See Configuring the Gold Image on p. 109 for more details.

After the image has been installed, follow these steps to ensure remote access from other computers is enabled:

1. Navigate to the Windows "Start" menu and right-click on "Computer."
2. Select "Properties." The **System** window will open.
3. On the left panel, select the "Remote Settings" option. The **System Properties** window will open.
4. In the **Remote Desktop** section, select the "Allow connections from computers running any version of Remote Desktop (less secure)" option.
5. Select "Apply" to save your changes.

Note: Windows 10 is not pre-configured for optimal VDI performance and several services. and settings should be turned off. Please refer to the **NComputing Knowledge Base articles "VERDE VDI Optimization for Windows 10."**

RUN THE VERDE POST INSTALLATION SCRIPT

1. Login to the desktop session and select **Start** > **Computer**.
2. In the right pane, select the VERDE CD (CD Drive with the VERDE icon).

   Run the post-installation script to configure VERDE components and make the Gold Image operational.
3. Double-select "FinishWindowsInstall." Follow the on-screen prompts to install the VERDE VDI User Tools. Several software driver packages will install.
4. When the installation is complete, Windows will shut down.
5. Log into the VERDE User Console as an administrator and launch the desktop.
6. Select **Start** > **Computer**. Go to **Control Panel** > **System and Security** > **Windows Update**.
7. Immediately install all Windows updates.
8. Select "Install updates" and follow the prompts to complete the installation.
9. Select **Start** > **Computer**.
10. Right-select "Properties."
11. Select the "(number of) days to activate. Activate Windows now" or the "Select here to activate" link at the bottom of the window.
12. Follow the prompts to complete the activation.
13. When this phase is complete, the status of the Gold Image is "NEW (INSTALL COMPLETE)" in the VERDE Management Console.
14. When the image is ready to be checked in, the Gold Image status will change to "NEW." Select "CHECK IN" to make the image available for deployment.

Installing a Linux Desktop Gold Image

For a list of supported guest operating systems, see the **VERDE Configuration Planning and Installation Guide**. To join a Linux image to Active Directory, you'll need to install Centrify Express on the Gold Image. The steps to perform that action are listed below. Lastly, before attempting to install a Linux Gold Image, confirm the VERDE VDI User Tools and the SPICE Client are installed.

Note: User accounts should not be created inside the Gold Image.

QXL DRIVER GUEST-SPECIFIC REQUIREMENTS

When creating Linux Gold Images, install the following (32-bit and 64-bit versions) guests from the VERDE Management Console by choosing the Linux option from the Operating System menu:

- CentOS/RHEL 6.x and 7.x
- Ubuntu 12.04, 14.04, and 16.04
- Linux Mint 18

Due to Ubuntu system limitations in version 12.04, Ubuntu 12.04 virtual desktops do not support the latest version of KVM. It is still possible to run Ubuntu 12.04 virtual desktops in VERDE but additional configuration steps must be followed to set the virtual desktop to use an earlier version of KVM.

1. In the VERDE Management Console, navigate to the Gold Images screen and create a Ubuntu 12 gold image. Select "Linux" in the "Operating System" field.
2. After the Gold Image has been created in the VERDE Management Console, open a terminal window to modify the `settings.local` file.
3. In the terminal window, navigate to the gold image install directory '/home/vb-verde/verde-orgs/<org id>/gold/<Image Name>'. Open the `settings.local` file and set 'WIN4_MACH_TYPE-E="4".
4. Save the file. Then start the OS installation process from the VERDE Client or the VERDE User Console.

POST-INSTALLATION SCRIPTS

When installation is complete and the image restarts, open the CD named VERDE mounted on your desktop, and run the script `Install_VERDE_Guest_Tools`.

Note: If setting up a CentOS 7.x image you must be logged in as a root user to execute the post-install script.

SETTING UP THE VERDE SYSTEM TO DYNAMICALLY JOIN LINUX GOLD IMAGES TO ACTIVE DIRECTORY

VERDE offers the possibility to dynamically join Linux Gold Images to Active Directory. This means that each time a Linux virtual desktop initializes, it will register with Active Directory where a computer object will be created. The virtual desktop leaves the domain when it shuts down.

To be able to dynamically join a Linux virtual desktop -Gold Image - to AD, a third-party software is required in the Gold Image. VERDE currently supports Centrify Express for Active Directory (AD) integration.

If you are using another third-party software (for example, Powerbroker), you will have to do a "static join" instead. In this case, the Gold Image itself joins the Active Directory domain, and the virtual desktops will inherit the trust relationship established with the Gold Image. While this simplifies and eliminates the need to create additional resources in AD, a drawback of this approach is that the administrator has to schedule a Gold Image "leave and rejoin domain" operation before the "lease" expires (ninety (90) days); otherwise users will not be able to log in.

To install Centrify Express for Active Directory (AD) integration:

1. In the VERDE Management Console, navigate to the **Gold Images** screen. Under the "Actions" column, select “Check Out” in the row of the Gold Image.
2. Open a new browser in the Gold Image and download "Centrify Agent for CentOS Linux" from **Centrify**.
3. Extract the tar package: `tar xvzf centrify-suite-<version>-<platform>.tgz`.
4. Run the `./install-express.sh` script. The default options are acceptable unless needed for customization. After the script has completed processing, the Gold Image will reboot.
5. Back on the VERDE Management Console, on the **Gold Images** screen, check in the Gold Image.
6. On the server, open a terminal window. Go to the gold image directory, '/home/vb-verde/verde-orgs/<org id>/gold/<Image Name>' and open the `settings.local` file. Change the 'WIN4_LINUX_AD_AGENT' value to 'Centrify'. Save the file.

CENTOS/RHEL GOLD IMAGES INSTALLATION

- When logging in to the VERDE User Console as the VERDE Management Console administrator to build the image, select the option of using partition **hda** instead of **hdb**.
- When creating a CentOS/RHEL 6 image, install it with two virtual CPU's in VERDE Management Console **Session Settings** to make the RHEL installer choose the **smp** kernel instead of the uniprocessor kernel.
- When installing a RHEL image, confirm that the machine is registered with the RHEL Network in order for all dependencies to be downloaded.

INSTALL AN UBUNTU 12.04 GOLD IMAGE

To benefit from accelerated SPICE features, install the Ubuntu Gold Image using the VERDE Management Console. See Gold Images on p. 83 for more details.

VERDE does not support Unity interface. After the operating system installation, a warning states that Ubuntu Classic should be chosen. Choose this option from **System —> Administration —> Login** screen.

Perform the following steps to install Ubuntu:

1. Enable `sshd` to run at boot time.
2. Run `Install_VERDE_Guest_Tools` to shut down the Gold Image.
3. Restart the image and install the gdm package `apt-get install --reinstall gdm`.
4. **(Optional for AD User Access)** To enable access to the Ubuntu Gold Image by AD users, perform the following steps:
   a. Run `vi /etc/pam.d/common-session`.
   b. Change `session sufficient pam_lsass.so` to `session [success=ok default=ignore] pam_lsass.so`.
5. Shutdown the Gold Image.
6. Check in the Gold Image on the VERDE Management Console.
7. **(Optional for AD User Access)** Assign the Gold Image to an AD user.
8. Save the changes.

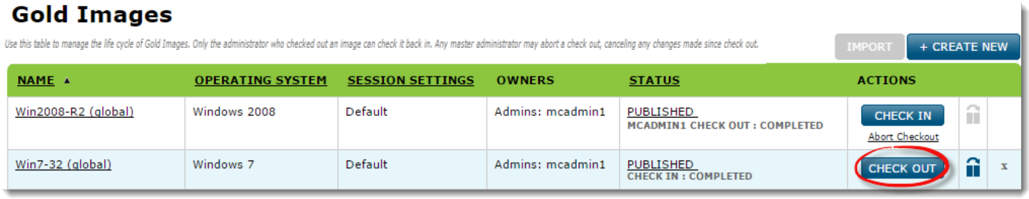
Making Changes to a Gold Image

To make changes to a Gold Image after it has been published, the image must be checked out. To keep guest sessions from being impacted, the checkout process creates a temporary copy of the image. When the changes are checked in, users are notified and offered the opportunity to shutdown their Virtual Desktop to obtain the latest update.

CHECK OUT AND CHANGE THE GOLD IMAGE

Perform the following steps to check out and change a Gold Image:

1. Log into the VERDE Management Console and select **Configuration** > **Gold Images**.
2. In the row that contains the image to be changed, select "CHECK OUT."

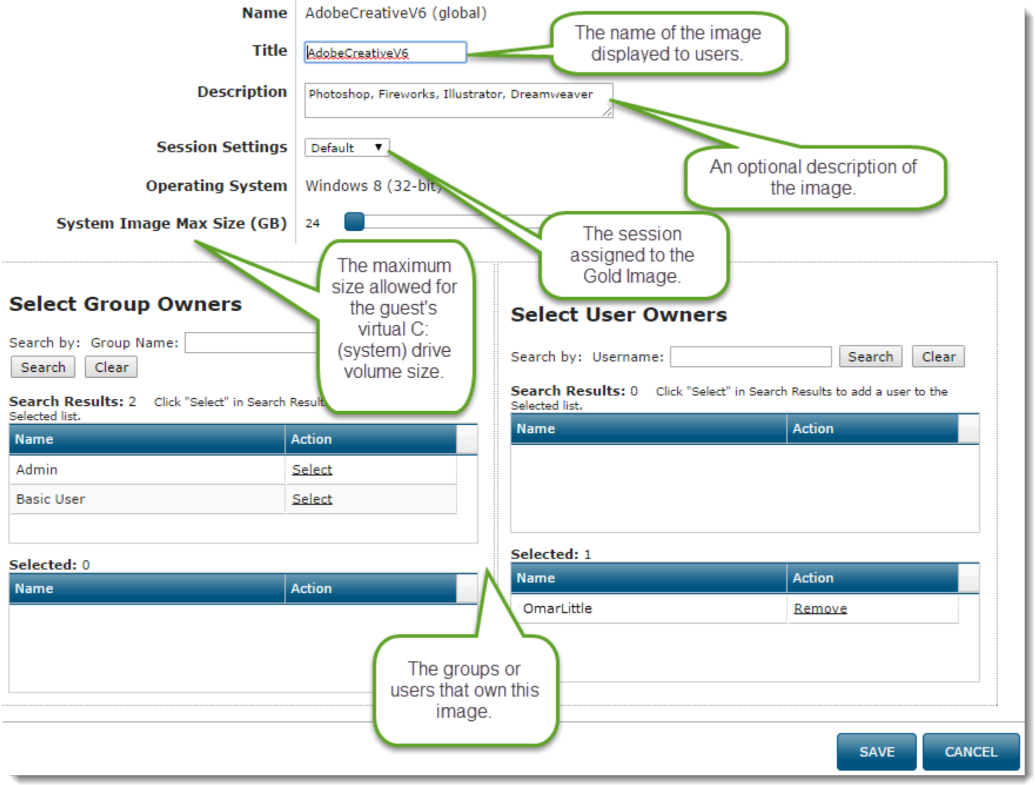


Gold Images

Use this table to manage the life cycle of Gold Images. Only the administrator who checked out an image can check it back in. Any master administrator may abort a check out, canceling any changes made since check out.

NAME ▲	OPERATING SYSTEM	SESSION SETTINGS	OWNERS	STATUS	ACTIONS		
Win2008-R2 (global)	Windows 2008	Default	Admins: mcadmin1	PUBLISHED MCADMIN1 CHECK OUT : COMPLETED	CHECK IN Abort Checkout		
Win7-32 (global)	Windows 7	Default	Admins: mcadmin1	PUBLISHED CHECK IN : COMPLETED	CHECK OUT		x

3. Depending on the size of the image, the check out process may take a few minutes.
4. After the checkout is complete, the Gold Image is available for update. Click on the name of the Gold Image under the "Name" column. A new window listing the Gold Image details will appear.
5. Select "Edit."
6. From the VERDE Management Console, the following settings can be changed:
   - **Title**. The name of the image displayed to users.
   - **Description**. An optional description of the image.
   - **Session Settings**. The session assigned to the Gold Image. To learn more about session settings, see Managing Session Settings on pg. 51.
   - **System Image Max Size (GB)**. The maximum size allowed for the guest's virtual C: (system) drive volume size.
   - **Group/User Owners**. The groups or users to own this image. The accounts selected must have the Gold Image ownership permission. If an account is not selected, ownership of the image is assigned to the creator of the image.



Name AdobeCreativeV6 (global)

Title AdobeCreativeV6

Description Photoshop, Fireworks, Illustrator, Dreamweaver

Session Settings Default

Operating System Windows 8 (32-bit)

System Image Max Size (GB) 24

The name of the image displayed to users.

An optional description of the image.

The session assigned to the Gold Image.

The maximum size allowed for the guest's virtual C: (system) drive volume size.

The groups or users that own this image.

Select Group Owners

Search by: Group Name:

Search Results: 2 Click "Select" in Search Result Selected list.

Name	Action
Admin	Select
Basic User	Select

Selected: 0

Name	Action

Select User Owners

Search by: Username:

Search Results: 0 Click "Select" in Search Results to add a user to the Selected list.

Name	Action

Selected: 1

Name	Action
OmarLittle	Remove

7. Select "Save" to save your changes. The previous window will appear. Select "Close" to close the window.
8. Select "CHECK IN" to deploy the changes.
9. Back on the main screen, select "CHECK IN" to deploy the changes.

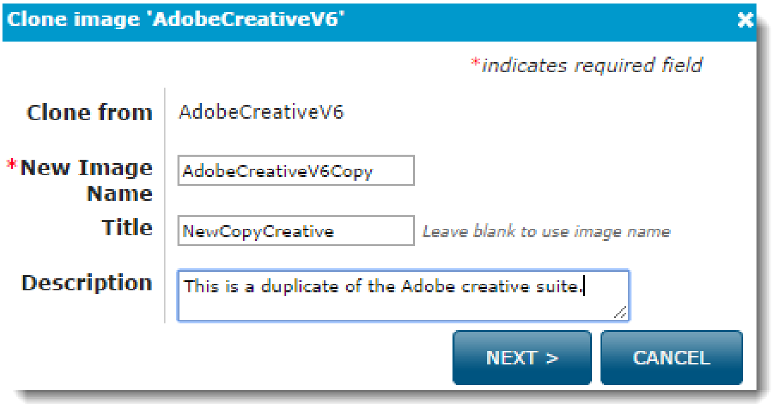
Users running an active VDI session with the dynamic instance of this Gold Image will be notified of the update and will be prompted to shutdown and restart their session. See Customizing the Gold Image Update Notification on p. 145 for more details.

CLONING A GOLD IMAGE

Important: In the current version of VERDE, the cloned Gold Image is linked to the original Gold Image. This means that the original Gold Image should not be deleted—doing so would render the clone non-operational.

A Gold Image clone is a copy of an existing image. Cloning an image is useful for testing configuration settings and/or installing new applications. To create a clone of a Gold Image:

1. On the **Gold Images** screen, select the "Clone" icon . The Clone dialog displays.
2. Enter a name for the new image.
3. Enter a unique name in the "Title" field for guest sessions. While not required, if a unique name is not specified, the clone will be listed with the same title as the original Gold Image.
4. If needed, enter a description.
5. Select "NEXT."

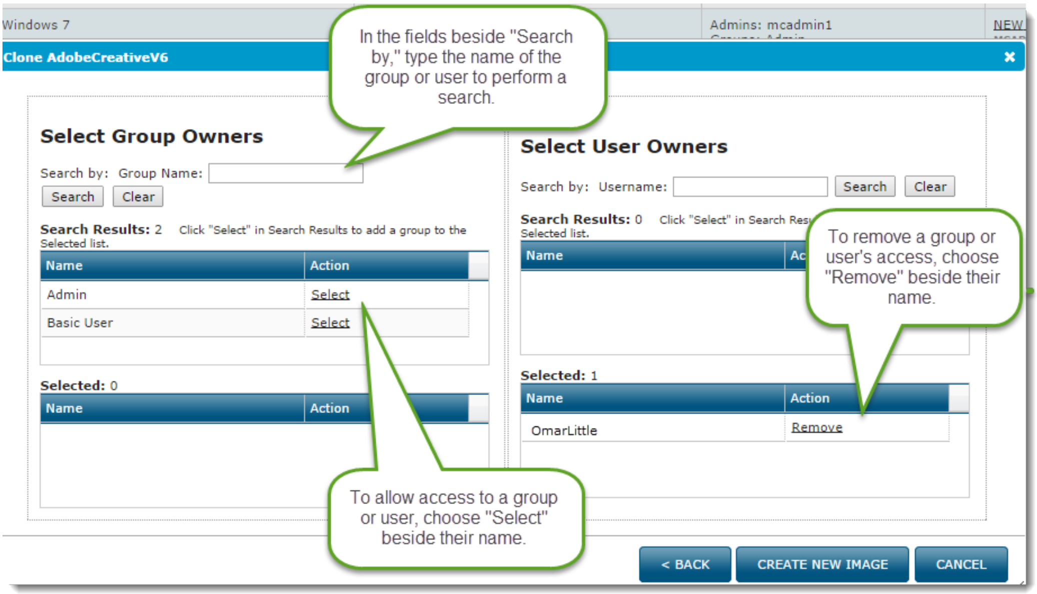


Clone image 'AdobeCreativeV6'

*indicates required field

Clone from	AdobeCreativeV6
*New Image Name	AdobeCreativeV6Copy
Title	NewCopyCreative *Leave blank to use image name*
Description	This is a duplicate of the Adobe creative suite.

6. A new dialogue window will open that will allow you to select groups or users that will have access to this image. Groups and users are broken up into two panels. The actions listed below are relevant for both panels:
   - **Perform a search for groups or users**. Type the name of a group or user in the field beside "Search by," then click "Search." The search results will appear in the table below.
   - **Add access**. Choose "Select" beside the group or user name. Observe that the group or user will then be visible in the "Selected" tables.
   - **Remove access**. In the "Selected" table, click "Remove" by the name of the group or user.

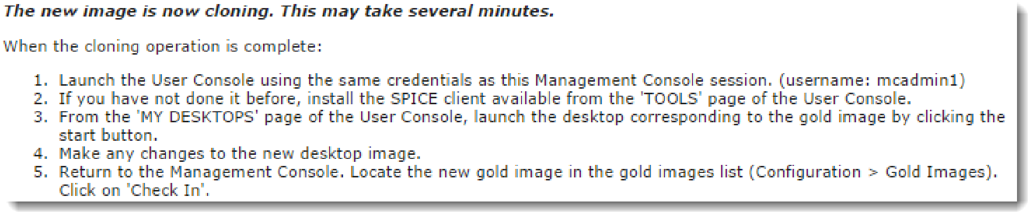


In the fields beside "Search by," type the name of the group or user to perform a search.

To remove a group or user's access, choose "Remove" beside their name.

To allow access to a group or user, choose "Select" beside their name.

7. Select "CREATE NEW IMAGE." A message displays stating that the image is cloning.



The new image is now cloning. This may take several minutes.

When the cloning operation is complete:

1. Launch the User Console using the same credentials as this Management Console session. (username: mcadmin1)
2. If you have not done it before, install the SPICE client available from the 'TOOLS' page of the User Console.
3. From the 'MY DESKTOPS' page of the User Console, launch the desktop corresponding to the gold image by clicking the start button.
4. Make any changes to the new desktop image.
5. Return to the Management Console. Locate the new gold image in the gold images list (Configuration > Gold Images). Click on 'Check In'.

8. On the main screen, you'll see the addition of the cloned Gold Image. Select "PUBLISH" to publish the Gold Image, making it accessible to groups and users. To edit the Gold Image's information, you'll need to check it out first.

Upgrading Gold Image Guest Drivers

When the VERDE server is upgraded, Gold Image guest drivers must be upgraded to match the VERDE server version.

UPGRADING LINUX IMAGES

Linux Client Software Tools are stateless and do not require a manual upgrade. The tools load dynamically on each boot.

UPGRADING WINDOWS 7

After the VERDE server upgrade is complete, perform the following steps to upgrade Windows 7:

First check out the gold images from the Management Console and refer to the sections below to upgrade the Guest Tools to VERDE 8.2.

Note: Upgrades should be performed in full screen mode to avoid encountering a mouse offset that can hinder the upgrade process.

Upgrading Windows 7 and later Guest Tools

Note: On initial startup of a Windows guest from VERDE 7.2, a message appears indicating that files or directories are missing. Ignore these messages.

1. If the guest is Windows 7 or Windows 2008 Server R2 64-bit, apply the Windows KB3033929 update before upgrading the guest tools. You can download the KB update from the following location:

   https://technet.microsoft.com/en-us/library/security/3033929.aspx
2. Restart the gold image and install the KB update.
3. In the Windows Control Panel, uninstall `vb-guest-drivers` and `vb-guest-usb-tools`.
4. Use the following options to complete the upgrade for Windows 7 or Windows 2008 guest images:

   FOR 64 BIT IMAGES

   1. Rename `C:\Program Files (x86)\Virtual Bridges` to `C:\Program Files (x86)\VERDE`.
   2. Navigate to C:\Program Files (x86)\VERDE\System.
   3. Right click on the `UpgradeGuestTools.cmd` script and select "Run as Administrator".
   4. Follow the prompts to upgrade the guest tools.

FOR 32 BIT IMAGES

1. Rename `C:\Program Files\NComputing` to `C:\Program Files\VERDE.`
2. Navigate to C:\Program Files\VERDE\System.
3. Select the `UpgradeGuestTools.cmd` script and 'Run as Administrator."
4. Follow the prompts to upgrade the guest tools.

UPGRADING WINDOWS 8.1

Once VERDE server upgrade is complete, perform the following steps to upgrade Windows 8.1:

1. Log in to the VERDE Management Console and check out the Gold Image.
2. Log in to the VERDE User Console as the administrator who checked out the Gold Image.
3. Launch the Gold Image and open the **Control Panel**. Go to **Programs** > **Programs and Features** to uninstall **VERDE Guest USB Tools**.

   ⚠ **Important:** If the BASE tools were inadvertently removed, log in to the VERDE Management Console and select **Abort Checkout** for the selected Gold Image. Start the upgrade from the beginning.

4. Restart the image. The new VERDE Guest USB Tools will install.
5. Uninstall **vb-guest-drivers**. Restart the Gold Image.
6. From the **User Account Control** screen, select "Yes" to allow Windows to install vb-guest-drivers. If prompted, select "Install this driver software anyway" to allow the installation to continue.

After you have completed these steps, the Gold Image will be upgraded and should work properly with the new guest drivers.

UPGRADING IMAGES TO SUPPORT MULTIPLE CPUS

For previously installed Windows Gold Images perform the following step to confirm that the proper drivers are installed:

1. With the Gold Image checked in, assign a Session Setting that has the number of virtual CPUs that will be allocated.
2. Check out the Gold Image.
3. Log into the VERDE User Console as the administrator who checked out the Gold Image.
4. Launch the Gold Image session and let Windows install its drivers and reboot.
5. Shutdown the session.
6. Log into the VERDE Management Console and check in the Gold Image.

Upgrading and Importing Gold Images

If the VERDE server is upgraded from a previous installation, Gold Images can be imported or transferred. If upgrading, Gold Images can be imported through the VERDE Management Console.

IMPORTING GOLD IMAGES FROM A PREVIOUS INSTALLATION

For the VERDE Management Console to recognize an image as a qualified candidate to import, the Gold Image must reside in `/home/vb-verde/verde-orgs/org-0/users/0local/<administrator>`. The Gold Image can reside in any console administrator directory.

- If the home directory exists on a cluster server, the directory is stored on the shared storage.
- If the home directory exists on a single server, the directory is stored on the host server's hard drive.

The structure of a Gold Image is a directory whose name is the name of the Gold Image itself (such as Windows 7). The directory contains the image files and configuration files. If copying Gold Image directories to a new location, copy all contents of each directory. (There are hidden files in these directories. Confirm all contents are copied.)

Importing Images in a Tenant Organization

Importing gold images into a tenant organization requires copying files into the organization's directory structure.

1. On the **Organizations** screen, locate the ID of the organization, for example *org-7*.
2. In the VERDE Management Console, switch context to the organization and select on the **Gold Images** screen. This creates the directory structure for the Gold Image.
3. Copy the gold image folder (WIN7, for example) to: `/home/vb-verde/verde-orgs/org-7/users/0local/<administrator>/WIN7#org-7`

Note: The organization ID is present twice in this path. It specifies a directory inside `verde-orgs` and is used a second time as a "qualifier" for the Gold Image name.

Importing Images in the VERDE Management Console

1. After copying directories to the new location, change the ownership of the folder to the VERDE Management Console user `(vb-verde)`. Then, import the images with the VERDE Management Console.
2. If VERDE detects existing images on the server, the "IMPORT" button is activated. Select "IMPORT" and the images will be imported. The operation takes a few seconds. The imported image is listed as "NEW" in the list of Gold Images. (After successfully importing the gold images, refer to the "Upgrading Gold Images Guest Drivers" section to upgrade the guest tools.)

CHAPTER 6

Configuring the Gold Image

This chapter discusses the following.

Start the virtual machine by logging into the VERDE User Console. The first time the virtual desktop is started, the application will recommend configuring the following:

- Activate the installation if required (Windows systems).
  - For Windows 2008 Server R2, 7, 8.1, and 10, see Windows Activation Tasks on pg. 111.
- Configure the image for best performance.
  - For Windows users, see Windows Advanced Configuration on pg. 112.
  - For Linux users, see Linux Activation Tasks on pg. 123.
- Confirm the anti-virus software has VERDE processes listed as trusted.
- Linux configures the Gnome Display Manager (GDM) to automatically log in the non-root user created during installation.

See Making Changes to a Gold Image on p. 102 before attempting to adjust settings to the Gold Image. Once changes are complete, check in the image.

Windows Activation Tasks

For Windows 7, 8.1, and 10.

When logging in to a Windows image for the first time, perform the following steps:

1. Select **Start** > **Computer**.
2. Right-select "Properties."
3. Select the "(number of) days to activate. Activate Windows now" or the "Select here to activate" link at the bottom of the window.
4. Follow the prompts to complete the activation.

Windows Advanced Configuration

The standard Windows installation contains some services, policies, and settings that may affect the performance of a guest session. The following are recommended changes to a Windows Gold Image to improve the end user's experience. This list is based on the Windows 10 operating system.

Refer to the Microsoft Windows documentation for steps to configure or disable settings for all Windows Gold Images.

Table 6-1 Recommended Windows Changes

Service or Feature	Recommended Action	Reason for Change	Automated in Gold Image Install
Automatic Updates	Disable	Updates the operating system, which should be managed through a VDI-aware endpoint management product.	Must be disabled manually.
Offline Files	Disable	Enables users to synchronize data with a shared network drive. Normally disabled, this can be enabled if there is a specific need for offline users.	Must be disabled manually.
Internet Explorer First Run screen	Disable	Configures Internet Explorer, which would require each user of the image to navigate through this screen.	Automatically disabled.
Background Intelligent Transfer Service	Disable	Uses network bandwidth to retrieve system updates.	Automatically disabled.
Superfetch	Disable	Caches data to RAM so that it can be immediately available to an application. This can affect the performance of some multi-media applications.	Automatically disabled.
System Restore	Disable	Creates system snapshots and restore points for recovery, which is unneeded in a virtual session.	Automatically disabled.
Windows Logon Screen Saver	Disable	Displays a logon screen saver, which is not needed in a virtual session.	Must be disabled manually.

Service or Feature	Recommended Action	Reason for Change	Automated in Gold Image Install
Sleep Mode	Disable	Puts a machine into a low power state without entirely shutting it off, which should be disabled for virtual sessions.	Must be disabled manually.
Screen File	Set Minimum and Maximum to an identical value	A single size screen file prevents the system from expanding and creating significant IO.	Must be performed manually.
Boot Animation	Disable	Animation, which uses system resources and creates a longer boot time, should be disabled,	Must be disabled manually.
Background Defragmenter	Disable	Rearranges data on the disk to create contiguous sections of data, which can lessen performance. Must be disabled.	Must be disabled manually.
Scheduled Defragmenter	Disable	Rearranges data on the disk to create contiguous sections of data, which can lessen performance. Must be disabled.	Automatically disabled.
Background Auto-layout	Disable	Moves the most-used data closer to the center of the disk to expedite boot time, which can impact performance.	Must be disabled manually.
Machine Account Password	Disable	Forces a reset of the machine account password after 30 days by default, which is unnecessary for virtual sessions.	Automatically disabled.

Audio recording and playback, and Video Playback	Enable	Enables users to record and listen to audio and play video in a session. To allow audio recording, VERDE sets the following registry key:
		`HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp`
		`fDisableAudioCapture REG_DWORD 0 | 1`
		The setting is disabled by default (). VERDE sets it to (0) and then enables the Windows Audio Service.
			Automatically enabled.

Service or Feature	Recom-mended Action	Reason for Change	Automated in Gold Image Install
Windows Defender	Disable	Press the Windws key + R and run `gpedit.msc`. In the Local Group Policy Editor, navigate to `Computer Configuration > Administrative Templates > Windows Components > Windows Defender`. Set "Turn off Windows Defender" to Enabled.	Must be enabled manually.
One Drive			

DISABLE JAVA UPDATES

It's important that Java automatic updates are disabled in the Gold Image. To ensure disablement is in effect, perform the following steps:

1. Check out and start the Gold Image.
2. Open the **Java Control Panel —> Update** tab and disable "Check for Updates Automatically."
3. Select "Apply" and then "OK."
4. Automatic updates must also be disabled in the guest. This action can be performed from the Windows registry in the Gold Image. Open the Windows registry and search for the following key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Update\Policy
   ```

5. Set "EnableJavaUpdate" to "0."

⚠ **Important:** These settings must be reconfigured any time after a Java update is allowed.

Setting Up the Virtual Environment to Support Audio

Windows 7 (32-bit and 64-bit) guest sessions do not require special configuration to enable audio when using the latest version of softphone applications such as Skype or GTalk.

ENABLING AUDIO FOR A WINDOWS 2008 SERVER R2 SERVER GOLD IMAGE

Audio may need to be configured for Windows 2008 Server R2 R2 Data Center Edition Gold Images.

SPICE - Windows 2008 Server R2 64 bit images

Audio is currently only supported in Windows 2008 Server R2 64 bit images when using the SPICE protocol.

Follow these steps to ensure that audio works properly in a Windows 2008 Server R2 64-bit image via SPICE:

1. Log into the VERDE Management Console and check out Windows 2008 Server R2 64-bit Gold Image.
2. Log into the VERDE User Console as admin and launch a Windows 2008 Server R2 64-bit Gold Image.
3. In the Gold Image, open the file:

   ```
   services.msc
   ```

4. In the "Services" list, right-select on "Windows" Audio and select "Properties."
5. Change the "Startup Type" from "Manual" to "Automatic." Stop and start the services.
6. Play a file that has audio to verify it is working properly.

RDP - Windows 2008 Server R2 32 and 64 bit

To enable RDP audio pass through in Windows Server 2008 images, follow these steps:

1. From the VERDE Management Console, check out the Windows 2008 Server R2 64-bit Gold Image.
2. From the User Console, login as the administrator and launch a Windows Server 2008 R2.
3. From a Windows command prompt, run the program:

   ```
   tsconfig.msc (Terminal Server Configuration)
   ```

4. When the configuration screen opens, select the Server RDP instance and right-select on it . This will open the **Properties** window.
5. In the **Client Settings** tab of the **Properties** window, uncheck the "Audio and Video" playback option. Unchecking the option will enable it.
6. Select "Apply," then "OK" to commit the change, then restart the Gold Image. The sound should now be enabled for RDP.
7. Shut down the server and check in the Gold Image.

Enable Audio Recording for Windows Guests

The user console now supports audio recording using RDP for the following:

- Client is using RDP 7 (Windows 10, 8.1, or 7 with latest RDP client)
- Guest supports RDP 7 (Windows 10, 8.1, Windows 7 Enterprise Edition, or Windows 2008 Server R2 Datacenter Edition 64-bit)

A group policy and registry setting and possible group policy is required in the Gold Image to enable recording.

Windows 8.1, 7 and Windows 2008 Server R2 allow redirection of audio recording into a Remote Desktop Session using Remote Desktop Connection. For Windows 8.1 and 7, the Allow audio recording redirection policy does not need to be enabled to allow audio recording redirection, unless it was explicitly disabled. To confirm its status, review the following setting:

```
HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

fDisableAudioCapture REG_DWORD 0 | 1
```

The setting is disabled by default (1).

START THE WINDOWS AUDIO SERVICE

Configure the audio settings for Windows Server R2 and Windows 7, 8.1, and 10 by performing the following steps:

1. From the VERDE Management Console, check out the Windows Gold Image.
2. From the User Console, log into the image as administrator.
3. On the remote desktop session host, open the Services snap-in. Select **Start** > (**Control Panel** for Windows 7) > **Administrative Tools** > **Services**.
4. If the **User Account Control** dialog is displayed, confirm the desired action and select "Yes."
5. In the **Services** pane, right-click on "Windows Audio," and select "Properties."
6. On the **General** tab, in the **Startup type** box, select "Automatic," then "Apply."
7. Under **Service status**, select "Start."
8. Select "OK" to close the **Windows Audio Properties** dialog box.
9. Confirm the "Status" column for the Windows Audio service displays "Started."

ENABLE "ALLOW AUDIO RECORDING REDIRECTION" IN GROUP POLICY

To allow audio recording redirection when connecting to a computer running Windows 2008 Server R2, enable the "Allow audio recording redirection" Group Policy setting in the following location:

```
Computer Configuration\Policies\AdministrativeTemplates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and
Resource Redirection
```

This can be configured by using either the Local Group Policy Editor or the Group Policy Management Console (GPMC).

Note: For more information about Group Policy settings for Remote Desktop Services, see the Microsoft Remote Desktop Services Technical Reference.

ENABLING A START-UP COMMAND IN POOLED WINDOWS SESSIONS

To configure pooled guest Windows sessions for running a specific command or script prior to launching the session, follow the steps listed below:

1. From the VERDE Management Console, check out the Windows Gold Image.
2. From the User Console, log into the image as administrator.
3. Run `regedit` to edit the Windows Registry.
4. Locate the following key in the registry:

   ```
   HKEY_LOCAL_MACHINE\Software\VERDE
   ```

5. From the **Edit** menu, select **New > String Value**.
6. Set the following value:
   - **Value Name.**`PreStartCommandLine`
   - **Value Data.** `<command_line>`
7. Close the Registry Editor and restart the Gold Image. The command will execute once per guest session start, followed by a mandatory reboot. After this occurs, the session will display as available.

Printing from Windows Sessions

Additional configuration is required in Windows Gold Images to install the drivers required for a user to print from the guest session. The following are supported for printing from a virtual Windows session:

- **Print with VERDE print facilities**. VERDE's print facilities enable printing to the client's default printer. This option does not require installing the specific driver for the printer in the Gold Image. Instead, VERDE uses a generic printer driver. To enable the VERDE print facilities, confirm the desired printer is already set as the default on the client, install the VERDE printer driver on the Gold Image, and select the printer as the default in the guest session. If you're using a Windows client, you'll also need to confirm Adobe Acrobat Reader is installed.
- **Printing to a network printer only**. There is no printer installation required on the client. The specific printer driver must be installed in the Gold Image and the printer must be available on the network.
- **USB printer attached to the client device**. If a USB printer is attached and working with the client device, this printer will be re-directed into the guest session. Confirm the correct printer driver is also installed in the Gold Image.

Important: If you're planning on utilizing the VERDE User Console5 to launch remote sessions, special steps apply for accessing printing services. See the topic **Printing for VERDE User Console5** below for more information.

SETTING THE CLIENT'S DEFAULT PRINTER IN THE GOLD IMAGE

This section applies to the first scenario previously described. The solution requires the installation of a printer on the client workstation. The setup applies to RDP and SPICE sessions launched from the VERDE User Console. Create a generic printer `(\\host\client-printer)` inside a Windows Gold Image that will allow any virtual desktop launched from the Gold Image to print to the client's default printer. The configuration will also allow the user to print to a USB printer that is connected to the client workstation.

Important: A default printer must be properly configured for the user's workstation.

Log in to the VERDE Management Console as an administrator and check out the Gold Image to modify. Launch the Gold Image from the User Console.

CONFIGURE PRINTING FOR WINDOWS 7

Perform the following steps to enable printing for Windows 7 guests:

1. Select **Start > Devices and Printers**.
2. Select "Add a printer."
3. In the **Add Printer** dialog box, select "Add a network, wireless, or Bluetooth printer."
4. Select "The printer I want isn't listed."
5. Choose the radial button for "Select a shared printer by name."
6. Type "\\host\client-printer" in the **Browse** text box and select "Next." If the **Connect to Printer** dialog box appears, select "OK" to proceed.
7. Search for the "HP Color LaserJet 2800 Series PS" (or a similar name) and install the printer driver.
8. Leave the Printer name as is and select "Next." If you'd like to test the printer, select "Print a test screen."
9. Select "Finish."
10. In the **Printers and Faxes** section, check to see whether or not your printer has been added successfully. If it has, you will see a new printer icon named **client-printer on host** with a green check mark to indicate that this is the default printer.
11. In the VERDE Management Console, check in the Gold Image. To learn how to check in a Gold Image,

Any virtual desktop session using that Gold Image will now be able to print to its client's default printer. Test the deployed image's printing from a user's client/workstation.

CONFIGURE PRINTING FOR WINDOWS 8.1 AND 10

Configure Printing for Windows 8.1 and 10

Perform the following steps to enable printing for Windows 8.1 and 10 guests:

1. Enter "Devices and Printers" in the Windows search box, or select "Devices and Printers." The **Devices and Printers** window will open.
2. Select "Add a Printer." The **Add Printer** window will open.
3. Select the option, "The printer that I want isn't listed," A new window will appear.
4. Choose "Select a shared printer by name."
5. Type " \\host\client-printer" in the "Browse" text box and select "Next." This will prompt the system to search for the printer and add its driver.
6. After the printer has been successfully added, a new window will appear. Leave the Printer name as is and select "Next."
7. In the next window, select "Print a test screen" if you'd like to test the printer connection. Otherwise, select "Finish."
8. In the **Printers** section, check whether or not your printer has been added successfully. If it has, you'll see a new printer icon named "client-printer on host" with a green check mark to indicate that this is the default printer.
9. In the VERDE Management Console, check in the Gold Image.

Any virtual desktop session using that Gold Image will now be able to print to its client's default printer. Test the deployed image's printing from a user's client/workstation.

SELECTING THE DEFAULT PRINTER IN THE GUEST SESSION

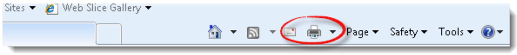
In the guest session, during initial access, the user should define the default printer. For example, in a Windows guest image, the user should select "Start", then click on "Devices and Printers" and select "client-printer on host" as the default.

If required, update the Desktop Policies in the VERDE Management Console to enable the client USB printer.

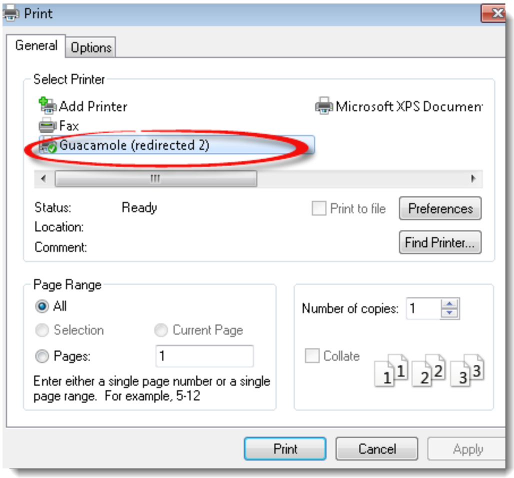
PRINTING FOR VERDE USER CONSOLE5

If you are using VERDE User Console5 to connect to a virtual desktop , you will need to follow the steps below for printing from the session:

1. On the browser or application that contains the item you wish to print, select the **Print** option. The example below depicts the “Print” option of a Chrome browser.



2. After the **Print** window appears, select “**Guacamole <redirect>**” as the desired printer.

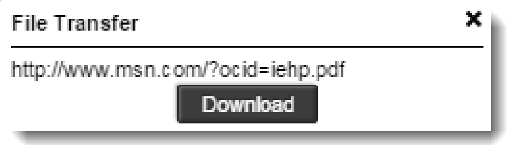


Status: Ready
Location:
Comment:

● All
○ Selection ○ Current Page
○ Pages: 1
Enter either a single page number or a single page range. For example, 5-12

Number of copies: 1
□ Collate

3. Select "**Print**."
4. After you perform Step 4, a small download box will appear on the bottom-right of the screen. This is your virtual print file.



http://www.msn.com/?ocid=iehp.pdf

Select “**Download**” to download the file to your client. The item will download to the folder you have chosen as the default for file downloads. From there, you will be able to print the item on any printer accessible by your client machine.

USB DEVICE SHARING

When USB Redirect service is enabled, the USB ports of the client are accessible from the guest session. When the session starts, the USB ports are no longer available to the client. The USB peripherals, including the printer, are available only to the user through the guest session.

Linux Activation Tasks

Perform the following Linux activation tasks:

1. Set the VERDE server to automatically log in as the VERDE system user.
2. Check out the Gold Image and start it with the VERDE User Console.
3. In Ubuntu, either select **System** > **Administration** > **Login** screen or run the following command with root privileges:

   ```
   /usr/bin/gdmsetup
   ```

4. When finished, shut down the virtual desktop.

ENABLING USB SHARING FOR UBUNTU GUESTS

Ubuntu 12.04 32- and 64-bit guests support USB redirection with the following steps:

1. After completing the Gold Image installation and running the post installation script, launch the desktop as an administrator.
2. As root enter the following commands:

   ```
   cd /usr/lib/verde-guest

   ./build-verde-usb-client.sh
   ```

3. Shut down the desktop. USB is enabled in the guest from the next session start, . Confirm that any applied Session Settings have been USB-enabled.

ENABLING USB SHARING FOR CENTOS/RHEL 6.X GUESTS

CentOS/RHEL 6.x 32- and 64-bit guests support USB redirection with the following steps:

1. Complete the Gold Image installation and launch the desktop as root.
2. Either disable the firewall or open port `48666/tcp` on the firewall.
3. Apply the changes.
4. Open a terminal window, and enter the commands:

   ```
   yum update kernel

   reboot
   ```

5. After the image restarts, open a terminal and enter the command:

   ```
   yum install kernel-devel gcc
   ```

```
/usr/lib/verde-guest/build-verde-usb-client.sh
```

6. Shut down the image.
7. Check the image into the VERDE Management Console. Confirm all applied Session Settings have been USB-enabled.

CENTOS/RHEL 6.0: UPDATING THE QXL DRIVER

Users can increase their screen resolution if the CentOS/RHEL QXL driver is updated in the Gold Image.

To update the QXL driver and the SPICE vdagent, follow these steps:

1. From the Management Console, check out the CentOS/RHEL 6 (64) image.
2. Log into a User Console and start the CentOS/RHEL 6 64 bit image using SPICE.
3. Download the `xorg-x11-drv-qxl-0.0.12-9.el6.x86_64.rpm` file from the **NComputing Support** screen, or from the **RPM Web site.**
4. Select the link:

   ```
   CentOS/RHEL 6: ftp.CentOS.org/6.1/os/x86_64/Packages/xorg-x11-drv-
   qxl-0.0.12-9.el6.x86_64.rpm
   ```

5. Download:

   ```
   ftp.muug.mb.ca:xorg-x11-drv-qxl-0.0.12-9.el6.x86_64.rpm
   ```

6. Install the file inside the CentOS/RHEL 6 Gold image.
7. Run the following commands:

   ```
   yum install spice-vdagent

   chkconfig spice-vdagentd on
   ```

8. Restart the Gold Image. Once the session has started, users can increase their resolution up to 2560 x 1600.

Printing for Linux Guests

Linux Virtual Desktops are configured to print by default. A standard default PostScript printer is configured in CUPS. CUPS is the standards-based, open source printing system developed by Apple Inc. for Mac OS® X and other UNIX®-like operating systems.

The BSD-style `lpr` program must be available. On platforms using the CUPS engine, typically this is available in the `cups-bsd` package. Print to the default printer from a shell using the `lpr` command.

Follow the steps below to install a default printer in the Linux guest:

1. Install the `cups-bsd` package.
2. Ensure that the CUPS service is running.
3. Obtain and install the driver for the printer.
4. Register the printer as the default printer.
5. Run a test print on the client.

In the Gold Image, install the printer according to your guest OS.

DISABLE AUTOMATIC UPDATES ON UBUNTU

Disable automatic updates in the Gold Image so that users are not prompted to update.

1. Select **System** > **Administration** > **Update Manager**.
2. Select the "Settings… "Button.
3. Uncheck the box "Check for updates."

CHAPTER 7

Enabling RDP in Gold Images

This chapter discusses the following.

Define Session Settings to Support RDP

Desktops using RDP may need to use NAT networking, which is the default setting in Session Settings. See Managing Session Settings on p. 51 for more details.

To define session settings to support RDH:

1. From the **Desktop Policy** screen, assign the new session settings to the user(s) who require it.
2. Select "Update" button to save the changes.
3. Start the VERDE User Console to launch the RDP connection.

ENABLING RDP 8.1 FOR WINDOWS 2008 SERVER R2 AND 7 CLIENTS AND GUESTS

RemoteFX-capable RDP, or RDP 8.1, can be used in the guest and on the client. The following are supported:

Client machines:

- Windows 7 32-bit, with SP1
- Windows 7 64-bit, with SP1

An update of RDP in a Windows Gold Image can improve performance, even if the client machine is an older Windows or a non-Windows platform.

Gold Images:

- Windows 7 32-bit, with SP1
- Windows 7 64-bit, with SP1
- Windows Server 2008 R2 Datacenter Edition 64-bit, with SP1

Download and Install the RDP Update

Visit this Windows support site to download the files. After the files are downloaded, perform the following steps:

1. Install the hotfix and the appropriate version of the RDP 8.1 update.
2. Restart the operating system.
3. Open the **Local Group Policy Editor**.
4. Enable the **Remote Desktop Protocol** policy. The setting for this policy is under the following node:

   ```
   Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Remote Session Environment
   ```

5. Restart the operating system. Do not enable UDP transport.

CHAPTER 8

Provisioning a Gold Image Virtual Machine

This chapter discusses the following.

Three types of desktop sessions can be deployed: dynamic, dynamic long-life, and static. These attributes control the lifespan of system data persistence within virtual machines. System data includes the operating system and applications.

DYNAMIC

Dynamic desktops keep all system image changes in transient storage, which gets flushed automatically when the desktops exit a session or the Gold Image changes. This is the default deployment mode.

Normal desktops keep transient changes only until the desktop is shut down. Users will get a fresh copy of the Gold Image each time the session is launched. Changes to the Gold Image are lost after every shutdown.

DYNAMIC LONG-LIFE

Long-life desktops keep the changes until the Gold Image is altered in some way. User changes to the Gold Image are preserved until the Gold Image is updated. This setting is typically used to enable frequent AntiVirus updates without requiring Gold Image changes.

This setting will increase storage requirements.

STATIC

Static desktops are provisioned from a Gold Image and become owned by a user—meaning the user is responsible for all changes to the system areas. They do not inherit changes from the Gold Image the way dynamic desktops do. Static desktops allow users to install their own applications, make system configuration changes, and apply security patches within their virtual machines. It is the virtual world's equivalency to a fully stateful PC. Any security policies applied from the Active Directory on what the user can access within the image still apply.

Important: In a multiple server deployment (cluster), long-life and static desktops use shared storage for the system change deltas. The storage requirements for these deltas are much greater than that for normal (locally stored) delta files.

Deploying a Gold Image Virtual Machine

In the VERDE Management Console, the Gold Image is ready to be published when the installation of the image operation system has completed. If the Gold Image status is **New (Install Complete)**, your next step is to assign the desktop policy, then check in the image.

Important: VERDE Management Console administrator(s) should not be assigned to a Gold Image.

1. On the **Desktop Policy** screen, select "ADD RULE."
2. Enter the user or group to assign and select the Assignment Type as "Gold Image."
3. On the drop-down beside "Gold Image," select the Gold Image to be deployed with this policy.
4. Beside "Select Settings," use the drop-down menu to select the settings where you wish to apply the rule.
5. If it is necessary to restrict access to the Gold Image based on client location or IP address, define a range of addresses in the "Client Address Range" field. The format should be `aa.bb.cc.dd/n` where n is a number between 32 and 1. For example, `170.17.0.0/16`.
6. Under the **Application Layers** tab, you can perform a search to find the application layers in which you want the rule to apply. Choose "Select" next to the application and it will appear in the "Selected" table.
7. Under the "Deployment" column, select the type you'd like to apply to the application. Your options include: the latest, the staging version, or a specific version.
8. Select the **Deployment Modes** tab to choose the deployment mode for this image. Refer to the **Gold Image Deployment Modes** table in this section to learn about the different deployment modes.
9. Choose the deployment types for this image. Refer to the **Gold Image Deployment Types** table in this section to learn about the different deployment types.
10. Select "Save" or "Update."
11. Check in the Gold Image to make it available, then select the deployment types for this image. .

Table 8-1 Gold Image Deployment Modes

Deployment Mode	Description
VDI	Deployed from the VDI server.
BRANCH	Deployed and synchronized to the listed branches.

Table 8-2 Gold Image Deployment Types

Deployment	Description
Normal	Users receive a fresh copy of the Gold Image each time the session is launched. Changes to the system are lost after every shutdown.
Long	User changes to the Gold Image are preserved until the Gold Image is updated. .
Static	User changes to the Gold Image persist after the session shuts down. The user is responsible for all changes to the system areas. Users do not get any Gold Image changes, as with dynamic desktops. Gold Images that are static should not be joined to Active Directory.

DEPLOYMENT MODE, TYPE, AND ACTIVE DIRECTORY

The default deployment mode is VDI. The default deployment type is Normal.

In most instances, deployed Windows Gold Images should be dynamically joined to Active Directory through **Session Settings** in the VERDE Management Console.

For Session Settings information, see Managing Session Settings on pg. 51.

CHAPTER 9

Connecting Users to VERDE

This chapter discusses the following.

Remote users connect to VERDE from the VERDE User Console, the VERDE User Console5, or the VERDE Client.

The User Console supports access to virtual desktops using SPICE and RDP protocols. VERDE secures the remote session with SSL/TLS encryption when applicable.

The VERDE User Console5 contains functionality similar to the standard console, but with the benefit of not requiring additional software to be installed on the client. Only users wanting to connect to a Windows guest session should use the VERDE User Console5 for access; currently, Linux guest sessions are not supported on this platform.

The VERDE Client will be the primary way that end users will access their virtual desktops. The VERDE Client is installed with the VERDE user tools. VERDE provides all of the tools required to enable the client for virtual sessions. The VERDE client is currently the only software client that supports the UXP protocol. The UXP protocol is also available using the NComputing RX-300 thin client. See Starting the User Console on p. 135 for more details.

Confirm the following items are configured to support virtual desktop sessions:

- Enable RDP support in the Windows Gold Images to launch an RDP session from the User Console.
- Advanced RDP features like multimedia redirection and support of multiple monitors are only available with Windows 7 Enterprise or Ultimate Editions.
- The VERDE User Console requires a browser that is Java-enabled. Confirm only one version of the Java Runtime Environment is installed.
- Ubuntu 12.04 client requires installation of the `libjpeg62` package to support SPICE.

CONFIGURING THE FIREWALL FOR THE VERDE USER CONSOLE

User Console connections use outbound ports only—meaning that the client computers themselves can be behind a standard firewall or NAT device. If the VERDE server(s) is also behind a firewall, verify the following ports are open and can route to the appropriate VERDE server(s):

- **8443**. https access to the VERDE Management Consoles.
- **48622/tcp**. VERDE Use Console – RDP and SPICE connections.
- **48642**. Used by the SmartSync protocol (Branch). Previous versions of VERDE used port 48632. Keep this port available in deployments that have been upgraded.

Starting the User Console

After signing into the console, users are able to connect to different Gold Image sessions that have been assigned to them by the administrator. The VERDE User Console can be accessed at one of the following locations:

`http://<server-name-or-IP>:80` or `https://<server-name-or-IP>:443`

Upon accessing one of these locations, the **Login** screen is displayed. If the console is connected to the Active Directory, log in with Active Directory credentials—if not, sign in using the account credentials created on the VERDE Server. Any additional users must be defined in the Gold Image.

Note: A Java plugin is required for viewing the VERDE User Console.

Note: For security reasons, many modern-day browsers no longer support Java Applets. As a result, end-users will not be able to use the VERDE User Console to launch desktops. See **https://java.com/en/download/faq/chrome.xml** for more details.

VERDE User Console5

VERDE also offers an HTML5-based console that can be accessed on the majority of HTML5-ready browsers. The VERDE User Console5 has similar functionality as the VERDE User Console—but unlike the standard console, you won't need to install a Java plugin to launch virtual desktops. Once you select a desktop, the VDI session will open in the browser.

Important: The current version of the VERDE User Console5 only supports RDP protocol, and does not support USB drives functionality.

The VERDE User Console5 is the only available option for VERDE users utilizing a Chromebook client to connect to the VERDE application.

To access the VERDE User Console5, you’ll need to open a browser and navigate to one of the following addresses:

`http://<server-name-or-IP>:8080/uc5` or `https://<server-name-or-IP>:8443/uc5`

Once you’ve navigated to the site, add the appropriate username and password in the fields provided, then select “Login.”

VERDE Client

The VERDE client is an alternative to the VERDE User Console. It is installed with the VERDE Client Software Tools. If you configured VERDE using General Settings, Windows tools and the VERDE Client can be updated automatically.

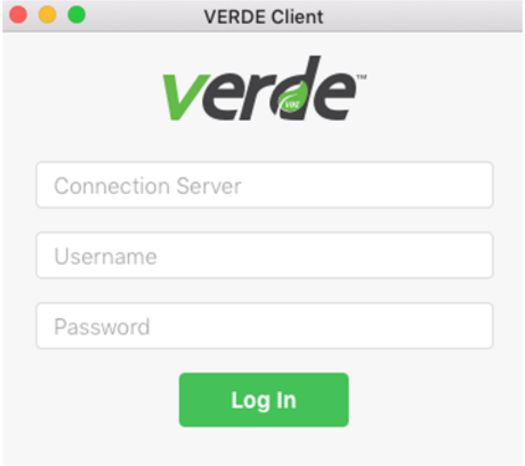
Linux and MAC tools and the client are verified to ensure you're using the latest version.

MAC clients can only run guest sessions from the VERDE Client. Sessions cannot be launched from the VERDE User Console.

USING VERDE CLIENT

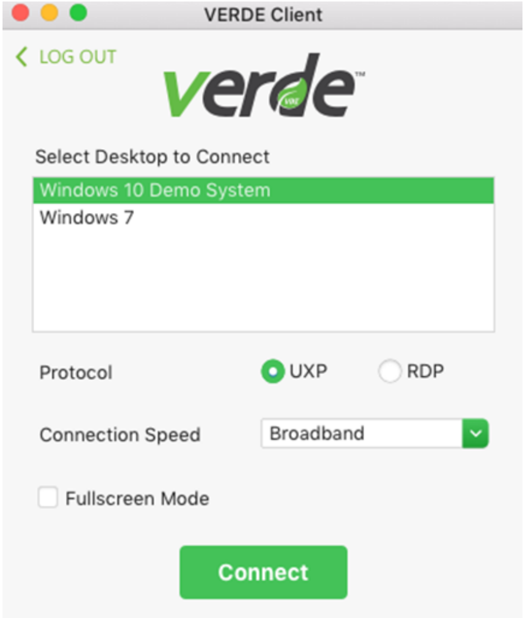
Perform the following steps to launch a desktop from the VERDE Client:

1. After VERDE Client Software Tools are installed on a client machine, double-click the VERDE Client desktop icon.



2. In the field under "Connection Server," enter the URL for the server on which this user can run sessions.
3. Under "Username", enter the username. If the user account resides on an LDAP server, the entry is `user@<name>`, where ,`<name>` is the name specified when the server was added on the LDAP Servers screen.
4. Enter the account password.

5. **For Linux Clients Only**. If you are on a Linux client, you will also see a "Domain" field where you'll need to apply the domain name of the server. You can select a domain name from the drop-down list. If the drop-down list is empty, an administrator will need to run an executable through the command line on the VERDE server to provide domain name options.
6. Select "Login." The desktops that have been assigned to this user will be listed.



Select Desktop to Connect

Windows 10 Demo System
Windows 7

Protocol ● UXP ○ RDP

Connection Speed Broadband

□ Fullscreen Mode

7. Select the desktop to launch. If necessary, adjust the connection speed, fullscreen mode, and the preferred protocol.
8. Select "Login."

CONFIGURING VERDE CLIENT

The VERDE Client can be customized to reflect the preferences of an organization and the default settings displayed to users. For example, the window title and default protocol settings can be configured. The VERDE Client can also be started from the command line with a set of configuration options. Review the table for Installation locations.

Table 9-1 VERDE Client Installation Locations

OS	Command
Linux	`/usr/bin/verde-client`
Windows	`C:\Program Files\VERDE\verde-client.exe`

Type `--help` or `-?` for a complete list of command and configuration options.

Configure Client and Guest Time Zone

The guest session time zone matches that of the client machine if the two are the same operating system type. If the client is a Linux machine, and the guest session is a Windows desktop, or vice versa, a zone name conversion is required.

Microsoft (Windows) clients and guests use Microsoft time zone names, which can be found **here**.

Linux clients and guests use a more standard set of names. You can review them **here**.

VERDE provides a default set of name mappings in `/usr/lib/verde/etc/timezones.txt`, but these might not cover all that are needed in an environment. To customize the zone name mapping, create a`timezones.txt` file in the `.verde` directory in the home directory of the VERDE system account (`vb-verde`). Each line in the file should contain:

`<windows name>|<standard name>` which translates to: **Taipei Standard Time|Asia/Taipei**

Mappings provided by this file take precedence over VERDE mappings.

ANTI-VIRUS SOFTWARE ON THE CLIENT

Anti-virus software may single out VERDE processes as suspicious. To circumvent this event from occurring, add the VERDE process, and any other required processes, to the anti-virus program's trusted list.

For the Windows client, these files include:

```
%ProgramFiles%\VERDE\rdppass.exe

%ProgramFiles%\VERDE\spicec.exe

%ProgramFiles%\VERDE\verde-usb-server.exe

%ProgramFiles%\VERDE\verdeprint.exe

%windir%\system32\vbrusbservicews.exe
```

RDP Connection Scripts

RDP connection scripts can be created to customize the connection settings permanently. These settings include components such as the display size, user experience, and compression.

Sample scripts are provided in:

```
/usr/lib/verde/etc/apache-tomcat/webapps/VIA/verde-scripts
```

The files must be named:

```
rdp-connection-settings

rdc-connection-settings

rdesktop-connection-settings

nx-connection-settings
```

Create a verde-scripts directory in:

```
/home/vb-verde
```

Create and store scripts in this directory. VERDE does not verify that the custom connection script is syntactically correct before it is used. If custom scripts are not present, the User Console will start the session with RDP connection defaults.

CONFIGURING AUTOMATIC LOGOUT FOR THE USER CONSOLE

The auto log out feature closes the VERDE User Console as a security measure. To confirm that a user has logged out of the User Console, perform the following steps:

1. Log into the VERDE Server as root.
2. Change directory to:

   ```
   /usr/lib/verde/etc/apache-tomcat/webapps/VIA/WEB-INF/classes
   ```

3. Edit the `uc.properties` file.
4. Change `logout.ondissconnect = false` to `logout.ondissconnect = true`
5. Restart VERDE Services.

To test the new settings in the User Console, launch several sessions. After you close the last session, the User Console will log out automatically.

In a cluster environment, manually apply this change to each node.

Connections for iPad, iPhone, iPod, and Android

You can use an iPad, iPhone, iPod, or Android clients to access guest sessions by downloading Microsoft RD Client from their app store.

The client makes one Gold Image available to users or groups from a device. To install the client, perform the following steps:

1. From the device, access the Application Store, then select "FREE."
2. Search for and download iFreeRDP or Microsoft RD Client. Select "Install."
3. After the application has finished installing, launch the applet.
4. To connect to a guest session, at a minimum you'll need to add the following information:
   - **Title.** Name of the connection.
   - **Host Name.** The FQDN or IP address of the VERDE server.
   - **Username.** Your username (`user@AD_domain` if it is an Active Directory domain user, `user@0local` if it is a local user). The UPN username must be recognized by the Active Directory. If the LDAP configuration lists a friendly name for the UPN suffix, it must match the UPN suffix understood by the Active Directory.
   - **Password.** The password associated with your username.
   - **Domain.** (optional) If the domain is specified with the username, leave the field empty.
5. Select "Save." You should now be able to access a guest session from the device.

Note: If you already have a session running on a computer and start a session on another device, the original session will shut down.

CHAPTER 10

Administering Virtual Desktops

This chapter discusses the following.

This section discusses updating Gold Images and publishing the changes to users. Notification messages are configured to alert users when changes are made available. Users are then prompted to restart their virtual machine. Notification messages and the frequency of the alerts can be customized. see Customizing the Gold Image Update Notification on pg. 145 for more details.

To learn more about creating a Gold Image, and the check-out and check-in procedures, see Gold Images on pg. 83.

Customizing the Gold Image Update Notification

Update notification messages can be customized by updating the **verde-restart.txt** file for its corresponding language folder. This alert file is read when the Gold Image is checked in which is the use case for when users are notified. The alert message requires users to update their dynamic guest sessions.

CHANGING THE NOTIFICATION MESSAGE

Default output `verde-restart.txt` files are added during the installation of VERDE and available in the following folder: `/usr/lib/verde/etc/alerts/<locale-code>` where the `<locale-code>` corresponds to one of the supported languages listed in the table below.

Table 10-1 VERDE Supported Languages

Local Code	Language
zh_CN	Chinese (Simplified)
zh_TW	Chinese (Traditional)
en	English
fr	French
de	German
it	Italian
pt	Portuguese
es	Spanish

Creating a New Message

In the following example, a source file is created and named `en.txt` to replace the English alert message:

# VERDE alert catalog

[verde-restart]

caption = "VERDE - ALERT MESSAGE TITLE such as ADMINISTRATOR REQUESTS SHUTDOWN"

text =

Enter the text of your new message here.

Generating the New Output Message

Once the edits are complete, process the `en.txt file` through the message creation script, located in:

```
/usr/lib/verde/bin/win4-alert-catalog-preprocess.pl
```

This is a PERL script that generates text according to parameters in the output `verde-restart.txt` file.

Note: The source file can be created in a temporary directory. The script will create a new folder named after the input file name (en) in this directory, then create and add the `verde-restart.txt` file in it.

Script Usage

```
win4-alert-catalog-process.pl [options]
```

Table 10-2 Catalog Process Script Options

Option	Description
-input <catalog>	The source file to process
-output <output-directory>	The folder where to place resulting file

In this example:

```
/usr/lib/verde/bin/win4-alert-catalog-preprocess.pl -input
/home/test/en.txt -output /home/test/
```

The `verde-restart.txt` is created in `/home/test/en`.

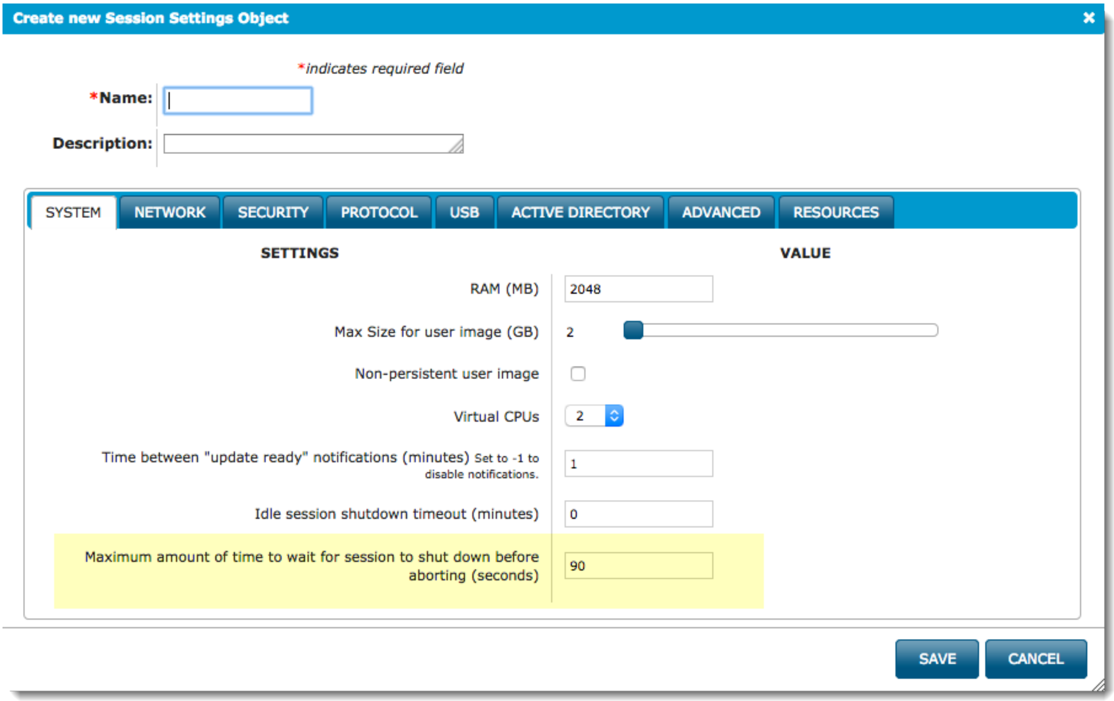
Important: Do not modify the output files. The codes at the top of the file correspond to the length of the alert title or body since they are automatically generated by the script.

Activating the New Notification Message

Save the files to `/usr/lib/verde/etc/alerts/<language>`. File contents display in the guest session after Gold Image check- in.

CHANGING THE FREQUENCY OF THE MESSAGE

1. Log into the VERDE Management Console.
2. Select the **Session Settings** tab on the left panel.
3. On the **Session Settings** screen, select the **System** tab.
4. In the field beside "Time between update ready notifications (minutes)", set the value.
5. Select "SAVE" to save the changes. The changes will take effect after the virtual desktop is restarted.



Create new Session Settings Object

*indicates required field

*Name:

Description:

SETTINGS	VALUE
RAM (MB)	2048
Max Size for user image (GB)	2
Non-persistent user image	□
Virtual CPUs	2
Time between "update ready" notifications (minutes) Set to -1 to disable notifications.	1
Idle session shutdown timeout (minutes)	0
Maximum amount of time to wait for session to shut down before aborting (seconds)	90

Customizing the User Console URL

Change the User Console link to use certain ports accessible through the firewall. VERDE software, by default, uses ports 8080 and 8443 with a self-signed certificate.

The following example illustrates a RedHat Linux user changing the User Console links to ports 80 and 443:

```
/sbin/iptables -t nat -A PREROUTING -p tcp --dport 80 -d <host_ip_address>
-j DNAT --to <host_ip_address>:8080

/sbin/iptables -t nat -A PREROUTING -p tcp --dport 443 -d <host_ip_
address> -j DNAT --to <host_ip_address>:8443
```

BACKING UP THE VIRTUAL DESKTOP AND DATA

If all images and data are stored on a single server, develop a backup plan that makes sense for your environment. In a clustered environment where shared storage is used, the storage device acts as the backup for Gold Images and user profile information. NComputing Professional Services can assist you with your backup planning if needed.

CHAPTER 11

VERDE Management Console Reporting

This chapter discusses the following.

The **Reporting** screen displays information about system components, desktop sessions, and events.

SYSTEM REPORTS

System information includes:

- Local server status
- Branch server status
- Charts
- Events

See System Status Reporting on p. 152 for more details.

USER REPORTS

User information is reported as:

- Live Sessions
- MAC Addresses
- Desktop Usage

See User Session Reporting on p. 154 for more details.

ADMINISTRATION REPORT

Administration is a single table of administrator events.

All reports provide a search capability. The search is dynamic and applies to all fields in the table. Select a search icon to open the Search panel. The System Events and User Events event logs, and the Administration audit log, have multi-field search options.

Data can be exported to a comma separated value CSV file or ELFF on the local desktop. See Administration Report on p. 156 for more details.

System Status Reporting

System status reporting is available for all VERDE Servers.

LOCAL SERVERS

The Local Servers table lists servers, metrics, and status. Select any column in the table to sort by that data set.

Select **TOGGLE ONLINE STATUS** to take a selected server offline.

The following data is available:

- **Server**. Name of the server.
- **Current**. Number of sessions currently running.
- **Reserved**. When a new session is initiated, the server checks the number of available licenses as its workload and reserves a spot for the opening session. The reservation automatically expires if the session does not open.
- **Utilization %**. Percentage of total VERDE system utilization. This value is a guideline and can be used to determine when the system is reaching capacity. It is a combination of CPU load, storage load, and network load based on performance testing using the LoginVSI tool from Login Consultants. A high value may indicate some combination of CPU-bound tasks, I/O-bound tasks, and network load. Even if CPU load is low, the Utilization% may still be high if for example the external storage is slow to respond, or if the internal storage is inadequate for the disk cache. For example, a system running a moderate workload with multimedia applications may show 100% utilization, indicating user responsiveness is unacceptable. This may vary based on the workloads running.
- **Memory %**. Percentage of available memory used. The background of this field changes to yellow when memory use reaches 95% and changes to red when 100% of memory is used.
- **Memory Threshold %**. Percentage of use for triggering the warning in the Memory % field.
- **Status**. Indicates on or offline status.

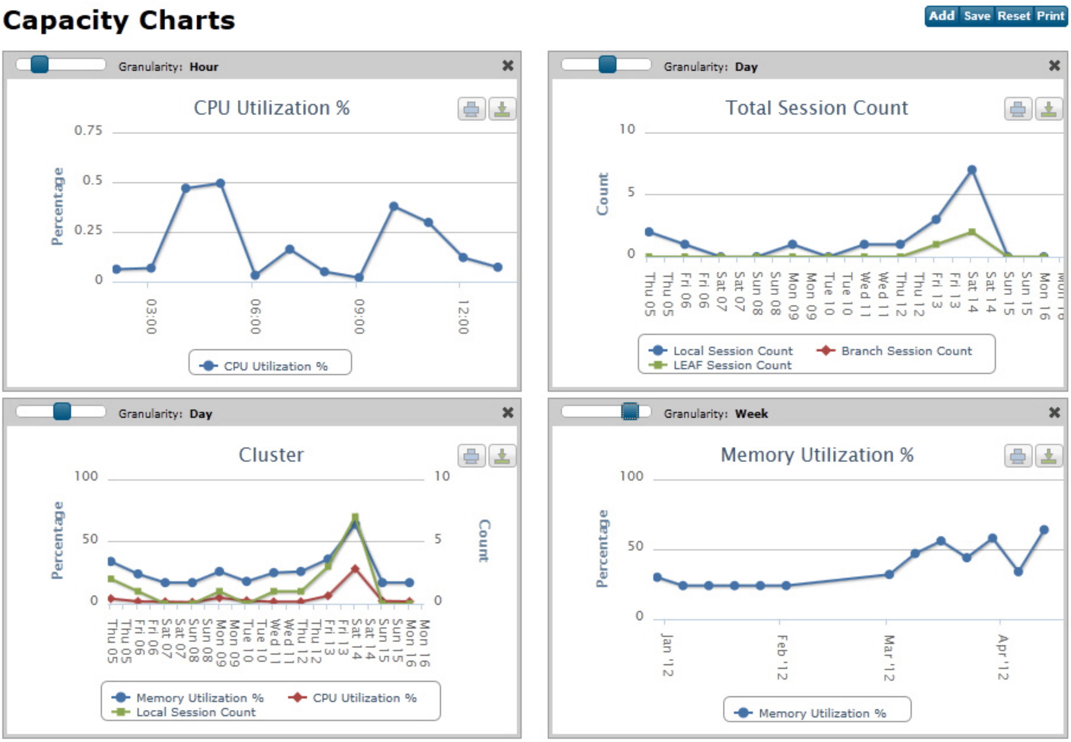
BRANCH SERVERS

The Branch Servers table lists servers, metrics, and status. Select any column in the table to sort by that data set. In addition to the local server settings, the branch server table lists the cluster to which a server is joined and the date and time of the last update from the cluster.

System Charts

Capacity charts show CPU consumption, session counts, cluster, and memory usage. You can perform the following chart functions:

- Use the slider in the upper left corner of each chart to change the granularity of the data from minutes, to hours, days, weeks, or months.
- Pass the cursor over data in the charts to view information about that data point.
- Resize the charts by dragging the vertical resizing bar with your mouse between the two columns of charts.
- Rearrange charts by select and drag the gray area above the title to move the chart.
- Select "Reset" in the upper right corner to move all charts to the original position at the original size.
- Add, save, or print a chart with the buttons in the upper right. To add a chart, select "Add" and select the data to display.



Capacity Charts

Granularity: Hour

Granularity: Day

Granularity: Day

Granularity: Week

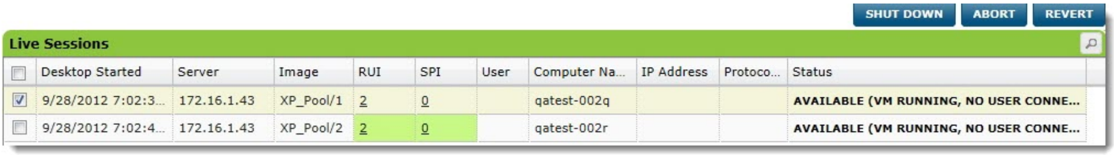
User Session Reporting

Users Sessions can be viewed and shutdown through the different Reporting screens.

LIVE SESSIONS

The Live Sessions table lists guest sessions that are currently active. Review the following to monitor session resource use and performance:

- **Resource Utilization Index**. A representation of virtual machine consumption rates for CPU, memory, Virtual Network, display protocol, and IOPS. These rates reflect relative consumption of server resources, not performance.
- **Session Performance Index**. A performance index of session CPU, RAM, amount of data swapping, system disk use, and user disk use.



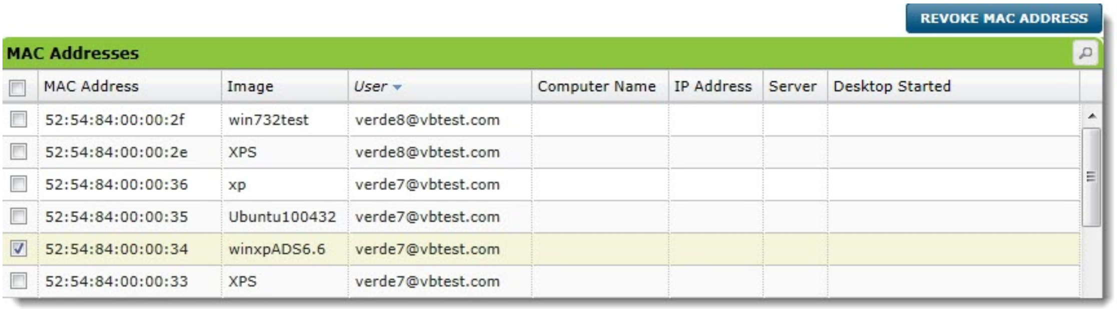
□	Desktop Started	Server	Image	RUI	SPI	User	Computer Na...	IP Address	Protoco...	Status
☑	9/28/2012 7:02:3...	172.16.1.43	XP_Pool/1	2	0		qatest-002q			AVAILABLE (VM RUNNING, NO USER CONNE...
□	9/28/2012 7:02:4...	172.16.1.43	XP_Pool/2	2	0		qatest-002r			AVAILABLE (VM RUNNING, NO USER CONNE...

Sort session data by selecting a column in the table. Two columns are available but are not displayed by default: "Organization" and "MAC Address." To enable them, right-click in any column header to display a menu showing all available columns. Select the ones that are unchecked. Preferences are maintained for each administrator account.

Select a session and pick one of the buttons at the top of the table to perform the following:

- **Shut Down**. Shuts down the session and saves user data.
- **Abort**. Stops the session immediately without saving data.
- **Revert**. Reverts the session image back to its original state. Any changes to the image that were made in this session are lost.

The **MAC Address** screen lists the MAC Addresses that are being used.



MAC Addresses

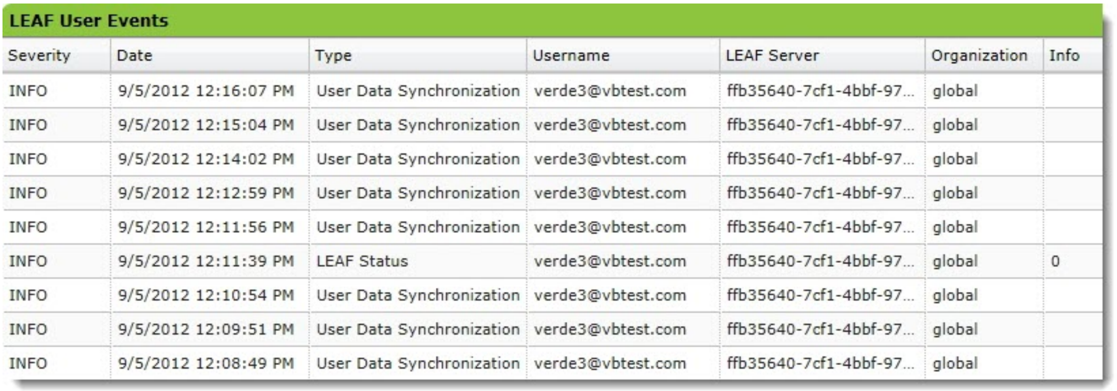
□	MAC Address	Image	User	Computer Name	IP Address	Server	Desktop Started
□	52:54:84:00:00:2f	win732test	verde8@vbtest.com				
□	52:54:84:00:00:2e	XPS	verde8@vbtest.com				
□	52:54:84:00:00:36	xp	verde7@vbtest.com				
□	52:54:84:00:00:35	Ubuntu100432	verde7@vbtest.com				
☑	52:54:84:00:00:34	winxpADS6.6	verde7@vbtest.com				
□	52:54:84:00:00:33	XPS	verde7@vbtest.com				

Select "REVOKE MAC ADDRESS" to make an address available or to return a selected address to a pool.

DESKTOP USAGE

Desktop Usage displays an audit log of desktop use. This report includes the severity of the event, date, type, server, username, Gold Image used, and deployment information.

Select any table title to sort information by that data type.

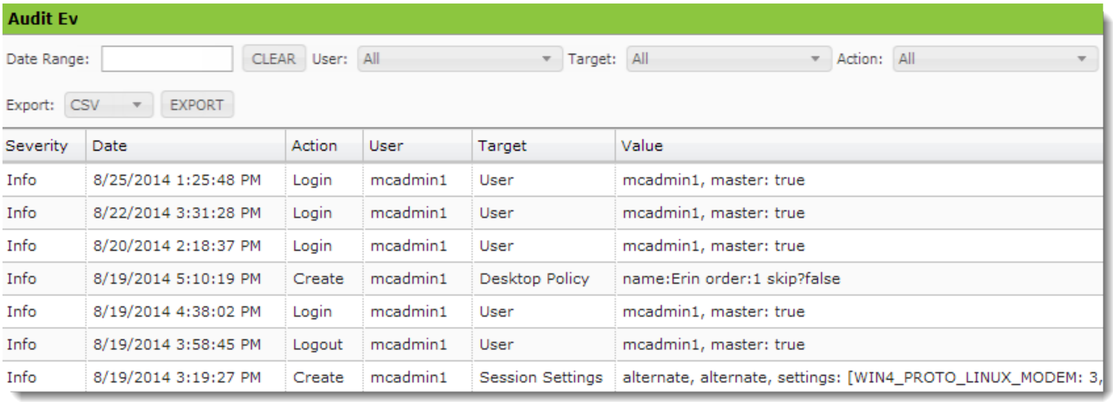


LEAF User Events

Severity	Date	Type	Username	LEAF Server	Organization	Info
INFO	9/5/2012 12:16:07 PM	User Data Synchronization	verde3@vbtest.com	ffb35640-7cf1-4bbf-97...	global	
INFO	9/5/2012 12:15:04 PM	User Data Synchronization	verde3@vbtest.com	ffb35640-7cf1-4bbf-97...	global	
INFO	9/5/2012 12:14:02 PM	User Data Synchronization	verde3@vbtest.com	ffb35640-7cf1-4bbf-97...	global	
INFO	9/5/2012 12:12:59 PM	User Data Synchronization	verde3@vbtest.com	ffb35640-7cf1-4bbf-97...	global	
INFO	9/5/2012 12:11:56 PM	User Data Synchronization	verde3@vbtest.com	ffb35640-7cf1-4bbf-97...	global	
INFO	9/5/2012 12:11:39 PM	LEAF Status	verde3@vbtest.com	ffb35640-7cf1-4bbf-97...	global	0
INFO	9/5/2012 12:10:54 PM	User Data Synchronization	verde3@vbtest.com	ffb35640-7cf1-4bbf-97...	global	
INFO	9/5/2012 12:09:51 PM	User Data Synchronization	verde3@vbtest.com	ffb35640-7cf1-4bbf-97...	global	
INFO	9/5/2012 12:08:49 PM	User Data Synchronization	verde3@vbtest.com	ffb35640-7cf1-4bbf-97...	global	

Administration Report

This report lists audit events for the system. Select the "Search" icon at the top of the table to filter by entered criteria. Data can be sorted by selecting a column inside the table.



Severity	Date	Action	User	Target	Value
Info	8/25/2014 1:25:48 PM	Login	mcadmin1	User	mcadmin1, master: true
Info	8/22/2014 3:31:28 PM	Login	mcadmin1	User	mcadmin1, master: true
Info	8/20/2014 2:18:37 PM	Login	mcadmin1	User	mcadmin1, master: true
Info	8/19/2014 5:10:19 PM	Create	mcadmin1	Desktop Policy	name:Erin order:1 skip?false
Info	8/19/2014 4:38:02 PM	Login	mcadmin1	User	mcadmin1, master: true
Info	8/19/2014 3:58:45 PM	Logout	mcadmin1	User	mcadmin1, master: true
Info	8/19/2014 3:19:27 PM	Create	mcadmin1	Session Settings	alternate, alternate, settings: [WIN4_PROTO_LINUX_MODEM: 3,

CHAPTER 12

VERDE Dynamic Network Configuration

This chapter discusses the following.

VERDE Dynamic Network Configuration assigns static network parameters to dynamic virtual desktop environments. For example, permissions or policies may need to be configured for given desktops by specifying their computer names, IP addresses, or MAC addresses. This file enables VERDE to work with these assigned values. Common uses include:

- **Support application access restricted by IP address**. Assign static IP addresses to dynamic virtual desktops using bridged networking without requiring a DHCP server or static MAC address assignment.
- **Support Windows workgroup functions requiring static computer names (network scanners, etc.)**. Assign static Windows computer names to dynamic virtual desktops using bridged networking.

Note: Dynamic Network Configuration is currently limited to Windows virtual desktop environments . For both computer name and IP address, the netcfg settings overwrite Session Settings.

Dynamic Network Configuration Process

VERDE runs an agent inside Windows virtual machines that automatically performs dynamic network configuration.

If specified, it assigns any IPv4 parameters for the session as well as a Windows Computer Name, and the virtual desktop will join the Active Directory domain.

After the virtual desktop joins the domain, it will reboot twice. The first reboot displays a Windows login credentials screen. Windows is trying to login with an Active Directory account when the virtual session has not yet joined Active Directory. The session will restart within a few seconds.

Note: There may be a delay on the credentials screen as the session joins the domain.

A virtual desktop goes through the domain join procedure described above every time the Gold Image is updated. If the Gold Image is updated, the delta file is no longer valid. The next time the dynamic desktop starts, it must join the domain again.

Creating a CSV Map

VERDE Dynamic Network Configuration uses a CSV file to map dynamic virtual desktops to specific network configurations. Create this file and import it into the VERDE Management Console.

Note: Fields must be separated with a comma. Use of spaces or other characters will cause the file to fail. The last three fields are being deprecated, the domain name, administrator and password should be left blank (do not remove the comma separators). The information to join the domain is not set in the netcfg file anymore, it is done in the Session Settings in the VERDE Management Console.

Table 12-1 Fields for netcfg.csv file Configuration

Field	Description
<user>	The user name or Linux user ID of the user receiving the virtual desktop. This is case sensitive.`<username@<LDAP_Alias>@<org-ID>` Where <LDAP_Alias> is set in the LDAP server definition in the VERDE Management Console and <org-ID> is the id attributed to a new organization (the ID column in the Organization screen).For a user "joe," AD domain "addomain.com," belonging to an organization with LDAP server name "Org1-AD" (org-ID: org-7), the user syntax is:`joe@Org-AD@org-7`To only set the computer name to "Test-Netcfg-01" for that user starting the desktop "Win7-32", the entry would look like:`joe@Org1-AD#org-7,Win7-32,,,,Test-Netcfg-01,,,`
<gold-image>	The image name of the virtual desktop, as defined in the VERDE Management Console. This is case sensitive.
<ip-address>	The IPv4 address to set for the session, if using bridged networking.
<netmask>	The IPv4 network mask to set for the session, if using bridged networking.
<gateway>	The IPv4 default gateway to set for the session, if using bridged networking.
<Computer-Name>	The Windows Computer Name to set for the session, up to 15 characters in length (longer names are automatically truncated).
<domain>	The fully qualified Active Directory domain name (domain.company.com). This setting is Deprecated. The VERDE server should still have the domain controller as the primary DNS. The guest still uses that in NAT mode.
<domain-admin>	The Active Directory domain administrator who can join computers to the domain. Type the domain name in capital letters when specifying users, such as `AUS\verde1`**.** This setting is Deprecated.
<domain-password>	The Active Directory domain administrator's password, in plain text format. This setting is Deprecated.

For example, to assign the image **winxp** for the user **xpuser** to IPv4 parameters:

- **IP Address**. 192.168.10.5
- **Network Mask**.255.255.255.0
- **Default Gateway**. 192.168.10.1
- **Windows Computer Name**. xpuser-winxp
- **Active Directory domain**. ad.corp.com

- **Domain administrator**. admin
- **Domain password**. password

The row in the `netcfg.csv` file would look like:

```
xpuser,winxp,192.168.10.5,255.255.255.0,192.168.10.1,xpuser-winxp,ad.-
corp.com,admin,password
```

To perform the same assignment but without IPv4 parameters (defaults to DHCP):

```
xpuser,winxp,,,,xpuser-winxp,ad.corp.com,admin,password
```

To perform the same assignment but without joining the Active Directory domain:

```
xpuser,winxp,192.168.10.5,255.255.255.0,192.168.10.1,xpuser-winxp,,,
```

Note: Blank fields must still be separated by commas. Improperly formatted rows are ignored.

GENERAL RULES

The VERDE Server must have the IP address of the Windows Domain Controller as the first name entry in the /etc/resolv.conf file; for example:

```
# ***** resolv.conf *****

search ad.corp.com

nameserver 192.168.1.111 (IP address of Windows Active Directory server)

nameserver 24.93.41.115

nameserver 24.93.41.116
```

IPv4 parameters are only recognized if using bridged networking.

In order to join Active Directory, all three parameters (FQDN, domain administrator user name, and domain administrator password) must be correctly listed.

The user name and image name are case sensitive. Windows fields are generally not case sensitive unless required by the domain controller.

There is no limit to the number of rows in the CSV file.

BRANCH DEPLOYMENT

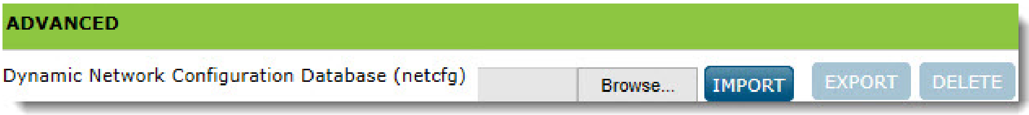
By default, the `netcfg.csv` file is not synchronized with VERDE branch servers. This is for security reasons, as the file contains administrator login information.

To enable the branch and branch server synchronization, add the `VERDE_BRANCH_SYNC_NETCFG=1` settings line to the `/home/vb-verde/.verde-local/settings.cluster` file.

Importing the netcfg.csv File

To import the `netcfg.csv` file:

1. Login to the VERDE Management Console.
2. Select **Configuration > General Settings**.
3. In the **Advanced** section, select "Browse" and locate the `netcfg.csv` file.
4. Select "Import."



ADVANCED

Dynamic Network Configuration Database (netcfg)

5. Select "Export" to export the `netcfg.csv` file to the local machine.

APPENDIX

Troubleshooting

This chapter discusses the following.

NComputing

Log Files

Log files are an essential way to investigate issues you may be having with performing certain VERDE tasks. The following topics discuss different aspects of log files.

ENABLE LOGGING

By default, logging is enabled at the "note" level. To change the logging level, edit the server logging level in the `/var/lib/verde/settings.node` configuration file. The VERDE services will immediately start logging in the new log level; however, the guest image(s) must be restarted for the new log level to affect them.

LOG FILE TABLE

VERDE provides several ways to log system information. Individual logs are available for each functional area of the system

Table 13-1 Log Files

File Name and Location	Description
`/home/vb-verde/logs/<ServerIP>-mc.log`	This is the main Console log and is rolled every day into a new file. It is safe to delete log files that are older than the current date, unless they are needed.
`/home/vb-verde/logs/<Server IP>-audit.log`	This is the VERDE Management Console administrator activity audit trail.
`/var/log/verde/1`	Server log activity. (By default logging is enabled at the "note" level. When the server restarts, a new set of log files will be created and the old ones will be moved to /var/-log/2.)
`/var/log/verde/1/vbbranch.txt`	The branch server activity log file.
`/var/log/verde/1/vbsmartd.txt`	Information relating to the VDI server's branch synchronization.
`/var/log/verde/1/verdecmd.txt`	Information relating to VERDE Cluster Master activity
`/var/log/verde/1/win4prod.txt`	Information relating to VDI sessions running on the server being used.

File Name and Location	Description
/var/log/verde/1/verdempcd.txt	Information relating to SPICE, RDP, and NX VDI connections.
/var/log/verde/1/win4-autobr.txt	Information relating to configuration of the host-side network bridges.
/var/log/verde/verde-network/verde-menu-log.txt	Complete trace of VERDE Menu actions and any networking problems or failures for a new VERDE installation. Also contains information if verde-support-report fails.
/var/log/verde/verde-network/verde-tap-control-log.txt	Information generated by the verde-tap-control executable when called by win4prod to set up and take down virtual guest sessions.
/home/vb-verde/verde-orgs/org-XX/users/<domain>/<user>/<gold-image>/win4.txt	Contains the Gold Image information logged during the session.
/var/log/verde/verde-network/rc.vb-ovs-network-log.txt	Contains a log of network startup and shut-down events.
/var/log/verde/verde-network/verde-auto-config-log.txt	Contains deployment automation related messages.
Windows 7, 8.1, and Windows 2008 Server R2: C:\Users\<local-user>\AppData\Local\Temp verde-client.txt Linux : /home/<local-user>/VIA.log	User Console log file. *This file is located on the client (the computer where the User Console runs), not on the guest.*
VIA.log: /home/vb-verde/logs/<server>-VIA.log	This log file may be useful for issues when connecting to the VERDE server from the VERDE User Console.
Catalina/Tomcat log files:/var/lib/verde/mc/catalina.<date> .log/var/lib/verde/mc/tmp/catalina.out	This log file may be useful for issues when connecting to the VERDE Management Console (http://<Server IP>:8080/mc), such as http 500 and 404 errors. Every day and when VERDE restarts, catalina.out is saved as catalina.<date>.log in the /var/lib/verde/mc/ folder.

Changing the Debugging Level

If the “note” level does not provide enough information, it is possible to change the level of details provided in the log files.

Edit these settings in the `/var/lib/verde/settings.node` file.

Add this command:

```
WIN4_DBG_MOD_ALL="info"
```

Table 13-2 Debug Levels

Level	Description
note	Default mode. Intended to trace the main events in the execution of the system. The note logging level is a good debugging starting point.
info	Includes the note logging level plus some moderate levels of debugging information.
debug	The debugging level that provides the most details.

The “info” and “debug” levels are intended for use only during the debugging process. These levels can cause the log files to get large.

VERDE SUPPORT REPORT

The VERDE support report collects system information and all log files and generates a `.tar` or `.zip` file. The report can be generated from the VERDE Menu or from the command line:

```
/usr/lib/verde/bin/verde-support-report
```

Use `--help` for options.

If saved to removable media, the support report files are uniquely named with the host name or IP of the server, date, and time stamp that the snapshot was taken, such as:

```
VERDE-Support-Report-<hostname>-<date_stamp>-<time_stamp>.tgz
```

Administration Issues

The following topics discuss issues or limitations you may come across as a VERDE administrator, and solutions or workarounds to fix the issue. Because many issues run across different tasks, if you don't find a particular issue you're searching for, please refer to a different section.

REMOVING ORGANIZATION FILES FROM SHARED STORAGE

When an organization is deleted from the VERDE Management Console, a confirmation is displayed with the location of the organization's files. These files should be deleted manually.

To delete the files, perform one of the following tasks:

- If using CIFS for VERDE, browse the CIFS share from any computer in the network with an account that has read, write, and delete access. Delete the path listed in the VERDE Management Console confirmation message, for example: `verde-orgs/org-21`.
- If using NFS for VERDE or using a single VERDE node, open a secure shell into the VERDE server, and run the following command with root privileges:

  ```
  rm -rf /home/vb-verde/<path>
  ```

  where <path> is the path listed in the VERDE Management Console confirmation message.

The following table contains known issues users have reported when accessing a virtual session, and possible solutions to these issues.

Remote Connection Problems and Solutions

Table 13-3 Remote Connection Problems and Solutions

Issue	Solution
Client cannot connect.	Confirm the firewall is configured to allow TCP connect to the VERDE server.
Client cannot print.	If using a Windows client, confirm Adobe Acrobat Reader is installed on the client platform. If you are using a Linux client, confirm a default printer is specified on the client and that the client can print.

Issue	Solution
Remote virtual desktop cannot access shared folders on client.	1. Confirm that the client can be reached from the server. If it is behind a network router and not visible on the Internet, it will not work. 2. Share the folder on the client with the appropriate permissions. From the guest, connect to the client to access the share using the following path: `\\<client_IP>\SharedFolder`
Remote virtual Linux desktop does not resize properly (for example, the menu bar or task bar is off the client screen).	The user may have manually set the screen resolution within the guest. Perform each of the following tasks in the order shown until the issue is resolved:- Close the client session, reconnect, reauthenticate, and launch the guest session again. - In the guest session, remove the directory `$HOME/.gconf/desktop/gnome/screen`, or the file `$HOME/.config/monitors.xml`, and restart the guest session.- Instruct users to never manually set the screen resolution in the guest.
Virtual machine does not shutdown.	This could be caused by antivirus software. If antivirus software is enabled, stop the process to enable shutdown of the session. To prevent it from happening, remove scanning of floppy drives in the Gold Image.
When running a Windows 7 guest on a Linux client and attempting to access the USB share to write inside a folder, a permissions error displays and the USB share breaks.	This is caused by a bug in rdesktop which is fixed with patch `fix-2022945.patch` available from SourceForge.net.

UBUNTU CLIENT DOES NOT CONNECT RDP TO WINDOWS GUEST

Product Version	VERDE
Host/Server	RHEL/CentOS 6.5
Guest/Image	Any Windows
Client/Workstation	Ubuntu
Issue Description	**Steps to replicate**: 1. Install the VERDE client on an Ubuntu 12.04 client workstation. 2. Start the VERDE client. 3. Log in as a user and launch a guest using RDP. **Expected Result**: The session should start without incident. **Actual Result**: The UI will show that it is connected for approximately five (5) seconds before disconnecting again. The RDP Windows session is never seen.
Solution	Remove all versions of FreeRDP from the client, then download and install » libfreerdp1_1.0.2-2ubuntu1_amd64.deb from **https://launchpad.net/ubuntu/+source/freerdp/1.0.2-2ubuntu1**. » freerdp-x11_1.0.2-1ubuntu1_amd64.deb from **https://launchpad.net/ubuntu/trusty/amd64/freerdp-x11/1.0.2-1ubuntu1**
Note	N/A

INDEX