Technical Support
See the Support Web site for technical updates, additional warranty information and documentation, and software revisions:
Web:  http://www.clearcube.com/support/
Email: support@clearcube.com
Phone:  (512) 652-3400
             (866) 652-3400

ClearCube Technology, Inc.
1505 Volta Drive, Suite 100
Cedar Park, TX 78641
E-mail     info@clearcube.com
Phone:  (512) 652-3500 or call toll free (866) 652-3500
Alternatively, contact your local ClearCube Reseller or Authorized Service Provider.

Copyrights
© 2018 ClearCube Technology, Inc. All rights reserved. Under copyright laws, this publication may not be reproduced or transmitted in any form, electronic or mechanical, including photocopying, recording, storing in an information retrieval system, or translating, in whole or in part, without the prior written consent of ClearCube Technology, Inc.
This information is subject to change without notice and ClearCube shall not be liable for any direct, indirect, special, incidental or consequential damages in connection with the use of this material.

Trademarks
ClearCube® and Sentral® are trademarks or registered trademarks of ClearCube Technology, Inc.
Adobe PDF is a registered trademark of Adobe Systems Incorporated in the United States and/or other countries. Catalyst, Cisco, and Cisco Nexus are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Intel, Intel Core, Pentium, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Microsoft, Windows, and Windows Vista are registered trademarks of Microsoft Corporation in the United States and/or other countries. Oracle and Java are registered trademarks of Oracle and/or its affiliates. PCIE and PCIe are registered trademarks and/or service marks of PCI-SIG. PCover-IP and PCoIP are registered trademarks of Teradici Corporation in the United States and/or other countries. Raspberry Pi is a trademark of the Raspberry Pi Foundation. Realtek is a trademark of Realtek Semiconductor Corporation. Red Hat, Red Hat Enterprise Linux, the Shadowman logo and JBoss are registered trademarks of Red Hat, Inc. in the U.S. and other countries. Ubuntu and Canonical are registered trademarks of Canonical Ltd. VMware and VMware View are trademarks or registered trademarks of VMware, Inc. in the United States and/or other jurisdictions. Other product and company names mentioned herein are trademarks or trade names of their respective companies.

Patents
Direct all inquiries about patented technology to ClearCube Corporate Headquarters.
Contents

1: Introduction .................................................................................................................................................. 1

2: New in ClearCube Sentral 6.9.6 .................................................................................................................... 2

3: Requesting a Sentral License Key .............................................................................................................. 2

4: Minimum Requirements and Support ......................................................................................................... 3

5: Installation Prerequisites ............................................................................................................................. 4
   5.1: Overview.................................................................................................................................................. 4
   5.2: Choosing and Configuring a Sentral Database ....................................................................................... 5
   5.3: For Deployments Using Microsoft IIS .................................................................................................. 6
   5.4: Enabling Endpoint Devices for Remote Access ..................................................................................... 6
      5.4.1: Enabling Remote Control of Endpoints from Sentral Console .................................................... 6
      5.4.2: Enabling RDP ...................................................................................................................................... 7
   5.5: Configuring Network Ports .................................................................................................................... 7
   5.6: Virtual Machine Snapshots ................................................................................................................... 8

6: Installing Sentral ........................................................................................................................................... 9

7: Starting Sentral Console ................................................................................................................................. 15

8: Using the Sentral Administrator Account .................................................................................................. 15

9: Sentral Configuration Options ................................................................................................................... 16
   9.1: Using the Configuration Wizard ........................................................................................................... 16
   9.2: Using the Configuration Screen.............................................................................................................. 18
   9.3: Email Configuration .................................................................................................................................. 19
   9.4: Server Configuration ............................................................................................................................... 20
   9.5: TLS Configuration ................................................................................................................................... 21
      9.5.1: More about TLS in Sentral ................................................................................................................. 21
      9.5.2: Generating a Private Certificate ...................................................................................................... 22
      9.5.3: Exporting a Public Certificate from a Private Certificate .............................................................. 22
      9.5.4: Uploading Certificates to Sentral .................................................................................................... 22
   9.6: Alert Configuration .................................................................................................................................. 23
   9.7: FTP Configuration .................................................................................................................................... 24
   9.8: Database Configuration ........................................................................................................................... 25
   9.9: Discovery Configuration ........................................................................................................................... 26
   9.10: System Configuration ............................................................................................................................ 28
   9.11: Dashboard Configuration ....................................................................................................................... 29
   9.12: Security Groups Configuration ............................................................................................................. 29
10: Apply Your Sentral License Key ................................................................. 37
11: Server Log and Settings ........................................................................ 38
  11.1: Log Location .................................................................................. 38
  11.2: Turning off Logging ...................................................................... 38
12: Backups after Initial Configuration .......................................................... 39
  12.1: Backing up Sentral Server and Sentral Console ......................... 39
  12.2: Backing up Sentral Database Schema ....................................... 39
  12.3: Backing up Virtual Machines and Snapshots ....................... 40
13: Preparing Sentral Endpoint Devices ......................................................... 41
  13.1: Installing Sentral Host Agent ....................................................... 41
    13.1.1: Windows ............................................................................. 41
    13.1.2: Red Hat Enterprise Linux (RHEL) .................................. 43
    13.1.3: Ubuntu ............................................................................... 45
  13.2: Installing Sentral Thin Client Agent ........................................... 45
    13.2.1: Windows Operating Systems .......................................... 46
    13.2.2: Linux-Based Operating Systems ..................................... 48
14: Basic Operations ...................................................................................... 49
  14.1: Integrating VMware vCenter Server ......................................... 49
  14.2: About the Virtualization Wizard ............................................... 49
    14.2.1: Creating a Cluster ............................................................. 50
    14.2.2: Modifying or Deleting a Cluster ....................................... 51
  14.3: Creating VM Pools ....................................................................... 51
    14.3.1: Adding a Hypervisor ............................................................. 51
    14.3.2: Verify Connection to Hypervisor ....................................... 52
    14.3.3: Viewing Hypervisor Details: Components and Storage Capacity ............................................................................. 52
    14.3.4: Creating VM Templates ....................................................... 52
    14.3.5: Creating VM Pools ............................................................... 55
  14.4: Device Discovery ............................................................................ 57
14.5: Hierarchical Tree and Right-Click Management Options ........................................... 58
  14.5.1: Blade with PCoIP Host Card .................................................................................. 60
  14.5.2: Zero Clients ............................................................................................................ 60
14.6: Search Options ............................................................................................................. 62
14.7: Creating Groups and Subgroups (Required for All Management Tasks) ...................... 62
14.8: Configuring Endpoints Using Client Profiles ............................................................... 63
  14.8.1: About Client Profiles ............................................................................................. 63
  14.8.2: Default Client Profiles ......................................................................................... 63
  14.8.3: Creating Profiles ................................................................................................... 63
  14.8.4: Apply a Profile to a Group ..................................................................................... 64
  14.8.5: View the Profile Applied to a Device ....................................................................... 64
14.9: Renaming Zero Clients (I/Ports) .................................................................................. 65
14.10: Discovering and Adding Device Users ..................................................................... 65
  14.10.1: Specifying the User Type to Discover ................................................................. 65
  14.10.2: Discovering Users ............................................................................................... 67
  14.10.3: Adding a User to Sentral ..................................................................................... 67
  14.10.4: Adding a Large Number of Users ....................................................................... 68
14.11: About Allocations and Allocation Types .................................................................... 70
14.12: Creating Allocations (Mapping Devices and Users) .................................................. 71
  14.12.1: Creating Device-Based Allocations ..................................................................... 71
  14.12.2: Creating User-Based Allocations ....................................................................... 72
  14.12.3: Allocating Client or User Groups to Device Groups .......................................... 73
14.13: Recording Device-Related Information (Equipment History) .................................... 73
15: When Users Move from One Location to Another .......................................................... 74
16: Updating PCoIP Host Card and Zero Client Firmware ..................................................... 75
  16.1: Uploading Files ....................................................................................................... 75
  16.2: Monitoring Progress and Restarting Devices ............................................................ 75
17: Creating Custom Views in Sentral .................................................................................. 76
18: Additional Logging .......................................................................................................... 78
  18.1: Viewing Sentral Activity (View All Logging Screen) ................................................ 78
  18.2: PCoIP Events Log ..................................................................................................... 78
19: Generating Reports ........................................................................................................ 80
  19.1: Connection History .................................................................................................. 80
  19.2: Inventory Report ...................................................................................................... 81
  19.3: Report Scheduler ...................................................................................................... 82
19.4: Alerts Report .................................................................................................................. 82
19.5: Equipment History ........................................................................................................... 83
19.6: Device Accessibility ......................................................................................................... 83
19.7: Profile Application Status ................................................................................................. 83
20: Sentral Alerts ...................................................................................................................... 85
   20.1: Viewing Alerts .............................................................................................................. 85
   20.2: Creating Alerts ............................................................................................................ 86
       20.2.1: About Alerts That Monitor Multiple Conditions .............................................. 86
       20.2.2: About Evaluation Parameters ............................................................................ 86
       20.2.3: Using the Shutdown and Restart Actions in Alerts ...................................... 87
       20.2.4: Creating a New Alert ....................................................................................... 87
       20.2.5: Using Scripts in Custom Alerts and in Automated Actions ......................... 88
   20.3: Deploying Alerts ......................................................................................................... 90
   20.4: Viewing Deployed Alerts ............................................................................................ 91
   20.5: Modifying Alerts ....................................................................................................... 92
       20.5.1: Modifying Alerts that Monitor a Single Condition ...................................... 92
       20.5.2: Modifying Alerts that Monitor Multiple Conditions .................................. 92
   20.6: Removing Alerts from Sentral Console ...................................................................... 93
21: Client Profile Field Descriptions ..................................................................................... 94
   21.1: PCoIP Profile Fields .................................................................................................... 94
   21.2: Thin Client Agent Profile Fields ............................................................................... 98
22: Troubleshooting .............................................................................................................. 108
   22.1: Console Response Issues ......................................................................................... 108
   22.2: Server Performance Is Slow or Server Is Not Responding ................................... 108
   22.3: Sentral Errors and Messages ................................................................................... 108
23: Important Account Information ....................................................................................... 109
<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.06.20.2012</td>
<td>06/21/2012</td>
<td>First release, details installation steps and configurations necessary for initial setup and preliminary configuration</td>
</tr>
<tr>
<td>1.1.08.29.2012</td>
<td>08/29/2012</td>
<td>Updated contact information, Included content for IIS support, Additional detail about permissions required during installation, Added details about Database Server installation, Added installation Troubleshooting information</td>
</tr>
<tr>
<td>1.2.01.23.2013</td>
<td>01/23/2013</td>
<td>Updated for release 6.8, Noted performance improvements constituting this release</td>
</tr>
<tr>
<td>2.0.07.30.2013</td>
<td>07/30/2013</td>
<td>Updated for release 6.9</td>
</tr>
<tr>
<td>2.1.02.24.2014</td>
<td>02/24/2014</td>
<td>Updated for release 6.9.3, Added SNMP configuration content, Added log performance and configuration content, Added Windows® and Linux® Host Agent, Thin Client Agent content</td>
</tr>
<tr>
<td>2.2.08.06.2014</td>
<td>08/06/2014</td>
<td>Updated content about requesting a Sentral® License Key</td>
</tr>
<tr>
<td>2.3.10.02.2015</td>
<td>10/02/2015</td>
<td>Updated for release 6.9.5, Added installation prerequisites, Revised Sentral installation, Revised Sentral Administrator account content, Added content for Windows Authentication mode for MS SQL database, Added Sentral Configuration Wizard and Configuration Screen content, Added SNMP configuration content, Added Dashboard configuration content, Revised user discovery, Added new Sentral logging content, Added VM Pool content, Added new Client Profile content, Added Sentral Reports content, Added Sentral Alerts content, Added new PCoIP Profile tables, Added new Thin Client Agent Profile tables</td>
</tr>
<tr>
<td>2.4.09.05.2018</td>
<td>09/05/2018</td>
<td>Updated for release 6.9.6, Noted performance improvements constituting this release, Removed support for MySQL, Added new Configuration Wizard &gt; Miscellaneous section content (Primary and Secondary switchover, Allocation content), Added new virtualization options, vCenter Server integration, clustering, Added new shared grouping options, Added new security (TLS) content, Changed ISO Country Code URL</td>
</tr>
</tbody>
</table>
This Page Is Intentionally Blank
1: Introduction

ClearCube® Sentral® 6.9.6 gives IT administrators one console to monitor and control their entire deployment of local and remote computing assets: hypervisors, virtual machines, physical hosts (blades and traditional computers), thin clients, and zero clients. Sentral builds on six generations of ClearCube management software with many innovative new features. It delivers proven cost reductions through unique features such as dynamic resource allocation, virtual desktop management, active health monitoring, and host management. Sentral offers these benefits across platforms, with support for other vendors’ host systems. Designed to scale from small businesses to large enterprises, ClearCube Sentral gives IT departments total control.

The picture below shows the Sentral architecture, where all Sentral components are installed on individual computers.

*Figure 1. Sentral Architecture Components*
2: New in ClearCube Sentral 6.9.6
The list below shows new features in this Sentral release.

- **Support for new ClearCube hardware**
  Support for new ClearCube Blade PCs, workstations, servers, thin clients, and zero clients.

- **Virtualization with multiple hypervisors**
  Sentral can now create and manage virtual machine pools for different hypervisors in your environment.

- **Virtualization Wizard**
  The Virtualization Wizard enables Administrators to add vCenter information to Sentral, import hypervisor information, use clusters to group hypervisors in resource pools, and use a VM as a golden image to create VM pools.

- **TLS Configuration**
  Administrators can now provide Public and Private certificates from the Configuration Wizard to implement TLS (Transport Layer Security) in an environment.

- **Additional security with PCoIP**
  When implemented, PCoIP® clients and hosts use TLS.

- **Upgraded Java and Apache Tomcat services**
  Sentral supports Java™ 1.8.171 and Apache Tomcat® 9.10.

- **High Availability**
  Deployments can now include a secondary Sentral Server, and Administrators can configure thresholds for high availability settings.

3: Requesting a Sentral License Key
Contact ClearCube Support for a Sentral license.

**Email:** support@clearcube.com

**Phone:** (866) 652-3400

**NOTE:** You must apply a license within 60 days of installing Sentral. Sentral documentation details how to apply a Sentral license.

**Next step:** Apply the license key after installing Sentral Console. See **10: “Apply Your Sentral License Key”** below for instructions.
# 4: Minimum Requirements and Support

The table below shows minimum requirements for Sentral components, supported operating systems, and supported VM host applications.

**Table 1. Minimum requirements for Sentral components and supported software**

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirements and Supported Items</th>
<th>Recommended or Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sentral Console</td>
<td>2.4 GHz processor, Intel Core™ i7 1st generation or higher, Xeon® 3400 series (4 cores) or higher, 1 GB RAM, 8 GB RAM or higher, 2 GB free space, Windows® 2012 R2 64-bit Server VM</td>
<td></td>
</tr>
<tr>
<td>Sentral Server</td>
<td>2.4 GHz processor, Intel Core™ i7 1st generation or higher, Xeon® 3400 series (4 cores) or higher, 1 GB RAM, 8 GB RAM or higher, 2 GB free space, Windows 2012 R2 64-bit Server VM</td>
<td></td>
</tr>
<tr>
<td>Sentral Database</td>
<td>2.4 GHz processor, Intel Core™ i7 1st generation or higher, Xeon® 3400 series (4 cores) or higher, 1 GB RAM, 8 GB RAM or higher, 10 GB free space, Windows 2012 R2 64-bit Server VM</td>
<td></td>
</tr>
<tr>
<td>Hosts running Sentral Host Agent</td>
<td>1.8 GHz processor, 1 GB RAM, 2 GB free space</td>
<td></td>
</tr>
<tr>
<td>Operating systems</td>
<td>Windows 7, Windows 10, Supported on Console, Server, Database, and Host Agent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows 2008 Server, Supported on Console, Server, Database, and Host Agent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows 2012 Server R2, Supported on Console, Server, Database, and Host Agent</td>
<td></td>
</tr>
<tr>
<td>(Optional) VM host application</td>
<td>Microsoft Hyper-V®, VMware® ESX Server 5.5 or higher, VMware Server, Xen® Hypervisor 6.0 or higher</td>
<td></td>
</tr>
</tbody>
</table>
5: Installation Prerequisites

The sections below give an overview of installation prerequisites and show important items to remember when installing each component.

5.1: Overview

Before installing Sentral components, install a database server and select the Sentral Server to use in your deployment. Depending on the Sentral Server you select, you might need to install it before installing other Sentral components.

- **Database server**
  
  You must install a database server before installing other Sentral components. Select and install a supported database server: MS SQL 2008, MS SQL 2012

  See section 5.2: “Choosing and Configuring a Sentral Database” below for more important Sentral Database server requirements and recommendations.

  Install your database server before starting the Sentral installer. For high availability, follow the recommendations made by your database server manufacturer.

- **Sentral Server**
  
  Select a supported Sentral Server (Web server) for your Sentral deployment.
  
  - **Apache Tomcat**. Tomcat is included in the Sentral installer. Install Tomcat by starting the Sentral installer and selecting Tomcat during installation.
  
    —OR—
  
  - **Microsoft® Internet Information Services (IIS)**. IIS is not included in the Sentral installer. See the important notes below about installing and licensing a required IIS-related component.

    **NOTE:** If you select IIS as the server to use in your Sentral deployment, you must install and configure Microsoft IIS before starting the Sentral installer. See 5.3: “For Deployments Using Microsoft IIS” below for details.

    **NOTE:** If you are installing Microsoft IIS, Sentral requires ServletExec (this program enables Java® Servlets in IIS). If you indicate you are using IIS during your Sentral installation, the Sentral installer requests a ServletExec license. If you do not already have a ServletExec license, contact ClearCube Sales.

    **NOTE:** The Primary and Secondary Sentral Server databases must use the same login and password credentials.
For information about Sentral Server high availability, see the Server switchover information in 9.14.4: “Additional Miscellaneous Settings” below. For information about enabling TLS in your Sentral environment, see 9.5: “TLS Configuration” below.

- **Endpoint remote control package**
  To enable the remote control of physical endpoints from Sentral Console, install TightVNC (Virtual Network Computing) on the computer on which Sentral Console is installed. The TightVNC client/server software package allows remote network access to graphical desktops. Download TightVNC from [https://www.tightvnc.com/](https://www.tightvnc.com/).

### 5.2: Choosing and Configuring a Sentral Database

Supported databases are not included with Sentral. Install an MS SQL database in your Sentral environment.

**NOTE:** You must install the Sentral Database before installing Sentral Server.

See “Database server” above for a list of supported versions. See important notes about installation options below.

You can install Sentral Database on a remote computer or on the same computer as Sentral Server. For large deployments, ClearCube recommends installing the database server on:

- A different computer than the one running Sentral Server
- A computer with database redundancy or high availability

See the content below for important settings and configuration options for the database server that you install in your Sentral deployment.

This section explains MS SQL authentication modes, and contains important information about requirements when using Windows Authentication mode in MS SQL.

MS SQL is not included with Sentral. These instructions assume that the database installer has adequate knowledge about MS SQL and your environment to perform the installation.

The MS SQL database engine provides two authentication modes:

- **Windows Authentication mode:** this mode enables Windows Authentication and disables SQL Server Authentication.
- **Mixed mode:** in a Sentral environment, this mode uses local SQL server authentication.

When using Windows Authentication mode in MS SQL server, the MS SQL administrator must assign the **sysadmin** server role to the Windows account you use to install Sentral. Before
installing Sentral, contact your MS SQL administrator to ensure that the Windows account used to install Sentral has the sysadmin server role.

5.3: For Deployments Using Microsoft IIS
Perform this procedure only if you are using IIS as the Sentral Server in your environment. (If you have selected Apache Tomcat as your Sentral Server instead of IIS, you can install Tomcat after starting the Sentral installer.)

NOTE: Be sure to install all of the features—including all lower-level features included in the parent features—shown below.

The steps below show how to install IIS features on a computer running Windows 2008 Server, Enterprise operating system.

1. Click Start > Control Panel > Programs > Turn Windows features on or off.
2. Expand Internet Information Services.
3. Expand Web Management Tools and select all lower-level features.
4. Expand World Wide Web Services and select all lower-level features.
5. Select Internet Information Services Hostable Web Core.
6. Click OK. Windows displays a message while it makes changes and then minimizes the dialog box.

If you have already installed a database server, you can now continue to perform the configuration options shown below.

5.4: Enabling Endpoint Devices for Remote Access
The sections below show requirements for remote access and remote control of endpoints.

5.4.1: Enabling Remote Control of Endpoints from Sentral Console
To enable the remote control of physical endpoints from Sentral Console, install TightVNC (Virtual Network Computing) on the computer where Sentral Console is installed. The TightVNC client/server software package allows remote network access to graphical desktops. TightVNC is used to implement device remote control, which is primarily an administration function.

5.4.2: Enabling RDP
If your Sentral environment will include clients that connect to remote hosts (computers, blades, VMs) using Remote Desktop Protocol (RDP) or RDC, be sure to enable remote connections on each host device. This step is not necessary on devices using other protocols, including PCoIP.

The steps below assume you are using Windows 7. Other operating systems might differ slightly.

1. From the Windows Start button, right-click Computer, and then click Properties.
2. Click Remote settings to display the System Properties screen.
3. From the Remote Desktop section, select one of the Allow connections... options.
4. Optionally, click Select Users. You can click Add to add users or groups.
5. Click OK, and then click OK again.

Repeat this step for each host that users will connect to using RDP.

5.5: Configuring Network Ports
Configure firewalls and network ports to enable communication from one Sentral component to another and to endpoint devices.

The table below shows all pertinent ports and devices. Open these ports on all receiving devices. This assumes that no devices have any transmission restrictions.

Table 2. The network ports required in a Sentral environment

<table>
<thead>
<tr>
<th>TCP/UDP</th>
<th>Port #</th>
<th>Receiving Node (Inbound)</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>9</td>
<td>Host Agent</td>
<td>Wake on LAN – enable IP Directed Broadcasts on routers</td>
</tr>
<tr>
<td>TCP</td>
<td>21</td>
<td>FTP Server</td>
<td>FTP Server</td>
</tr>
<tr>
<td>TCP</td>
<td>25</td>
<td>Email Server</td>
<td>Email for Alerts</td>
</tr>
<tr>
<td>TCP</td>
<td>69</td>
<td>Sentral Server</td>
<td>TFTP</td>
</tr>
<tr>
<td>TCP</td>
<td>137</td>
<td>Windows</td>
<td>Win 7</td>
</tr>
<tr>
<td>UDP</td>
<td>137</td>
<td>Thin Client</td>
<td>Printer, file sharing support on Windows Thin Client</td>
</tr>
<tr>
<td>UDP</td>
<td>138</td>
<td>Thin Client</td>
<td>Printer support on Windows Thin Client</td>
</tr>
<tr>
<td>TCP</td>
<td>139</td>
<td>Windows</td>
<td>Win 7</td>
</tr>
<tr>
<td>UDP</td>
<td>162</td>
<td>Enterprise Management System</td>
<td>SNMP – Host to Sentral Console</td>
</tr>
</tbody>
</table>
5.6: Virtual Machine Snapshots
If you are installing Sentral Server on a virtual machine (VM), a best practice is to create a snapshot of the VM immediately after installing Sentral Server and applying any patches or updates (if applicable). If the need arises, this step can help to return the VM to known, pristine state. See 12: “Backups after Initial Configuration” below for more information about recommended backups.
6: Installing Sentral

Before installing Sentral, ensure that you have installed all prerequisites. See Figure 1. Sentral Architecture Components and 5: “Installation Prerequisites” above for details.

The steps below show how to install Sentral components.

**NOTE:** Do not install Sentral Host Agent on the Sentral Console computer.

**NOTE:** If you are using Microsoft IIS as your Sentral Web server, you must install IIS before installing Sentral FTP Server and Sentral Server. If you are using IIS and have not already installed it, stop, and install it now.

**NOTE:** If you are installing Microsoft IIS, Sentral requires the installation of ServletExec. If you do not already have a ServletExec license, contact ClearCube Sales.

1. This step is for Windows 7 only (skip this step if you are using Windows 10). If you are installing Sentral on a Windows 7 operating system, set Sentral installer’s Compatibility mode and Privilege Level.
   a. Right-click the **Sentral Console and Server installer** (file name `ClearCube Sentral ConsoleServer (mmddyyyy).exe`) and select **properties**.
   b. From the Compatibility tab, click **Change settings for all users**.
   c. Select the **Run this program in compatibility mode for** option and select **Windows 7**.
   d. In the Privilege Level area of the dialog box, select **Run this program as administrator**, and then click **OK**.
      
      **Result:** The Compatibility dialog box closes.
   e. Click **OK** to close the Properties dialog box.

2. Double-click the **Sentral Console and Server installer** (`ClearCube Sentral ConsoleServer (mmddyyyy).exe`). If User Account Control displays a message, click **Yes**.

   **Result:** The Setup Wizard appears. Click **Next**.

3. Read the license agreement, click the **I accept** option, and click **Next**.

4. Enter user-related information in the **Customer Information** dialog box.

<table>
<thead>
<tr>
<th>User Name</th>
<th>The name of the Sentral Administrator. Sentral uses this value during product registration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>The Sentral Administrator’s organization. Sentral uses this value during product registration.</td>
</tr>
</tbody>
</table>
Anyone who uses this computer | Select this option to make the Sentral desktop shortcut and Start menu item available for any user who logs in to the computer (the Sentral desktop shortcut is in C:\Users\Public).

Only for me | Select this option to make the Sentral shortcut and Start menu item available only for the user logged in during installation.

Click **Next** to continue.

5. The Setup Type screen enables you to select the Sentral components to install. Select one of the setup type options.
   - **Complete**: select this option to install all Sentral components on the same computer.
   - OR —
   - **Custom**: select this option to install specific Sentral components on a computer (for example, if you are installing the Sentral Console on multiple computers). If you select Custom installation, the installer detects if any of the components that Sentral requires are on the computer. If a component is required, the installer automatically selects it in the dialog box shown below.

![Figure 2. The Sentral Installer showing the components selected for installation](image)

Click **Next** to continue.

6. The installer displays the Database Configuration screen. Provide the database server credentials so the installer can insert the schema in the Sentral database (created before installation). The picture below shows the Database Configuration screen.
Figure 3. The Sentral Database configuration screen

The table below explains the Database Configuration fields.

**Table 3. The Database Configuration screen fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>Select <strong>SQL Server</strong> as appropriate for your installation. MySQL support is planned for future releases.</td>
</tr>
<tr>
<td>Server Authentication</td>
<td><strong>For MS SQL Server only.</strong> This option specifies the authentication mode that MS SQL uses. <strong>Yes</strong> provides local SQL authentication, and <strong>No</strong> provides Windows Authentication.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If you are using Windows Authentication (the <strong>No</strong> option), be sure that the Windows user account you are using to install Sentral has the MS SQL <strong>sysadmin</strong> server role. If necessary, contact your MS SQL administrator before continuing.</td>
</tr>
<tr>
<td>Database Server</td>
<td>Enter the network location (IP address or host name) of the Sentral Database. ClearCube recommends using a static IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Only if you are using a non-default port for your database server (the default SQL Server port is 1433), specify the port at the end of the IP address with a comma between the IP address and the port number. For example: <strong>192.168.3.52,nnnn</strong></td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
 | where 192.168.3.52 is the IP address and nnnn is the port number. If you are using default database server ports (see above), do not specify any port at the end of the IP address.
Username | Enter the user name of the Sentral Database administrator you specified during MS SQL or MySQL installation.
Password | Enter the password for the Sentral Database administrator you specified during MS SQL installation.
Create Database | Select Yes and Sentral will create the database schema you selected above, or overwrite any existing Sentral database. Select No if Sentral will use an existing schema, or you will manually insert a schema.

After providing the information, click **Next** to continue.

7. From the Server Selection screen, use the drop-down menu to select the Web server you are using in your Sentral deployment.

**NOTE:** If using TLS in your deployment, the Primary and Secondary Sentral Servers must use the same credentials (user name and password).

The list and tables below show the steps to perform for the Web server that you select. Select one of the following:

- **If using Tomcat as the Sentral Server**

<table>
<thead>
<tr>
<th>If you are ...</th>
<th>Then ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Sentral for <strong>device-based</strong> allocations only (where user accounts are not considered when allocating clients to hosts)</td>
<td>Leave the <strong>Username</strong>, <strong>Password</strong>, and <strong>Domain</strong> fields blank and click <strong>Next</strong> to continue to step 8 below.</td>
</tr>
<tr>
<td>Configuring Sentral for <strong>user-based</strong> allocations that use Active Directory Domains</td>
<td>Authorize the ClearCube Tomcat service to retrieve Active Directory security group information. Specify the appropriate <strong>Username</strong>, <strong>Password</strong>, and <strong>Domain</strong> values here. If an Active Directory account with this permission does not exist, create one now and specify the values here. Click <strong>Next</strong> to continue.</td>
</tr>
</tbody>
</table>

**NOTE:** For future configuration, you can specify or modify these settings by selecting **ClearCube Tomcat** from Services Microsoft Management Console (MMC). Open MMC by entering **services.msc** in the Start menu’s Search box.

—OR—
6: Installing Sentral

- **If using Internet Information Server as the Sentral Server**

  **NOTE:** If you are using IIS, you must install it before you can continue. If you have not already installed IIS, stop and do so now. See 5.3: “For Deployments Using Microsoft IIS” above for details.

You have now specified the Sentral Web server. Continue by performing the steps below.

8. Complete the SSL Certificate Information screen, shown below, to create an SSL certificate. This information is necessary when communicating with R-series chassis Remote Management Module (RMM). (See *R-Series Data Center Products User’s Guide* for more information about the RMM.)

- All fields are mandatory

  - **Country Code** field is a two-letter code. You can find a list of two-letter country codes (or code elements) in the ISO 3166-1 standard, located at:

    https://www.iso.org/publication/PUB500001.html

![Figure 4. Entering SSL certificate information](image)

Click **Next** to continue.

9. In the Server Configuration screen, Sentral automatically populates the Primary and Secondary Server fields with the hostname of the computer on which you are performing the installation. If you are using a different computer for the primary and secondary Sentral Servers, enter that information here. ClearCube recommends entering the computer’s IP address.

  **NOTE:** If you are installing only one Sentral Server, enter the same value in the Primary and Secondary server fields.

Click **Next** to display the Install screen.
10. Click **Install**. Sentral places a Sentral Console shortcut on the desktop and displays installation progress messages.

11. Click **Finish** when the Setup Wizard Completed screen appears.

   **Result:** a message is displayed showing that the computer needs to restart to complete Sentral installation. Click **Yes** to restart.

12. Be sure to install any Sentral patches or product updates that are available from the ClearCube Support site.


Remember that you must discover devices to manage them in a Sentral environment. Some devices require Sentral agents to enable discovery. See 13: “Preparing Sentral Endpoint Devices” below for more information.
7: Starting Sentral Console
The steps below show how to start Sentral Console for different Windows operating systems.

- **Windows 10:**
  Click Start > All Programs > ClearCube Sentral > ClearCube Sentral Console, then click the ClearCube Sentral Console menu item.

- **Windows 7:**
  Always start Sentral Console as a Windows administrator. From the right-click menu, select Run as administrator, and then click Yes.

![Screenshot of starting Sentral Console as administrator](image)

**Windows 10**
**Windows 7**

*Figure 5. Starting Sentral Console as administrator from the Start menu*

**Result:** Sentral displays the Login screen.

See the section below for information about using the Sentral Administrator account to configure Sentral when logging in for the first time.

8: Using the Sentral Administrator Account
Sentral provides a default Sentral Administrator account. Use the Administrator account to log in to Sentral for the first time, and configure Sentral settings before creating other Sentral user accounts.

After performing initial configurations and setting security options, you can disable the default account and use the local administrator account or a configured Domain account. The steps below show how to log in using the default Sentral account.
1. Start the Sentral Console as described in the previous section.

2. Enter the default Sentral account credentials shown in the table below.

<table>
<thead>
<tr>
<th>Login Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>administrator</td>
</tr>
<tr>
<td>Password</td>
<td>clearcube</td>
</tr>
<tr>
<td>Domain</td>
<td>CCT</td>
</tr>
</tbody>
</table>

3. Click Login.

   **Result:** Sentral displays the Configuration Wizard.

The sections below explain each field in the Configuration Wizard and Configuration Screen.

9: **Sentral Configuration Options**

Sentral configuration options apply to Sentral Console, Sentral Server, Sentral Database, Sentral FTP server, Sentral logs, and more.

**NOTE:** See 14.8: “Configuring Endpoints Using Client Profiles” below for information about how to configure endpoint devices using Client Profiles.

The sections below show the two main areas from which to configure Sentral system settings.

9.1: **Using the Configuration Wizard**

The Configuration Wizard provides a guided walk through of the main Sentral configuration options. After logging in, Sentral displays the Configuration Wizard by default. You can use the Sentral Administrator account to log in to Sentral for the first time to start your configuration (see 8: “Using the Sentral Administrator Account” above for more information).
To display the Configuration Wizard from the main menu, click **Edit > Configuration Wizard**. To prevent the Configuration Wizard from starting at login, select the **Do not show this window at startup** option, and then click **Finish**. The picture below shows the Configuration Wizard.

![Configuration Wizard](image)

*Figure 6. The Configuration Wizard (displayed at login and by clicking Edit > Configuration)*

The subsections below show each Configuration Wizard field. Note that some configuration options are available from the Configuration Screen only.
9.2: Using the Configuration Screen

The Sentral Configuration screen is available from the Sentral main menu. This screen provides most of the configuration options available from the Configuration Wizard (shown in detail in the following sections), and includes additional configuration options detailed in 9.14.1: “SNMP Configuration,” 9.14.2: “Additional Alert (Email) Configuration Options,” and 9.14.3: “VMware View Connection Server Settings” below.

To display the Configuration screen from the main menu, click Setup > Configuration. The picture below shows the Configuration screen.

![Configuration Screen Screenshot]

Figure 7. The Configuration Screen (Setup > Configuration)

The sections below provide detailed explanations about all Configuration options.
9.3: Email Configuration

The table below shows settings for the email notifications sent from Sentral Server. These fields are located in the Email Configuration section of the Configuration Wizard. (These settings are also available in the Alerts section of the Sentral Configuration screen.)

![Configuration Wizard](image)

**Table 5. Email Configuration fields and options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Email Sender</td>
<td>When Sentral Console sends Alert emails, the email's From field contains this value. The default value is <a href="mailto:you@yourdomain.com">you@yourdomain.com</a>. Change this value to the email address of the Sentral Administrator or an email address for Sentral Alerts. See 20: “Sentral Alerts” for information about Sentral Alerts.</td>
</tr>
<tr>
<td>Email Group</td>
<td>Use this field to specify the recipients of Sentral Console emails. The default value is <a href="mailto:you@yourdomain.com">you@yourdomain.com</a>. Change this value to a valid address or addresses. Use a comma separator to specify multiple email addresses.</td>
</tr>
<tr>
<td>SMTP Server</td>
<td>This field specifies the SMTP (email) server for Sentral Alert Emails. The default value is mail.yourdomain.com. Change this value to the name of your SMTP server for Alert emails. Incorrectly formatted SMTP names can provide unexpected results. Enter a valid SMTP mail server name.</td>
</tr>
</tbody>
</table>
9.4: Server Configuration

The table below shows settings for the Sentral Server. These fields are located in the Server Configuration section of the Configuration Wizard. (These settings are also available in the Sentral Server section of the Sentral Configuration screen).

<table>
<thead>
<tr>
<th>Table 6. Server Configuration fields and options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>Primary Server</td>
</tr>
<tr>
<td>Secondary Server</td>
</tr>
</tbody>
</table>
9.5:  **TLS Configuration**
TLS (Transport Layer Security) encrypts communication to and from Sentral Server for additional security. The table below shows settings for enabling TLS in Sentral. These fields are located in the TLS Configuration section of the Configuration Wizard.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable TLS</td>
<td>Select this option to enable TLS in Sentral.</td>
</tr>
<tr>
<td>Public Certificate</td>
<td>Click <strong>Upload</strong> and browse to the location of the public certificate for Sentral Server.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>If your environment includes a Secondary Sentral Server, the Primary and Secondary Servers must use the same public certificate and private keystore.</td>
</tr>
<tr>
<td></td>
<td>If your environment includes a Secondary Sentral Server, the public certificate must include the IP addresses of the Primary Sentral Server and the Secondary Sentral Server.</td>
</tr>
<tr>
<td>Private Keystore</td>
<td>Click <strong>Upload</strong> and browse to the location of the private keystore for Sentral Server. If using TLS, see note in the Enable TLS row, above.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>If your environment includes a Secondary Sentral Server, the Primary and Secondary Servers must use the same public certificate and private keystore.</td>
</tr>
<tr>
<td>Keystore Password</td>
<td>Enter the password for the keystore container.</td>
</tr>
</tbody>
</table>

9.5.1:  **More about TLS in Sentral**
Sentral uses asymmetric encryption (SHA-256 with RSA2048) using two-way keys. This requires two certificates:

**Public certificate**
- This is a general-purpose certificate used by client and host devices. The public certificate uses the **.cer** extension.

**Private certificate**
- This is a keystore used by the Sentral Server (HTTP server). The private certificate uses the **.keystore** extension.

By default, all communication uses TLS 1.2.
9.5.2: Generating a Private Certificate

The command below shows how to use the Java® keytool.exe command line utility to generate a private certificate. The utility is available in any JDK distribution, located in %JAVA_HOME%\bin.

**NOTE:** Type the command as a single line. Multiple lines in the example below are for used to improve legibility only.

Enter **bold** text as shown below. Replace **italics** text with values appropriate for your environment.

"path/to/keytool.exe" -genkeypair -dname "CN=commonName O=organizationName, OU=organizationUnit, L=localityName, S=stateName, C=country" -keyalg RSA -keysize 2048 -keystore "D:\privateCertPath.keystore" -storepass changeit -validity 999 -keypass changeit -ext SAN=ip:192.168.8.160

9.5.3: Exporting a Public Certificate from a Private Certificate

The command below shows how to use the keytool.exe command line utility to export a public certificate from the private certificate.

**NOTE:** Type the command as a single line. Multiple lines in the example below are for used to improve legibility only.

Text in **bold** should be entered as shown; replace **italics** text with the values appropriate for your environment.

“C:\Program Files\Java\jre1.8.0_181\bin\keytool.exe” -export -file “D:\publicCertPath.cer” -keystore “D:\privateCertPath\keystore” -storepass keystorePassInPreviousCommand

9.5.4: Uploading Certificates to Sentral

The steps below show how to upload public and private certificates to Sentral.

1. From the Sentral menu, click **Edit > Configuration Wizard**.

2. Click **TLS Configuration** on the left panel.

3. Select the **Enable TLS** option.

4. Click the Public Certificate **Upload** button and navigate to the public certificate you created (as shown in the previous sections). Select the certificate, and click **Open**.

5. Click the Private Keystore **Upload** button and navigate to the private certificate you created (as shown in the previous sections). Select the certificate, and click **Open**.

6. Enter the keystore password in the Keystore Password field. Optionally, click **Show** to see the password characters.
7. Click Finish.

8. From the Windows Services utility, restart Sentral Server (select the ClearCube Tomcat service). Sentral Server is now communicating securely using TLS encryption.

### 9.6: Alert Configuration

Sentral evaluates various system and device parameters and can provide alerts. The table below shows the settings for evaluating alert conditions and deploying alerts. (These settings are also available in the Alerts section of the Configuration screen.)

**NOTE:** Be sure to see the alert-related configuration options that are available in the Configuration Screen. See 9.14.2: “Additional Alert (Email) Configuration Options” below for details about these additional alert options.

<table>
<thead>
<tr>
<th>Alert Configuration fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Evaluation Interval (min)</td>
<td>This field specifies the time interval, in minutes, for evaluating an Alert. The default value is 30 minutes. A timer starts the first time Sentral sends an Alert. When the time specified in this field elapses, the Alert is re-evaluated.</td>
</tr>
<tr>
<td>Alert Firing Interval (hrs)</td>
<td>This field specifies the time interval, in hours, after which Sentral can send (trigger) an Alert again if the condition is still true. The default value is one hour.</td>
</tr>
</tbody>
</table>
9.7: FTP Configuration

The table below shows FTP-related settings in the FTP Configuration section of the Configuration Wizard. (These settings are also available in the FTP section of the Sentral Configuration screen.)

![FTP Configuration window](image)

### Table 8. FTP Configuration fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFTP Host IP</td>
<td>This field specifies the IP address for the TFTP host, which provides firmware updates for the R-Series Chassis’ RMM (Remote Management Module). The default value is 127.0.0.1. The value must be an IP address.</td>
</tr>
<tr>
<td>FTP Host</td>
<td>This field specifies the IP address of the computer on which the FTP Server is running. The FTP host permits software, BIOS, and thin client updates. The default value is 127.0.0.1. ClearCube recommends using a static IP address.</td>
</tr>
<tr>
<td>FTP User</td>
<td>This field specifies the user name for the FTP server. The default value is admin.</td>
</tr>
<tr>
<td>FTP Password</td>
<td>This field specifies the password for the FTP user. The default password is admin. Asterisks appear in place of the characters entered.</td>
</tr>
</tbody>
</table>
9.8: Database Configuration

The table below shows Sentral Database settings in the Database Configuration section of the Configuration Wizard. (These settings are also available in the Database section of the Sentral Configuration screen.)

Table 9. Database Configuration fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Database Server Name</strong></td>
<td>This field specifies the hostname of the database server computer. The default value is the name of the database server specified during Sentral Server installation.</td>
</tr>
<tr>
<td><strong>Database User Name</strong></td>
<td>This field specifies the name of the database user. The default value is the name of database user specified during Sentral Server installation.</td>
</tr>
<tr>
<td><strong>Database User Password</strong></td>
<td>This field specifies the password for the database user. Asterisks appear in place of the characters entered. The default value is the password specified during Sentral Server installation.</td>
</tr>
<tr>
<td><strong>Database Type</strong></td>
<td>This drop-down menu specifies the SQL database type. Choices are SQL Server and MySQL—note that MySQL is not supported in 6.9.6; support is planned in a future release. The default value is the database specified during Sentral Server installation.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Integrated Security</td>
<td>This field is available only when you select SQL Server in the Database Type field. Possible values:</td>
</tr>
<tr>
<td></td>
<td>- <strong>True</strong>—this setting enables Windows Authentication for the Sentral Database.</td>
</tr>
<tr>
<td></td>
<td>- <strong>False</strong>—this setting enables mixed-mode authentication for the Sentral Database.</td>
</tr>
<tr>
<td>Database Server Port</td>
<td>This field specifies the database server port. The default value is the port specified during Sentral installation. See “Database server” in 5.1: “Overview” above for details.</td>
</tr>
<tr>
<td>Database Name</td>
<td>Enter the database name here. The default is cms.</td>
</tr>
</tbody>
</table>
### Table 10. Discovery Configuration fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Thin Client Update Timeout (min)** | This field specifies the thin client timeout period. If Sentral does not receive a poll from a thin client in this time, Sentral Designates it offline. The default value is 10 minutes. ClearCube recommends making this value a multiple of the Thin Client Health Update Interval. ClearCube recommends following these best practices:  
- Timeout values are always larger than update intervals.  
- ClearCube recommends making this value a multiple of the Thin Client Health Update Interval (Set polling and timeout values so devices can send two polls within the timeout period). |
| **Physical Machine Update Timeout (min)** | This field specifies the device’s timeout period. If Sentral does not receive a poll from a physical machine in this time, Sentral Designates it offline. The default value is 10 minutes. ClearCube recommends following these best practices:  
- Timeout values are always larger than update intervals.  
- ClearCube recommends making this value a multiple of the Physical Machine Health Update Interval (Set polling and timeout values so devices can send two polls within the timeout period). |
| **Discovery Update Config** | This pull-down menu specifies whether Sentral Console uses the push discovery function for hosts (physical hosts and VMs) and thin clients. Choices are True (default) and False.  
| **Discovery User Preference** | This pull-down menu specifies which user discovery type takes preference. Options include:  
- **Domain**—Choose if Sentral user accounts are located in an Active Directory Domain  
- **Local**—Choose if Sentral users are defined in a Sentral Database or are Windows user accounts on the local computer.  
The default selection is Domain. (See 14.10: “Discovering and Adding Device Users” for more information.) |
| **Mapping User Type** | Specifies the type of mapping (allocations) to perform.  
- **Sentral**—Groups created and defined in Sentral.  
- **Windows**—Active Directory groups. |
| **Thin Client** | This field specifies the time after which a thin client reports to the |
### Update Interval (min)

Server with a heartbeat (in minutes). This value should be less than the thin client Refresh Time. The default value is five minutes.

### Physical Machine Health Update Interval (min)

This field specifies the time after which a host or VM reports back to the server with a heartbeat (in minutes). This value should be less than the Host Refresh Time. The default value is five minutes.

## 9.10: System Configuration

The table below shows the System discovery settings in the System Configuration portion of the Configuration Wizard. (These values are also available in the System Credentials area of the Sentral Configuration screen.)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update Interval (min)</strong></td>
<td>server with a heartbeat (in minutes). This value should be less than the thin client Refresh Time. The default value is five minutes.</td>
</tr>
<tr>
<td><strong>Physical Machine Health Update Interval (min)</strong></td>
<td>This field specifies the time after which a host or VM reports back to the server with a heartbeat (in minutes). This value should be less than the Host Refresh Time. The default value is five minutes.</td>
</tr>
</tbody>
</table>

### System User Name

This field specifies the Administrator username of the local system where Sentral Console is running. It is required for scheduling reports and other tasks. The default value is Administrator.

### System User Password

This field specifies the password for the Administrator account on the Sentral Console computer. Asterisks appear in place of the characters.
9.11: Dashboard Configuration
The Sentral dashboard shows status and activity information for Sentral components and endpoint devices. The fields shown below specify dashboard settings, and are located in the Dashboard Configuration portion of the Configuration Wizard. (These values are also available in the Dashboard area of the Sentral Configuration screen.)

![Dashboard Configuration Wizard](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard Refresh Time (min)</td>
<td>Specifies (in minutes) how frequently the Sentral dashboard refreshes.</td>
</tr>
<tr>
<td>Dashboard Scale (hrs)</td>
<td>Specifies the time (in hours) that the Polls Received item displays on the Sentral dashboard. The picture below shows the dashboard scale.</td>
</tr>
</tbody>
</table>

![Dashboard Scale](image)

**Table 12. Dashboard Configurations fields**

9.12: Security Groups Configuration
The table below shows security group settings you can specify for Sentral users when logging in to Sentral. This wizard page enables you to apply existing security groups to Sentral Console. For additional configuration from the Sentral menu, click **Setup > Security**.
Table 13. The Security Groups Configuration fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Local Security Groups      | This multi-select list box displays the Security Groups defined on the Sentral Server computer. Select multiple security groups by holding the **SHIFT** or **CTRL** key during selection.  
When a user logs in to Sentral Console (if the user is a member of multiple groups), the Login screen pull-down menu displays a list of groups the user can use for the session. |
| Domain Security Groups     | If Sentral Server is part of a Domain, this multi-select list box displays the Domain Groups. Only Domain Admins is available when logged in on the local machine. Select multiple security groups by holding the **SHIFT** or **CTRL** key during selection.  
When a user logs in to Sentral Console (if the user is a member of multiple groups), the Login screen pull-down menu displays a list of groups the user can use for that session. |

9.13: Miscellaneous Configuration Options

The table below shows the settings shown in the Miscellaneous (Other) portion of the Configuration Wizard. (These values and others are also available in the Miscellaneous area of the Sentral Configuration screen, shown in 9.14.4: “Additional Miscellaneous Settings” below.)
### Table 14: The Miscellaneous Configuration screen options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain Type</strong></td>
<td>This pull-down menu provides the basis for user authentication. Choices include:</td>
</tr>
<tr>
<td></td>
<td>• AD (Active Directory)</td>
</tr>
<tr>
<td></td>
<td>• NT (NT 4)</td>
</tr>
<tr>
<td></td>
<td>The default selection is AD.</td>
</tr>
<tr>
<td><strong>Logging Level</strong></td>
<td>This pull-down menu specifies the level of logging maintained by Sentral. Choices include:</td>
</tr>
<tr>
<td></td>
<td>• Debug (all group and device events are logged)</td>
</tr>
<tr>
<td></td>
<td>• Warning (warnings and critical errors are logged)</td>
</tr>
<tr>
<td></td>
<td>• Critical (only critical errors are logged)</td>
</tr>
<tr>
<td></td>
<td>• None (turns off log capturing)</td>
</tr>
<tr>
<td></td>
<td>The default selection is None.</td>
</tr>
<tr>
<td><strong>Connection Preference</strong></td>
<td>If a user and a thin client have allocations to the same host, this list specifies which allocation takes priority. Choices include:</td>
</tr>
<tr>
<td></td>
<td>• Thin Client</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The default selection is Thin Client.</td>
</tr>
<tr>
<td>Staggered Labels</td>
<td>This pull-down menu specifies how Switching Screen labels appear. Choices include:</td>
</tr>
<tr>
<td></td>
<td>- Host</td>
</tr>
<tr>
<td></td>
<td>- None</td>
</tr>
<tr>
<td>I9400 Disconnect upon Logoff</td>
<td>This setting specifies if a zero client session disconnects when a user logs off. Options include:</td>
</tr>
<tr>
<td></td>
<td>- True (this setting forces PCoIP sessions to disconnect when a user logs off of their computer)</td>
</tr>
<tr>
<td></td>
<td>- False (default) (This session enables a PCoIP session between a zero client and host to persist when a user logs off their computer).</td>
</tr>
</tbody>
</table>

#### 9.14: Additional Configuration Options

The Sentral Configuration screen provides configuration options not available from the Configuration Wizard. To display the Configuration screen from the main menu, click **Setup > Configuration**. (See Figure 7 above for a picture of the Configuration screen.)

#### 9.14.1: SNMP Configuration

Simple Network Management Protocol (SNMP) is a protocol that enables you to manage nodes on an IP network. SNMP allows sending alerts and other messages across your network, and can help network administrators manage network performance, find and solve network problems, and plan for network growth. You can set a global SNMP configuration for hosts in your environment from Sentral Console.

1. From the main menu, click **Setup > Configuration** to display the Configuration screen.
2. From the toolbar, click the **Configure SNMP** button (✓).
   
   **Result:** Sentral displays the SNMP Configuration screen.
3. Edit the following parameters as appropriate for your environment.
Table 15. SNMP Configuration Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>This field specifies the UDP port to which Sentral sends traps. The default is 162. This value should match the SNMP trap receiver port on your enterprise management system.</td>
</tr>
<tr>
<td>Generic Trap</td>
<td>This field indicates that the trap is enterprise-specific. SNMP vendors and users define their own traps under the private-enterprise branch of the SMI object tree. The default value is 6.</td>
</tr>
<tr>
<td>Trap Receiver</td>
<td>This field specifies the system that receives the SNMP traps. The default value is localhost. Change this value to the hostname or the IP address of the trap receiver system.</td>
</tr>
<tr>
<td>Specific Trap</td>
<td>This field specifies the enterprise-specific trap number, and applies only when the Generic Trap is 6. To process this trap properly, the NMS has to decode the specific trap number that is part of the SNMP message. The default value is 1.</td>
</tr>
<tr>
<td>Community String</td>
<td>This field specifies the SNMP community name used in traps sent to this destination. The default value is public.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>This field specifies the object identifier that uniquely identifies the Enterprise ID in the MIB. The default value is .1.3.6.1.4.1.2682.</td>
</tr>
<tr>
<td>Type of Trap Format</td>
<td>This field specifies the type of trap format. The default value is String.</td>
</tr>
<tr>
<td>Trap Sender</td>
<td>This field specifies the location of the system with the SNMP agent. The default value is localhost. Change this value to the hostname or the IP address of the trap sender system if it is different from the address of the Sentral Console computer.</td>
</tr>
<tr>
<td>SNMP Enabled</td>
<td>Select this option to enable SNMP traps on all Sentral hosts.</td>
</tr>
</tbody>
</table>

4. From the toolbar, click the Save button ( ) and then click OK.

   **Result:** Sentral displays a message indicating that you need to restart the Sentral Server to apply the SNMP configuration changes.

5. From the computer running Sentral Server, restart the server to deploy the SNMP configuration to Sentral hosts:
   a. From the Windows Start menu Search box, type services.msc and press Enter.
      
      **Result:** Your computer displays the Services Microsoft Management Console (MMC).
   b. From the Name column, right-click ClearCube Tomcat and select Restart.
      
      **Result:** a Service Control message indicates that the service is restarting.
   c. Close the Services MMC. The SNMP configuration is now in effect.
9.14.2: Additional Alert (Email) Configuration Options

The table below shows settings for email notifications that Sentral Server sends. These fields are located in the Alerts section of the Sentral Configuration screen (from the main menu, click Setup > Configuration).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Port</td>
<td>The port for the outgoing SMTP server.</td>
</tr>
<tr>
<td>Alert Email Sender Password</td>
<td>Password for the alert sender email account.</td>
</tr>
<tr>
<td>SSL Password Authentication</td>
<td>Select this option to enable SSL authentication for the alert email sender password.</td>
</tr>
<tr>
<td>Offline Node Notification</td>
<td>Select this option to send an email to the address or addresses specified in the Email Group field if a node goes offline.</td>
</tr>
</tbody>
</table>

Table 16. Alerts fields and options

9.14.3: VMware View Connection Server Settings

The table below shows View Connection Server settings that you can specify from Sentral Console. These fields are located in the View Connection Server section of the Sentral Configuration screen (from the main menu, click Setup > Configuration).

You can push these settings to client devices (endpoints) in your Sentral deployment. For information about pushing View Connection Server settings to devices during device discovery, see 14.8: “Configuring Endpoints Using Client Profiles” below.
### Table 17. View Connection Server fields and options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Connection Server IP</td>
<td>The IP address of the View Connection Server. This address defaults to 127.0.0.1 if Sentral Console is on the same computer as Sentral Server. Otherwise, specify the IP address of the Sentral Server.</td>
</tr>
<tr>
<td>View Connection Server Port</td>
<td>The port for the View Connection server. The default value is 443 (TCP).</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Select this option to enable SSL authentication for communication between Sentral Server and View Connection Server.</td>
</tr>
<tr>
<td>Enable Auto Connect</td>
<td>Select this option to enable View clients to connect automatically to an allocated desktop or VM. To enable auto-connection, you must allocate (map) a client to a VM host. See 14.11: “About Allocations and Allocation Types” below for more information.</td>
</tr>
</tbody>
</table>


In Sentral 6.9.6, the Primary and (optional) Secondary Sentral Server support increased communication for high availability. If a Primary Server becomes unavailable, the Secondary Server detects this event. The Secondary Server automatically re-discovers all devices in the environment and the Sentral environment remains available. If the Primary Server becomes available again, it automatically redisCOVERs devise and resumes operation as the Primary Server.

The table below shows additional high availability and allocation settings that you can specify from Sentral Console (features not discussed in this section are shown in 9.13: “Miscellaneous Configuration Options” above). These fields are located in the Miscellaneous section of the Sentral Configuration screen (from the main menu, click **Setup > Configuration**.)
Sentral regularly checks that the Primary Server is available. If it is not available, Sentral tries to connect to the Primary Server the number of times specified here. If Sentral cannot connect after the specified number of attempts (retries), Sentral switches over to the Secondary Server. The default value is 3.

The number of seconds that Sentral waits between each retry attempt (described above). The default value is 30 seconds.

Specifies the amount of time, in seconds, that Sentral reserves one or more hosts (blades or VMs) for a user to connect to. When a user tries to connect to a host from a zero client or thin client, Sentral presents a list of available hosts. If a user does not connect to a host in the specified Allocation Timeout period, the hosts are made available again. The default value is 30. See 14.12: Creating Allocations (Mapping Devices and Users)” below for more information.

The number of allocations (mappings, or assignments) a user, thin client, or zero client can have to other devices or users. The default value is 10.

9.14.5: Zero Client Login Screen

The Sentral Server ServerConfiguration.xml file specifies many server settings. The default location of ServerConfiguration.xml is:

C:\Program Files\ClearCube Sentral\CMSServer\WEB-INF\configuration\properties

This location might be different depending on where you installed Sentral.

The entry shown below shows or hides the zero client login screen. Credentials requested here are Windows user account credentials.

<entry key="iport.hide.login.screen">false</entry>

The default value is true, which hides the zero client login screen. Setting the value to false displays the zero client login screen.
10: Apply Your Sentral License Key

Section 3: “Requesting a Sentral License,” shows how to request a Sentral license key from ClearCube Support. After you receive the license key and install all Sentral components, apply the key as shown in the steps below (these steps assume Sentral is on a computer with a Windows 7 operating system).

1. Copy the license key from the email you received from ClearCube.
2. Start Sentral Console by running it as administrator. Click Start > All Programs > ClearCube Sentral, then right-click the ClearCube Sentral Console menu item.

![Figure 8. Starting Sentral Console](image)

3. From the right-click menu, select Run as administrator, and then click Yes.
4. From the Sentral menu, click Setup > License Information.
5. Paste the license key in the dialog box (press CTRL+V), then click Submit.
6. Sentral displays a message about restarting Sentral Console. Click OK to close Sentral Console.
7. Start Sentral Console again as described above and log in.

Your Sentral license is now applied.
11: Server Log and Settings
Logging is enabled by default so you can monitor Sentral Server performance after installation. After configuring server poll times, timeouts, and so on, ClearCube recommends turning logging off as described below.

Sentral Server logs are either:

- Written to a Server.log file (log files are saved daily as a zip file with the name format Server.log.YYYY-MM-DD, where YYYY is the year, MM is the month, and DD is the day).

--- OR ---

- Displayed in an Apache Tomcat Console
  (The console is available only when starting Tomcat as an application instead of as a service.)

11.1: Log Location
The log file, Server.log, is located in the C:\Program Files\ClearCube Sentral\CMSServer\WEB-INF\configuration\log directory.

11.2: Turning off Logging
The steps below show how to stop logging (where Sentral does not write logs to Server.log). To set logging level to OFF:

1. Locate log4j.xml in the following directory:
   C:\Program Files\ClearCube Sentral\CMSServer\WEB-INF\classes

2. Change level value from DEBUG to OFF, as shown below:

   <logger name="com">
   <level value="OFF" />
   <!--<appender-ref ref="CONSOLE" />-->
   <appender-ref ref="CSMSSERVER"/>
   </logger>
12: Backups after Initial Configuration

The sections below provide recommendations about backing up Sentral components.

12.1: Backing up Sentral Server and Sentral Console

ClearCube recommends backing up Sentral Server and console after making all configurations.

From the **C:\Program Files\ClearCube Sentral** directory, back up the directories shown below:

- **ClearCube Sentral Console:**
  - C:\Program Files\ClearCube Sentral\CMSServer\WEB-INF\classes
  - C:\Program Files\ClearCube Sentral\CMS\CMS.jar
- **Tomcat:**
  - C:\Program Files\ClearCube Sentral\Tomcat

12.2: Backing up Sentral Database Schema

ClearCube recommends creating an automated daily or weekly backup of the database schema.

You can create a batch file that gracefully stops the console and server, backs up the database, and then restarts the Apache Tomcat service.

The example below is a script you can use with Windows Scheduler that backs up a MySQL database. If you use a different database, write a script performing equivalent actions.

*Example 1. A script to back up MySQL database*

```bash
echo OFF
TASKKILL /F /IM "javaw.exe"
NET STOP "ClearCube Tomcat"
"C:\Program Files\MySQL\MySQL Server <Version>\bin\mysqldump" -u<USERNAME> -p<PASSWORD> --result-file="\NETWORK-LOCATION\FILE\date:=%date:=%\sql" cms
NET START "ClearCube Tomcat"
```

Save the script above as a .bat file. Schedule it to run using Task Scheduler (included with Windows operating systems). You can then use MySQL restore commands to restore the database if needed:

```bash
mysql --verbose --user=USERNAME --password=PASSWORD CMS2 < /PATH/TO/backufilename.SQL>
```
12.3: Backing up Virtual Machines and Snapshots

When you install Sentral on a virtual machine, it is a best practice to create a snapshot after completing all Sentral configurations. The snapshot enables you to return to a known instance if it is ever necessary. Additionally, it is a best practice to create backups of the Sentral Server virtual machine on a regular basis.
13: Preparing Sentral Endpoint Devices

Hosts and thin clients you manage in your Sentral environment require a Sentral Host Agent or Thin Client Agent. The sections below show how to install Host Agents and Thin Client Agents. (Note that zero clients and host cards using PCoIP technology do not require agent software.)


13.1: Installing Sentral Host Agent

This section shows how to install the Sentral Host Agent. You must install Sentral Host Agent on each host (physical computer, blade, virtual machine, or other computing device) that Sentral manages.

NOTE: Remember that hosts require a Host Agent; thin clients require a Thin Client Agent. Zero clients do not require agent software.

See 13.2: “Installing Sentral Thin Client Agent” below for information about installing a Thin Client Agent.

13.1.1: Windows

This section shows how to install Sentral Host Agent on devices using a Windows operating system. ClearCube recommends copying the Host Agent installer to the host or VM and installing it locally.

The Sentral Host Agent requires administrator privileges for installation. These steps assume you are installing the Host Agent on a computer running a Windows 7 operating system. To install the Sentral Host Agent, perform the following steps:

1. Ensure that you:

   • Log in to the physical host or VM as an Administrator with installation privileges.

   • Open ports that Sentral requires for communication, specified in 5.5: “Configuring Network Ports” above.

   • **For remote control features on hosts:** Install TightVNC on each host device (and on the Sentral Server computer).

   • **For VMs only:** Install and configure VM host application and VMs according to your product documentation.
2. From the Sentral download, copy the ClearCube Sentral BladeAgent (mmddyy).exe installer to the host or VM.

3. Right-click ClearCube Sentral BladeAgent (mmddyy).exe and select Run as administrator to launch the Host Agent installer. User Account Control displays a message. Click Yes. The installer displays the Host Agent welcome screen and TightVNC message, shown below.

   ![Host Agent installer welcome screen](image)

   **Figure 9. The Host Agent installer welcome screen**

   **NOTE:** To enable Sentral remote control features (to mirror host desktops for remote support and troubleshooting tasks), install TightVNC on each host device.

4. Click Next to display the license agreement.

5. Accept the agreement and then click Next to display the Customer Information screen.

6. Complete the user name and organization fields, and then select the users for whom to install the application. Click Next to display the Installation screen.

7. Click Install to start Host Agent installation.

   **Result:** Progress messages are displayed.

8. The installer displays the Sentral Host Agent setup completion screen. Click Finish to complete Host Agent installation.
9. Restart the computer to complete installation. Click Yes to restart immediately or No to restart later.

You can now perform a device discovery to begin managing the host from Sentral Console. Remember to install Thin Client Agents on any thin clients in your Sentral environment. See 13.2: “Installing Sentral Thin Client Agent” below for instructions.

13.1.2: Red Hat Enterprise Linux (RHEL)
This section shows how to install Sentral Host Agent on devices using Red Hat® Enterprise Linux®

Dependencies for PCoIP support on a 64-bit operating system
To support PCoIP technology on a host, you must install PCoIP Host Software on the host before installing Sentral Host Agent.

PCoIP Host Software is a collection of drivers and applications that enable the operating system to interact with PCoIP firmware. This software enables features such as local cursor and keyboard, locking the computer when a session terminates, and more.

NOTE: PCoIP Host Software does not support 32-bit operating systems.

The steps below show how to install PCoIP Host Software on 64-bit RHEL. These steps assume you are working from a computer on the same network as the computer with the PCoIP host card.

1. From the x86_64 > PCoIP Agent folder in the Sentral download’s Host Agent folder, install the rpm package using following command:

   `rpm -ivh pcoip_host-4.0-8.el6.x86_64.rpm`

2. From a computer on the same network as the PCoIP host card, open the host card’s Web interface (type the host card’s IP address in your browser’s address bar) and log in (passwords are blank by default).

3. From the Configuration menu, select Host Driver Function.

4. Select Enable Host Driver Function, and then click Apply. A prompt appears to indicate that you must reset the PCoIP processor.

5. Click Reset and then click OK to schedule a deferred reset.

6. Restart the PCoIP host by restarting the computer.

You can now follow the steps below to install the Sentral Host Agent.
Installing Sentral Host Agent

1. From the Sentral download, copy the Host Agent installer from the Sentral Host Agent folder to the host or VM. Be sure the installer is for the appropriate operating system.

2. Change directory to the location of the installation rpm. Type the following command:

   ```
   sudo rpm -ivh --nodeps BladeAgent-6.9.6.x86_64.rpm
   ```

3. A success message indicates that the installation is complete. Restart the computer.

Post Installation Dependencies

Run the following commands in a terminal as superuser.

1. Get extra packages for Enterprise Linux:

   - For i386 only:
     ```
     wget http://dl.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm
     ```
   - For x86_64 only:
     ```
     wget http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
     ```

2. Enter the command:

   ```
   sudo rpm -Uvh epel-release-6*.rpm;rm -rf epel-release-6*;
   ```

3. Enter the command:

   ```
   yum -y install xrdp
   ```

4. Change directory:

   ```
   cd /etc/rc.d/init.d/ && chkconfig --add xrdp
   ```

5. Enter the command:

   ```
   chkconfig --level 2345 xrdp on
   ```

6. Restart the computer.

Uninstall

1. Enter the following command:

   ```
   rpm -e BladeAgent
   ```

2. Restart the computer.
13.1.3: **Ubuntu**
This section shows how to install Sentral Host Agent on devices using Ubuntu® Linux.

**Pre-Installation Dependencies**
From a terminal, enter these commands as superuser.
1. `sudo apt-get update`
2. `sudo apt-get install xrdp`

**Install**
From a terminal, enter these commands as superuser.
1. `dpkg -i BladeAgent-6.9.6_64.rpm`
2. Restart the computer.

**Uninstall**
1. `apt-get remove bladeagent`
2. Restart the computer.

13.2: **Installing Sentral Thin Client Agent**
Thin clients require the Sentral Thin Client Agent to enable Sentral to manage them. Install the Sentral Thin Client Agent on each thin client that Sentral manages. Sentral includes installers for Windows® 10, Windows Embedded Standard 7, and Linux®.

If the thin clients in your enterprise have pre-installed Sentral Thin Client Agents, you do not need to install or re-install the Thin Client Agent.

**NOTE:** Zero clients using PCoIP technology do not require a Thin Client Agent.

**NOTE:** If you are using clients that run a Linux operating system, consult the documentation included in the installation media for Linux Thin Client Agent installation instructions.
13.2.1: Windows Operating Systems

The steps below show how to install a Thin Client Agent locally on a single thin client. The screens below show installation on a Windows operating system.

1. Ensure that you:
   - Log in to the thin client as an Administrator with installation privileges.
   - Uninstall any Sentral software that is currently on the thin client.
   - Open ports that Sentral requires for communication. See 5.5: “Configuring Network Ports” above for details.
   - Attach any necessary peripherals to the thin client (such as a keyboard, mouse, monitor, and optionally a mass storage device).

2. If applicable, turn off or disable the thin client’s write filter.
   Ensure that the thin client has enough space to install the Thin Client Agent. This might require deleting items or moving items to another location, such as a network share.

3. From the thin client folder in the Sentral download, copy the ClearCube Sentral Thin Client Agent installer to the thin client. Choose the installer appropriate for your operating system.

4. Right-click the executable file and select Run as administrator to start the Thin Client Agent installer.

5. User Account Control displays a message. Click Yes. The installer shows progress messages and then displays the Thin Client Agent welcome screen and TightVNC message, shown below.

![Figure 10. Thin Client Agent welcome screen](image-url)
6. Click **Next** to display the license agreement.

7. Accept the agreement and click **Next** to display the Customer Information screen.

8. Complete the **User Name** and **Organization** fields, and then select the users for whom to install the application. Click **Next** to display the Setup Type screen.

9. From the Setup Type screen, you can select the features to install. You can include and remove features by choosing the **Custom** option. If you choose the Custom installation option, you must include the Thin Client Agent.

   - **ClearCube Sentral Thin Client Agent (Mandatory)** – Installs the Thin Client Agent.

   - **VNC (Optional)** – TightVNC is software administrators can use to mirror desktops for remote support and troubleshooting tasks. Select this option if you will use TightVNC and remote control features in your environment. You must manually install TightVNC after thin client installation.

![Figure 11. Selecting Thin Client Agent components to install](image)

After choosing features to install, click **Next**.

10. Enter the IP address or hostname of the Sentral **Primary Server** and **Secondary Server**. The default value is the hostname of the computer on which you are installing the Host Agent.

   **NOTE:** If you have a Primary Sentral Server only, enter the same values in the Primary and Secondary fields. The value here must be the same as the value you specified during Sentral Server installation.

   Click **Next**.
11. Click **Install** to start installation. The installer displays progress and status information.

12. The installer displays the Sentral Thin Client Agent setup completion screen. Click **Finish** to complete Thin Client Agent installation.

13. Restart the thin client to complete installation. Click **Yes** to restart immediately or **No** to restart later.

14. Optionally, if you moved any data to a network share or other location, move the data back to the thin client.

15. Optionally, if you are using remote control features from Sentral Console, install TightVNC on the thin client. Download TightVNC from [https://www.tightvnc.com/](https://www.tightvnc.com/).

16. If applicable, turn on or enable the write filter.

You can perform a device discovery to begin managing the client from Sentral Console.

### 13.2.2: Linux-Based Operating Systems

The sections below show how to install the Sentral Thin Client Agent on thin clients that use Linux-based operating systems.

#### 13.2.2.1: Ubuntu and Raspbian

The steps below show how to install and uninstall the Thin Client Agent package for Ubuntu and Raspbian operating systems.

**To install:**

1. From the thin client folder in the Sentral download, copy `iport_6.9.6.deb` to the thin client. Choose the file appropriate for your operating system.
2. Open a terminal window and change directory to the location of the `iport_6.9.6.deb` file.
3. Enter the command:

   ```bash
   sudo dpkg -i iport_6.9.6.deb
   ```

4. From the pop-up dialog box, enter the IP address or hostname of the Sentral **Primary Server** and **Secondary Server**. The default value is the hostname of the computer on which you are installing the Host Agent.

   **NOTE:** If you have a Primary Sentral Server only, enter the same values in the Primary and Secondary fields. The value here must be the same as the value you specified during Sentral Server installation.

5. Restart the thin client.
To uninstall:
1. Open a terminal window and change directory to the location of the iport_6.9.3.deb file.
2. Enter the command:
   \texttt{sudo apt-get remove iport}
3. Reboot the thin client.

14: Basic Operations
The sections show basic Sentral tasks you can perform after preparing Sentral endpoint devices (see 13: “Preparing Sentral Endpoint Devices” above for more information about preparing endpoint devices).

14.1: Integrating VMware vCenter Server
The steps below show how to integrate a vCenter Server instance into your Sentral environment.
1. From the Sentral main menu, click \texttt{Edit > Virtualization Wizard} to display the wizard.
2. From the Hypervisor Type area, select \texttt{vSphere ESXi} and click \texttt{Next}.
3. Click \texttt{Add vCenter} to display the credentials dialog box.
4. Enter the vCenter Server’s IP address, user name, and password, and then click \texttt{Add}. A progress indicator is displayed and the vCenter Server is shown in the central portion of the screen.
5. If vCenter contains hypervisor information, Sentral imports hypervisor information. To manually add hypervisor information, click \texttt{Skip vCenter} and manually enter hypervisor information.

14.2: About the Virtualization Wizard
Use the Virtualization Wizard to create and manage VM pools. You can use the Virtualization Wizard to:

- \textbf{Select vCenter}
  Use this screen to add vCenter information and import hypervisor information.

- \textbf{Configure Hypervisors}
  Select or add a hypervisor from a selected vCenter. Sentral retrieves hypervisor information from the selected vCenter.
• Select Clusters
  Use this screen to select clusters to modify or delete.

• Configure templates
  Select and configure a VM to use as a golden image. Sentral creates a VM pool from the golden image.

• Configure VM Pool
  Use the template to specify the number of VMs to create in the pool and start configurations. This creates VM pools that administrators can manage from Sentral.

### 14.2.1: Creating a Cluster

A cluster is a grouping of ESXi hosts (hypervisors) administered collectively by vCenter Server. Each hypervisor hosts View desktops. Administrators can use clusters to guard against physical server failures. To create a cluster:

1. Add a vCenter instance and hypervisors to the Sentral environment as shown in 14.1: “Integrating VMware vCenter Server” above

   **NOTE:** Clusters must contain two hypervisors or more.

   **NOTE:** You must have vCenter licenses available to create clusters.

2. After adding vCenter and hypervisors, click Next to display the Cluster Management Wizard.

   **NOTE:** The Cluster Management Wizard is available only after adding a vCenter instance to the Sentral environment.

3. Enter the details for the cluster, and then click **Add**. The cluster is displayed in the upper portion of the screen.

   ![Figure 12. The Cluster Details screen](image-url)
14.2.2: Modifying or Deleting a Cluster
The steps below show how to modify or delete a cluster.

1. From the Cluster Management screen, select and right-click a cluster to display the right-click menu. Choose one of the following:
   - To delete a cluster: click Delete from the right-click menu.
   — OR —
   - To modify a cluster: click Modify from the right-click menu.
     a. Select a hypervisor from the lower portion of the screen.
     b. Click the arrow buttons to move hypervisors into or out of a cluster.

2. Click Next to display the Template Management screen. You can now use clusters to group hypervisors into resource pools. (As noted above, vCenter licenses must be available.)

14.3: Creating VM Pools
The sections below show how to integrate a hypervisor into your Sentral environment, create VM templates from Sentral, and create VM pools.

14.3.1: Adding a Hypervisor
Sentral supports ESX and Xen hypervisors. The steps below show how to add an existing hypervisor to your Sentral environment.

1. From the main menu, click Management > Virtualization > Hypervisors.

2. Right-click an open space and select Add Hypervisor. The picture below shows the right-click menu.

3. Enter the hypervisor information. The table below shows each field.

   Table 18. The Hypervisor Information fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IP</td>
<td>Enter the IP address of the hypervisor.</td>
</tr>
<tr>
<td>Host Port</td>
<td>Enter the port for the hypervisor’s IP address (in many instances, the default port is 8080).</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the hypervisor administrator’s user name (in many instances, the default is root).</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the hypervisor administrator’s account.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the hypervisor manufacturer (XEN or vSphere ESXi)</td>
</tr>
</tbody>
</table>

4. Click Save ( ).
Sentral Quick Start Guide

Result: The hypervisor appears in the upper portion of the screen and any existing VMs appear in the hierarchical tree. You can now manage VMs using the right-click menus from the hierarchical tree or by clicking Management > Virtual Machines > All Virtual Machines.

14.3.2: Verify Connection to Hypervisor
After integrating a hypervisor to your Sentral environment, check the connection between Sentral and the hypervisor.

1. From the main menu, click Management > Virtualization > Hypervisors to display the Hypervisors Information screen.
2. Select a row containing your hypervisor from the upper portion of the screen.
3. Right-click the row and select Check Connection from the drop down menu. This command attempts to contact the hypervisor and retrieve hypervisor-related information.

Result: A success message should appear. Click OK to dismiss the message.

If the hypervisor does not connect successfully, ensure that the hypervisor’s IP address is correct and the login credentials are correct.

14.3.3: Viewing Hypervisor Details: Components and Storage Capacity
You can view information about hypervisor components and storage capacity.

1. From the main menu, click Management > Virtualization > Hypervisors to display the Hypervisors Information screen.
2. Select a row containing your hypervisor from the upper portion of the screen.
3. Right-click the hypervisor and select an option from the menu. The table below shows options to click and the information the options provide.

<table>
<thead>
<tr>
<th>Click …</th>
<th>To …</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Capacity</td>
<td>View information about the hypervisor components, including memory, processors, NICs, and drives.</td>
</tr>
<tr>
<td>Show Storage Information</td>
<td>View details about hypervisor storage devices, including hard drives, local storage, and repositories.</td>
</tr>
</tbody>
</table>

14.3.4: Creating VM Templates
You can create a VM template based on an existing VM (also called a golden VM) that you will use repeatedly to create other VMs.
14.3.4.1: Prerequisites

Before adding a VM to a template, ensure that:

- The ClearCube Host Agent is on the VM (see 13.1: “Installing Sentral Host Agent” above).
- Remote Desktop access is enabled on the VM (see 5.4: “Enabling Endpoint Devices for Remote Access” above).
- Appropriate ports are open on the VM (see 5.5: “Configuring Network Ports” above).
- You have discovered the VM in your Sentral environment (see 14.4: “Device Discovery” below).
- SSH is enabled on the hypervisor (see your hypervisor documentation for information).

14.3.4.2: Creating a VM Template

1. From the main menu, click Management > Virtualization > Hypervisors to display the Hypervisors Information screen.
2. Select a row containing your hypervisor from the upper portion of the screen.
3. Right-click the hypervisor and select View Templates to display the Templates Management screen. Any existing templates appear in the upper portion of the screen.
4. Right-click an empty space and select Add Template.

   **Result:** Sentral displays the Template Wizard.

5. Complete the Template Wizard fields. After completing each section of the wizard, click Next to continue. The table below shows all wizard fields.

<table>
<thead>
<tr>
<th>Template Configuration screen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Server</td>
</tr>
<tr>
<td>Virtual Machine</td>
</tr>
<tr>
<td>Storage</td>
</tr>
</tbody>
</table>
### VM Configuration screen

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Administrator Username</td>
<td>Enter the user name for a local Administrator account on the VM you specified as the golden image (in the Virtual Machine field above).</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the local Administrator you specified in the previous field.</td>
</tr>
<tr>
<td>Language</td>
<td>Select a language for the VM operating system to use.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Select a time zone for the VM.</td>
</tr>
</tbody>
</table>

### Domain Configuration screen

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workgroup</td>
<td>Select this option to ensure VMs created from the template are included in a Windows workgroup.</td>
</tr>
<tr>
<td>Domain Name (FQDN)</td>
<td>To have VMs created from a template join a Domain, clear the Workgroup option and specify the fully qualified domain name (FQDN) here.</td>
</tr>
<tr>
<td>Domain Administrator</td>
<td>To have VMs created from a template join a Domain, clear the Workgroup option, and enter the Domain administrator’s user name here.</td>
</tr>
<tr>
<td>Domain Password</td>
<td>To have VMs created from a template join a Domain, clear the Workgroup option, and enter the Domain administrator’s password here.</td>
</tr>
</tbody>
</table>

### CPU Configuration screen

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of vCPUs</td>
<td>Enter the number of virtual CPUs for VMs here. The maximum number is 16.</td>
</tr>
<tr>
<td>Memory (MB)</td>
<td>Enter the total memory for VMs (in MB) here. The maximum size is 131036 MB.</td>
</tr>
</tbody>
</table>

### Storage Configuration screen

Select or add a virtual storage for the VM here.

### Network Configuration screen

Select a network configured on the hypervisor.

6. Click **Finish** to begin creating the template. Progress messages appear. After several minutes, a success message appears. Click **OK** to dismiss the message.

Now use the template to create a *pool* of identical VMs. See the section below for instructions.
14.3.5: Creating VM Pools

A VM pool is a collection of identical VMs. You can create VM pools using a VM template as described in the previous section. The steps below show how to create a VM pool.

1. From the main menu, click Management > Virtualization > Hypervisors. Right-click an empty space in the upper portion of the screen, and select View VM Pools.

2. Right-click an empty space and select Add VM Pool (as shown in the picture below).

![Add VM Pool](image)

*Figure 13. Selecting the Add VM Pool option from the VM Pools Management screen*

**Result:** Sentrail displays the Add VM Pool wizard.

3. Complete the Template wizard fields. After completing each section of the wizard, click Next to continue. The table below shows all wizard fields.

<table>
<thead>
<tr>
<th>VM Pool Configuration screen</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Select the IP address of the hypervisor that contains the VM Template.</td>
</tr>
<tr>
<td>Name</td>
<td>Sentrail creates a group with this name that contains the VMs you create. Sentrail displays this group in the hierarchical tree.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Enter a prefix for the name of VMs in the VM pool, which will appear before a dash (-) and a sequence of ascending numbers starting with -000. For example, if you entered Sales in the Prefix field, VMs are named Sales-000, Sales-001, Sales-002, and so on.</td>
</tr>
<tr>
<td>No of VMs</td>
<td>Enter a number of VMs to create in the VM pool.</td>
</tr>
<tr>
<td>Template</td>
<td>Select the template to use for the VMs you are creating.</td>
</tr>
<tr>
<td>Storage</td>
<td>Select the storage to use for the VMs you are creating.</td>
</tr>
<tr>
<td>Type</td>
<td>This setting indicates the allocation type (Dedicated or Shared) for the VMs in the group. See 14.11: “About Allocations and Allocation Types” below for information about allocation types.</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CPU Configuration screen</td>
<td>Enter the number of virtual CPUs for VMs here. The maximum number is 16.</td>
</tr>
<tr>
<td>Memory (MB)</td>
<td>Enter the total memory for VMs (in MB) here. The maximum size is 131036 MB.</td>
</tr>
</tbody>
</table>

**Storage Configuration screen**

Select or add a virtual storage for the VM here.

**Network Configuration screen**

Select a network configured on the hypervisor.

4. Click **Finish** to begin creating VMs. Progress messages appear. After several minutes, a success message appears. Click **OK** to dismiss the message.

If there are hardware-related issues (such as insufficient storage), messages are displayed. When the VM creation process is complete, Sentral adds the VM pool to the Sentral hierarchical tree. The group ( ) contains the VMs ( ) you created. The picture below shows the hierarchical tree with a VM pool and VMs. The picture below shows the Sentral hierarchical tree with a VM pool (in this example, 1st Floor VMs) containing VMs (Home Office-000 and so on).

![Hierarchical tree showing a VM pool (1st Floor VMs) and VMs (Home Office-000, and so on)](image)

*Figure 14. Hierarchical tree showing a VM pool (1st Floor VMs) and VMs (Home Office-000, and so on)*
14.4: Device Discovery

You must discover devices and users in your Sentral environment to perform any management operations. Sentral enables you to discover zero clients, host blades, host cards, users, and more. After discovering devices and users, Sentral displays them in the hierarchical tree (shown below).

The steps below show how to perform a discovery from the Sentral menu.

1. Click Setup > Run Discovery.

2. Create a subnet range by right-clicking an empty space and selecting New Subnet.

3. From the lower portion of the screen (titled Subnet), complete the fields. Name the subnet range and specify a starting and ending IP address. The starting and ending addresses must be valid IPv4 addresses in standard, dotted-decimal notation (for example, 192.168.1.1).

4. Click Save ( ).

   **Result:** The subnet range appears in the Discovery portion of the screen.

5. Select and then right-click the subnet containing devices you want to discover. Select Device Discovery.

   **Result:** The Discovery Options dialog box appears.

6. Select one or more device types to discover (for example, Sentral Host Machines and PCoIP-enabled Devices). Click Discover.

   **Result:** An animated progress bar, located in the lower-right portion of the screen, appears during discovery. The discovery process can be lengthy. Be sure to allow the discovery to complete. Note that the discovery process configures devices to poll Sentral Server.

When the discovery process completes, all discovered devices appear in the hierarchical tree. See the section below about management options you can perform from the hierarchical tree, and see 14.6: “Search Options” below for information about finding devices.
14.5: Hierarchical Tree and Right-Click Management Options

After discovering endpoint devices, Sentral displays them in the hierarchical tree, located in the left side of the Sentral Console. The tree contains all discovered devices, groups, and users. The picture below shows the hierarchical tree.

![Hierarchical Tree and Right-Click Management Options](image)

*Figure 16. The right-click menu for blades with PCoIP host cards*

The table below shows the group, device, and user icons displayed in the hierarchical tree (icons showing a red X are offline, or have not reported to the console in the specified timeout period).

<table>
<thead>
<tr>
<th>Icon</th>
<th>Definition and Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>![CCT Icon]</td>
<td>CCT Node. This node contains all discovered devices and any nodes that administrators create. You cannot delete the CCT node, and you cannot edit the CCT name. (CCT refers to ClearCube Technology, Inc.)</td>
</tr>
<tr>
<td>![User Defined Group Icon]</td>
<td>User-defined group. Groups contain a collection of items. Group do not have to be homogenous, and can contain any combination of devices and nodes. You can move multiple devices from one group to another using CTRL+Click or SHIFT+Click operations.</td>
</tr>
<tr>
<td>![A-Series Chassis Icon]</td>
<td>A-Series chassis without Dual Power Input Module</td>
</tr>
<tr>
<td>![A-Series Chassis Icon]</td>
<td>A-Series chassis with Dual Input Power Module All AC inputs receiving power</td>
</tr>
<tr>
<td>![A-Series Chassis Icon]</td>
<td>A-Series chassis with Dual Input Power Module Primary or failover AC input without power</td>
</tr>
<tr>
<td>![A-Series Chassis Icon]</td>
<td>A-Series chassis with Dual Input Power Module Primary and failover AC inputs without power</td>
</tr>
<tr>
<td>Icon</td>
<td>Definition and Notes</td>
</tr>
<tr>
<td>------</td>
<td>---------------------</td>
</tr>
<tr>
<td><img src="image" alt="A-Series chassis" /></td>
<td>A-Series chassis</td>
</tr>
<tr>
<td><img src="image" alt="A-Series blade without PCoIP host card" /></td>
<td>A-Series blade without PCoIP host card</td>
</tr>
<tr>
<td><img src="image" alt="A-Series blade with dual-monitor PCoIP host card" /></td>
<td>A-Series blade with dual-monitor PCoIP host card</td>
</tr>
<tr>
<td><img src="image" alt="A-Series blade with tri-monitor PCoIP host card" /></td>
<td>A-Series blade with tri-monitor PCoIP host card</td>
</tr>
<tr>
<td><img src="image" alt="A-Series blade with quad-monitor PCoIP host card" /></td>
<td>A-Series blade with quad-monitor PCoIP host card</td>
</tr>
<tr>
<td><img src="image" alt="R-Series blade without PCoIP host card" /></td>
<td>R-Series blade without PCoIP host card</td>
</tr>
<tr>
<td><img src="image" alt="R-Series blade with dual-monitor PCoIP host card" /></td>
<td>R-Series blade with dual-monitor PCoIP host card</td>
</tr>
<tr>
<td><img src="image" alt="R-Series blade with tri-monitor PCoIP host card" /></td>
<td>R-Series blade with tri-monitor PCoIP host card</td>
</tr>
<tr>
<td><img src="image" alt="R-Series blade with quad-monitor PCoIP host card" /></td>
<td>R-Series blade with quad-monitor PCoIP host card</td>
</tr>
<tr>
<td><img src="image" alt="R-Series chassis" /></td>
<td>R-Series chassis</td>
</tr>
<tr>
<td><img src="image" alt="PCoIP host cards (dual-, tri-, and quad-monitor)" /></td>
<td>PCoIP host cards (dual-, tri-, and quad-monitor)</td>
</tr>
<tr>
<td><img src="image" alt="Zero client (dual- and quad-monitor)" /></td>
<td>Zero client (dual- and quad-monitor)</td>
</tr>
<tr>
<td><img src="image" alt="Thin client" /></td>
<td>Thin client</td>
</tr>
<tr>
<td><img src="image" alt="Virtual machine (vendor noted in display)" /></td>
<td>Virtual machine (vendor noted in display)</td>
</tr>
<tr>
<td><img src="image" alt="Active Directory group" /></td>
<td>Active Directory group</td>
</tr>
<tr>
<td><img src="image" alt="User" /></td>
<td>User</td>
</tr>
<tr>
<td><img src="image" alt="IPMI-enabled device" /></td>
<td>IPMI-enabled device</td>
</tr>
</tbody>
</table>

**Offline Nodes**

Offline devices appear with a red ✗, as shown below.
Right-click endpoint devices in the hierarchical to display common management options (see Figure 16 and Figure 17). The sections below show right-click menu options.

14.5.1:  **Blade with PCoIP Host Card**
The table below shows right-click menu options for blades with PCoIP host cards.

**Table 20. Right-click menu options for blades with host cards**

<table>
<thead>
<tr>
<th>Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure</td>
<td>Displays the Configure Physical Machines Management screen.</td>
</tr>
<tr>
<td>View Health &amp; Status</td>
<td>Displays the Health and Status – Physical Machines screen.</td>
</tr>
<tr>
<td>Advance PCoIP Configuration</td>
<td>Displays the PCoIP Client Host interface, from which you can configure all PCoIP options.</td>
</tr>
<tr>
<td>Allocate host with Thin Client</td>
<td>Displays the Connection Brokering – Mappings screen. See 14.11: “About Allocations and Allocation Types” below for details.</td>
</tr>
<tr>
<td>Remote Control</td>
<td>Enables administrators to log in to the blade remotely. Ensure you installed VNC during Host Agent installation, and have the password specified during VNC installation. See 13.1.1: “Windows” above for details about the VNC portion of Host Agent installation.</td>
</tr>
<tr>
<td>Remove Node</td>
<td>This option removes the host from the hierarchical tree. The host reappears when it polls Sentral Server.</td>
</tr>
<tr>
<td>Wake on LAN</td>
<td>Sends a Wake on LAN packet to the host.</td>
</tr>
<tr>
<td>Restart</td>
<td>Restarts the blade’s operating system.</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Shuts down the blade’s operating system.</td>
</tr>
<tr>
<td>Delete Node</td>
<td>This option deletes the host from the hierarchical tree and the Sentral Database. Shut down the blade before selecting this option. You must discover the device again to include it in your environment.</td>
</tr>
<tr>
<td>Rediscover Node</td>
<td>Rediscovers the blade (does not affect the host card).</td>
</tr>
</tbody>
</table>

14.5.2:  **Zero Clients**
The table below shows the zero client right-click menu options.

**Table 21. Zero client right-click menu options**

<table>
<thead>
<tr>
<th>Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced PCoIP Configuration</td>
<td>Displays the PCoIP Client Web interface, from which you can configure all PCoIP options.</td>
</tr>
<tr>
<td>Rename Device</td>
<td>Allows you to create an alias for the zero client.</td>
</tr>
<tr>
<td>Map Thin Client to</td>
<td>Displays the Connection Brokering – Mappings screen. See 14.11: About...</td>
</tr>
<tr>
<td>Physical Machine</td>
<td>Allocations and Allocation Types below for details.</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Reset</td>
<td>Power cycles the zero client.</td>
</tr>
<tr>
<td>Disconnect Device</td>
<td>Disconnect a zero client’s active session (see 15: “When Users Move from One Location to Another” below for a usage example).</td>
</tr>
<tr>
<td>Remove Node</td>
<td>This option removes the client from the hierarchical tree. The client reappears when it polls Sentral Server.</td>
</tr>
<tr>
<td>Delete Node</td>
<td>This option deletes the client from the hierarchical tree and the Sentral Database. You must discover the device again to include it in your environment.</td>
</tr>
<tr>
<td>Set Peer</td>
<td>Enables you to set the IP address of a peer host card (useful in deployments that do not use connection brokering).</td>
</tr>
<tr>
<td>Clear Peer</td>
<td>Clears the peer address if it is present on the zero client.</td>
</tr>
<tr>
<td>Set View Connection Server</td>
<td>Sends the View Connection Server parameters (specified in the Configuration screen) to the client. See 9.14.3: “VMware View Connection Server Settings” above for details.</td>
</tr>
<tr>
<td>Rediscover Node</td>
<td>Rediscover the zero client and applies a Client Profile.</td>
</tr>
<tr>
<td>View Profile</td>
<td>Displays the Client Profile applied to the device. See 14.8: “Configuring Endpoints Using Client Profiles” below for more information.</td>
</tr>
<tr>
<td>Change Static IP</td>
<td>Displays field to manually enter an IP address. Be sure that the IP address does not conflict with other devices on the network. Click OK to assign the IP address to the zero client.</td>
</tr>
</tbody>
</table>

![Figure 17. The zero client right-click menu options](image)

Rev H 2.4.09.05.2018
14.6: Search Options
Sentral enables you to search for devices in the hierarchical tree, the Connection Brokering screen, and within the PCoIP Event Log Screen.

<table>
<thead>
<tr>
<th>To search the ...</th>
<th>Then ...</th>
<th>Perform These Steps ...</th>
<th>To Clear Results ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchical tree</td>
<td>Navigate to the hierarchical tree.</td>
<td>Right-click the CCT group in the hierarchical tree and select <strong>Search Tree</strong>. From the text box, enter any part of a device name to find and click <strong>OK</strong>.</td>
<td>Right-click the CCT group and select <strong>Refresh</strong>.</td>
</tr>
<tr>
<td>Connection Brokering screen</td>
<td>Click <strong>Connection Brokering &gt; Allocation</strong>.</td>
<td>Search for devices or users in Dedicated Allocations by entering any text and clicking the magnifying glass icon.</td>
<td>Clear the text box and click the magnifying glass icon (🔍) again.</td>
</tr>
<tr>
<td>PCoIP Event Log</td>
<td>Click <strong>Reports &gt; PCoIP Events Log</strong>.</td>
<td>Search any field by entering text in the <strong>Filter</strong> text box and pressing the <strong>Enter</strong> key.</td>
<td>Clear the text box and press the <strong>Enter</strong> key again.</td>
</tr>
</tbody>
</table>

14.7: Creating Groups and Subgroups (Required for All Management Tasks)
Devices and users must be in a Sentral group to perform management tasks on them. Select and drag any device or node to a group to place it in the group. To create a group:

1. Right-click the **CCT** node (located at the top of the hierarchical tree).
2. Select **Add Group**.
3. Complete the group name fields and then click **Add Group**.
4. Optionally, create a subgroup. Right-click a group and perform the steps above.
14.8: Configuring Endpoints Using Client Profiles

The sections below show how to configure Sentral client (zero clients and thin clients) using Client Profiles.

14.8.1: About Client Profiles

Client profiles enable administrators to apply a device-level configuration to groups of clients through a RESTful API call, rather than configuring clients individually. There are two profile types:

**Thin Client Agent profile**

For thin clients in your Sentral environment. These profiles include configuration options for the Thin Client Agents deployed on thin clients and configuration options for the RDP (RDC) protocol that thin clients use.

**PCoIP profile**

For PCoIP zero clients in your Sentral environment. PCoIP profiles include configuration options for the following areas:

- PCoIP session
- PCoIP device discovery
- Network
- SNMP
- Displays
- Display topology
- Device power
- * PCoIP Host Software Driver
- * USB device permissions (mass storage lockout)

* See **PCoIP Zero Client and Host Administrator Guide** (techsupport.teradici.com) for detailed information about Host Software and USB authorization.

14.8.2: Default Client Profiles

Sentral applies a default Client Profile whenever you discover a zero client or thin client. The default profiles are:

- **PCoIPProfile**: the default Client Profile for PCoIP zero clients.
- **TCAPProfile**: the default Client Profile for thin clients.

You cannot edit or delete default profiles. Since the default profile is always applied when you discover a device, you can create custom profiles and apply them to groups of devices so devices are configured appropriately for your environment (for example, with a particular subnet and IP address, session type, and more).

14.8.3: Creating Profiles

If you have specific configuration requirements for groups of zero clients or thin clients (for example, clients used in particular departments, locations, or for types of users), you can create
custom profiles for those devices. Create a Sentral group for these devices, add the devices to the group, and then apply a custom profile to all of the devices in the group. You can apply a profile to any number of device groups (multiple groups can use the same profile).

**Create a New Profile**

1. From the main menu, click **Management > Client Profiles**.
   
   **Result:** The Profile Management screen appears

2. Right-click an empty area in the main window and select:
   
   - **Create new PCoIP Profile** for zero clients
   
   — OR —
   
   - **Create new Thin Client Agent Profile** for thin clients

3. Complete the profile fields and then click **Save ( )**. See 21: “Client Profile Field Descriptions” below for details about all Client Profile field descriptions.

   **Result:** A success message appears. Click **OK** to return to the previous screen.

**14.8.4: Apply a Profile to a Group**

This section shows how to apply a profile to a group.

1. From the main menu, click **Management > Client Profiles**.

2. Select and right-click the profile you want to apply to a Sentral group.

3. Select **Apply Profile to Group**.

4. From the Applicable Group Names column in the lower portion of the screen, select the name of the group to which you want to apply the profile.

5. Click the **right arrow ( )** to move the group name to the Applied Group Names column.

6. Click **Save ( )**. The status bar at the lower-right portion of the screen displays a message indicating that profile synchronization is complete.

**14.8.5: View the Profile Applied to a Device**

To view the Client Profile applied to a client, right-click the client in the hierarchical tree and select **View Profile**.

1. From the hierarchical tree, right-click a zero client or thin client icon.

2. Select **View Profile**. A progress bar appears.

   (If Sentral displays a message indicating that the device is not responding, the device might
be offline or has not polled Sentral Server. Right-click the client, select Rediscover Node, and then try viewing the profile again.)

3. Sentral displays the Client Profile applied to the client. The device’s IP address is shown at the top of the screen.

4. Optionally, click the Push Latest Profile button ( ), located on the upper-left portion of the screen, to apply the profile currently associated with the group. You must restart the thin client to complete applying the profile. If the thin client is not part of a Sentral group when you click the Push Latest Profile button, Sentral applies the default profile (TCAProfile) to the thin client.

14.9: Renaming Zero Clients (I/Ports)
For ease of management, it is a best practice to rename I/Ports (zero clients and thin clients) with an alias that allows you to identify them quickly. For example, an alias could be the I/Port’s desk or user location.

To rename zero clients (I/Ports):
1. From the hierarchical view, located on the left portion of the screen, right-click a zero client.
2. Select Rename Device.
3. Specify a new name and click OK.

14.10: Discovering and Adding Device Users
In Sentral environments, device users are the users defined in Windows user groups. Discover users in your environment and place them in logical groups. This process requires:

1. Discovering users
2. Creating a group or groups for users
3. Populating groups with discovered users

The sections below show how to perform these steps.

14.10.1: Specifying the User Type to Discover
You can discover Windows Domain users and Local Workgroup users. Specify the type of users to discover in the Configuration screen’s Discovery User Preference field.

1. From the main menu, click Setup > Configuration.
2. From the Discovery section in the right-hand column, verify your setting in the Discovery User Preference drop-down menu. Select Local to discover local users, and select Domain to discover Domain users. The picture below show the Discovery portion of the screen.
Figure 18. Selecting the User Discovery Preference

**NOTE:** You cannot discover Local and Domain users at the same time.

3. Click **Save** ( ). If you changed the user discovery type, Sentral displays a dialog box, asking if you want to delete any old user information.

   Click **Yes** to delete existing user and device data from the database. Running a discovery automatically repopulates these users and devices (see 14.4: “Device Discovery” above), on the specified network type (Local Workgroup or Domain). If you select **No**, your database can contain inaccurate information for the chosen authentication type, such as duplicate user names.

4. Ensure that all of the following are set for Domain or Local authentication according to the discovery preference you specified in step 2.
   - **Login on computer running Sentral Console**
     You logged in to a Local Workgroup or into a Domain, as appropriate, on the computer running Sentral Console.
   - **Server authentication**
     Authentication for the Sentral Server service you are using (Apache Tomcat or IIS) is set to Local Workgroup or to Domain (as appropriate).
   - **Sentral Console login**
     From the Sentral Console, ensure the login type shown in the Domain field matches the setting in the Discovery User Preference you specified above. The picture below shows the Sentral Console’s Domain field.

   ![Figure 19. Selecting the type of login for Sentral Console user](image)

You can now discover Windows users.
14.10.2: Discovering Users
The steps below show how to discover Sentral users.

1. From the main menu, click **Setup > Run Discovery** to display the Discovery screen.
2. Right-click an empty space in the upper portion of the screen and select **Discover Users**.
3. Click **Submit** to run the discovery. Sentral displays the Discovered Users screen.

**NOTE:** User discovery can take some time if your environment contains a large number of users.

Use the scroll bar on the right-hand side of the screen to view up to 100 users. If the discovery contains more than 100 users, you can:

- Select additional pages in the **Page #** drop-down box located near the bottom of the screen.
- Use the navigation buttons, located near the bottom of the screen, to move to the first page of users, the last page of users, or to move forward or backwards one page at a time.

You can now continue by adding the users you discovered to Sentral groups, as described in the following section.

14.10.3: Adding a User to Sentral
This section shows how to add users to Sentral (see the following section for instructions about adding large numbers of users).

1. From the main menu, click **Setup > Configuration**.
2. Click the **Add Users** icon ( ).
3. Enter a user name in the **User Name** field, select a **Security Group** for the user, and ensure the selection in the **Domain** drop-down menu is appropriate.
4. Click the **Save** icon ( ), and Sentral displays a confirmation message. Click **OK**. The user now appears in the upper portion of the screen.
5. Click **Management > Groups**.

**NOTE:** If you do not already have a group specified for users, create one from the hierarchical tree by right-clicking the **CCT** group, selecting **Add Group**, and specifying a name and additional details. Then click **Add Group**.

6. From the list of groups in the upper portion of the screen, right-click the row containing the group to which you are adding users. Select **Manage User Group**.
7. On the Connection Brokering – User Groups (New) screen, select the group again, right-click, and select **Add User**.

Rev H 2.4.09.05.2018 67
8. From the Group Name list, select the security group you specified for the user in step 3. Sentral displays all users in the group.
9. From the lower portion of the screen, select the user you want to add, and then select the group to which you want to add the user.
10. Click the Add User icon ().

The user appears in the selected group in the hierarchical tree and is now available for allocation to devices.

14.10.4: Adding a Large Number of Users

Add a large number of users to Sentral by creating user records directly in the Sentral Database.

**NOTE:** You can use this method to add users through batch scripts.

The high-level instructions below assume your Sentral Database is a MySQL database.

![Adding users directly through Sentral Database](image)

Figure 20. Adding users directly through Sentral Database
1. From the Sentral Database, open the `discovereduser` table.

2. Add a new record for each user in the format: `Username, SecurityGroups, DomainName, TypeID`. For Sentral Database, use the values shown below, where `User Name` is the name of each user:

   `User Name, Users, Local, 5`

3. Perform steps 5 to 10 as shown in the previous procedure.
14.11: About Allocations and Allocation Types

Allocations assign client devices and users in your Sentral deployment to specific hosts (individual or dedicated allocations) or to a group of devices (shared or group allocations).

Administrators can easily modify allocations to allow for changing business needs. The list below shows the types of allocations:

**Individual/Dedicated**

Connects the user or client device to the same assigned host or VM each time.

Administrators can also allocate a client to a specific host in a group. To do so, mark the group that contains the host computer as a dedicated group. The allocated computer should not be part of any other allocations.

You cannot allocate clients and users to more than 10 resources. You can configure the number of allocations allowed from the Sentral Configuration screen (see the Number of allocations allowed setting in 9.14.4: “Additional Miscellaneous Settings: Server Switchover and Allocation” above).

**Shared/Group**

Connects the user or client device to the best available host or VM in a shared group. Sentral uses a least load average algorithm to determine the best host or VM to assign to the user.

**Device-based allocation**

A device is associated with (mapped to) a specific host or a group of hosts.

In previous Sentral releases, when a client devices was allocated to a shared resource group, all free hosts were retrieved and displayed to users when they attempted to connect to a host. Now, Sentral provides only one host out of every shared group when a client attempts to connect. Allocated hosts are only available for a specified time (available from the Sentral Configuration screen). If a user attempts to connect after the allocation expires, Sentral notifies the user and they must retrieve the allocation again by attempting to reconnect (see the Allocation Timeout setting in 9.14.4: “Additional Miscellaneous Settings: Server Switchover and Allocation” above).

**User-based allocation**

A user is associated with (mapped to) a specific computer or a group of computers. Once allocated, client devices and user accounts automatically connect to a specified host or group of hosts.
14.12: Creating Allocations (Mapping Devices and Users)
Allocating clients and users to physical and virtual machines includes these tasks:

- Creating user or device groups
- Adding resources to the groups
- Assign allocations—this is mapping, or assigning, a user or client device (or groups of them) to a computing resource (or to groups of them.)

14.12.1: Creating Device-Based Allocations
The steps below show how to allocate clients to blades (a zero client to a blade in this example). Perform the same process to allocate zero clients or thin clients to virtual machines or PCoIP host cards.

NOTE: To allocate devices they must be in a group as shown 14.7: “Creating Groups and Subgroups (Required for All Management Tasks)” above.

1. From the Sentral menu, click **Connection Brokering > Allocation**.
2. From the upper-left portion of the Mappings area, click an Allocation tab:
   - **Individual Allocation**—Shows each discovered client. Select one client from the list to allocate to a device.
   - OR—
   - **Grouped Allocation**—Shows groups of Sentral clients. Select a group of clients to allocate to a group of devices (Physical Machines, Virtual Machines, or Host Cards).
3. Click the **Clients** tab.
4. From the Thinclient column, click the **client** you want to allocate.

5. From the pane on the right, select the tab for the type of host to allocate the device to:
   - **Physical Machines**
   - **Virtual Machines**
- **Host Cards** (a physical PCoIP host card in a blade or workstation)

6. From the Hostname or Host Cards column, select the **host** (blade, VM, or PCoIP host card) to allocate the client to

![devices selection pane](image)

7. Click **Allocate**, located on the bottom of the screen. The devices are now allocated. When the client user clicks their client’s Connect button, they will automatically connect to the specified host.

8. Optionally, to delete the allocation, select the **client** or the **host** (physical machine, VM, or host card) and click **Delete Current Allocation(s)** at the bottom of the device selection pane.

Perform the same process to allocate zero clients or thin clients to virtual machines or PCoIP host cards.

### 14.12.2: Creating User-Based Allocations

The steps below show how to allocate a user to a blade. Perform similar steps to allocated users to virtual machines.

1. From the Sentral menu, click **Connection Brokering > Allocation**.

2. From the upper-left portion of the Mappings area, click an Allocation tab:

   - **Individual Allocation**—Shows each discovered user in your environment. Select one user for the list to allocate to a device.
   
   —OR—

   - **Grouped Allocation**—Shows groups of Sentral users. Select a group of users to allocate to a group of devices (Physical Machines, Virtual Machines, or Host Cards).

3. Click the **Users** tab.

4. From the pane on the left, select the **user** (listed in the User Name column) you want to allocate. From the pane on the right, select the **device** (Physical Machine, Virtual Machine, or Host Card) to which to allocate the user.

5. Click **Allocate**, located on the bottom of the screen. The user and host device are now allocated. When the user logs on to any client and connects to a host, they will automatically connect to the specified host.

6. To delete the allocation, select the **user** or the **device** and click **Delete Current Allocation(s)** at the bottom of the device selection pane.
14.12.3: Allocating Client or User Groups to Device Groups

The steps below show how to allocate a group of client or users to any available host device in a device group. Note that groups can be dedicated or shared:

**Dedicated:** Connects the user or client device to the same assigned host or VM each time.

**Shared:** Connects the user or client device to the best available host or VM in a shared group.

1. Run a discovery for one of the following:
   - **Thin clients** (see 14.4: “Device Discovery” above)
   - OR —
   - **Users** (see 14.10: “Discovering and Adding Device Users” above)
2. Create a group for the discovered clients or users as described in 14.7: “Creating Groups and Subgroups (Required for All Management Tasks)” above.
3. Run another discovery to discover hosts for thin clients or users to connect to (see 14.4: “Device Discovery” above). When selecting devices to discover, Sentral Host Machines or PCoIP Enabled Devices.
4. Add discovered devices to groups as described 14.7: “Creating Groups and Subgroups (Required for All Management Tasks)” above.
5. From the main menu, click **Connection Brokering > Allocation** to display the Allocation screen. Client Groups are shown in the left pane, and device groups on the right pane.
6. Select a client or user group from left pane and one device group from right pane. Click the **Allocate** button located at the bottom of the screen. The selected groups are now mapped to each other.

14.13: Recording Device-Related Information (Equipment History)

You can use an equipment history to record information about devices that Sentral manages. An equipment history is a small text-based record, and you can add any number of equipment histories to a device. For example, you could use an equipment history to note a scheduled device repair time, when updates occurred, and so on. The steps below show how to view existing equipment history records, and how to add new equipment history records to Sentral devices.

1. From the main menu, go to the Management screen for the appropriate device:

   *Table 22. Management screen navigation for each device type*

<table>
<thead>
<tr>
<th>For ...</th>
<th>Click ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical machines</td>
<td>Management &gt; Physical Machines &gt; All Physical Machines</td>
</tr>
<tr>
<td>PCoIP Host Cards</td>
<td></td>
</tr>
</tbody>
</table>
2. From the device Management screen, select the row containing the device for which you are viewing or adding an equipment history record. (If a device does not appear, it is not discovered. See 14.4: “Device Discovery” above for information about device discovery.)

3. Right-click the selected row and select View Equipment History.

4. To view an existing equipment history, select the row in the upper portion of the screen.

   Result: The equipment history text appears in the lower portion of the screen. To modify or delete a record, right-click the row and select an option.

5. To create a new equipment history, right-click an empty space in the upper portion of the screen. Select Add Report.

   Result: The New Message portion of the screen becomes active. Click the lower portion of the screen and type any text. The maximum field length is 3,000 characters.

6. Click Save ( ) to save the record, and click OK to dismiss the success message.

   Result: The equipment history appears in the upper portion of the screen.

You can now view equipment history records and run equipment history reports as explain in 19.5: “Equipment History” below.

15: When Users Move from One Location to Another

The steps below show how to move users from one desk to another when using device-based allocation. (See 14.12.1: “Creating Device-Based Allocations” above for information about device-based allocations.)

Before you begin, obtain the MAC addresses of the zero client the user is currently using and of the zero client they will use. MAC addresses are located on zero client labels.

1. From the Connection Brokering > Allocation screen, right-click the zero client (listed in the Thinclient column) and select Disconnect device. (Use the MAC address to help identify the device.)

2. Right-click the zero client that the user is moving to and select Disconnect device.

   NOTE: Disconnect devices to ensure that you do not interrupt active PCoIP sessions.

3. From the user’s new zero client, ask them to enter their user name and click Connect. The zero client display shows the allocated device.

4. Ask the user to click Connect again. The PCoIP session starts.
16: Updating PCoIP Host Card and Zero Client Firmware

The sections below show how to update PCoIP firmware for host cards and zero clients.

16.1: Uploading Files

The steps below show how to upload firmware update files to the Sentral FTP Server.

NOTE: Before you begin, ensure you have:

- Created a group and dragged the devices you want to update to the group (updates is the group name used below; however, you can use any name)
- Placed the PCoIP firmware in a directory you can access from Sentral Console.

1. From the Sentral menu, access the devices you are updating.
   - For blades and host cards: click Management > Physical Machines > PCoIP Hosts.
     — OR —
   - For zero clients: Click Management > Thin Client > PCoIP Thin Clients.

2. Right-click an empty space in the screen and then select PCoIP Firmware Update.

3. Right-click the group you are updating and select New Update. The devices that you dragged to the group appear in the text box.

4. Click Browse to navigate to the firmware file. Select the file and then click Open.

5. Click Update (✔). Sentral uploads the file to the FTP server.
   - A confirmation message appears once the files are uploaded.
   - Sentral then sends the firmware update command to each device.

16.2: Monitoring Progress and Restarting Devices

The steps below show how to use the PCoIP Event Log to monitor update progress and restart devices to complete the update process.

1. From the Sentral menu, click Reports > PCoIP Events Log. Monitor progress from this screen.

2. The PCoIP Event Log displays the message FirmwareupdatedSuccessfully when the update process is complete.

3. Be sure to wait for an additional 10 minutes to ensure that the process completes gracefully.

4. Restart devices.
   - For blades and host cards: Restart blades by removing them from the chassis and reinserting them. Ensure blades power on automatically or by pressing the power button.
     — OR —
   - For zero clients: Power off and then power on the zero client.
17: Creating Custom Views in Sentral
Administrators can create custom views to filter data shown in the console.

![Custom Views](image1.png)

*Figure 21. The View menu with custom views*

The default view in Sentral shows all devices. By creating customized views, you can reduce the amount of information that Sentral Console displays. Custom views can:

- Simplify data management on screen
- Enable administrators to assess targeted information quickly
- Improve console performance.

The steps below show how to create views.

**Before you begin:**
You will add one or more groups to a view in the steps below, so be sure to have groups defined before creating a view. See 14.7: “Creating Groups and Subgroups (Required for All Management Tasks)” above for instructions about creating groups.

1. From the Sentral menu, click **Management > Views**.
2. From the **Defined Views** area in the upper portion of the screen, right-click an empty space and select **Add new View**.

![Add New View](image2.png)

*Figure 22. Right-click and select Add new View*
3. Give the view a name in the **View Name** field.

4. Select the **group(s)** that you want to include in the view (SHIFT+Click and CTRL+Click to select multiple groups).

![Figure 23. Selecting groups to include in a custom view](image)

5. Click the **right arrow** to move the groups you are including in the view the right panel.

6. Click the **Save** button. Sentral displays the **New view has been added** message.

7. Click **OK**. The view is now available from the **View** drop-down menu in the upper-right portion of the console (see **Figure 21** above).
18: Additional Logging
This section shows additional logging information available from Sentral Console.

18.1: Viewing Sentral Activity (View All Logging Screen)
The Reports - Logging screen shows all Sentral administrator and user activity. The list below shows how to view the screen:

1. From the main menu, click Reports > Alerts.
2. Right-click an empty area of the screen and select View All Logging to display the Reports - Logging screen.
3. From the right-click menu, you can:
   - Clear Selected Logs: select a log or multi-click to select more than one log
   - Clear All Logs
   - Export Logs: this option exports all logs. From the dialog box, enter a file name, specify a file format (.CSV, .XML, or .MIF), and click Save.
   - Export Selected Logs: this option exports the logs you have selected. From the dialog box, enter a file name, specify a file format (.CSV, .XML, or .MIF), and click Save.

18.2: PCoIP Events Log
This log records events performed by PCoIP devices in a Sentral environment.

To view the PCoIP Device Event Logging screen from the main menu, click Reports > PCoIP Events Log.

Use the screen’s right-click menu to perform screen-related tasks. The table below shows right-click menu options and page controls.

Table 23. Right-click menu options for the PCoIP Events Log screen

<table>
<thead>
<tr>
<th>Options and Controls</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>Refreshes the logging screen</td>
</tr>
<tr>
<td>Delete all record(s)</td>
<td>Deletes all records in the logging screen</td>
</tr>
<tr>
<td>Delete selected record(s)</td>
<td>Deletes only selected records (rows) in the logging screen</td>
</tr>
<tr>
<td>Clear selected records(s)</td>
<td>Reserved for future use</td>
</tr>
<tr>
<td>Details</td>
<td>Reserved for future use</td>
</tr>
<tr>
<td>Options and Controls</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Debug</td>
<td>Reserved for future use</td>
</tr>
<tr>
<td>Page navigation buttons</td>
<td>If there are multiple pages of logs, click these buttons to scroll through each page.</td>
</tr>
<tr>
<td>Page # drop-down menu</td>
<td>If there are multiple pages of logs, click this drop-down menu to display a specific page.</td>
</tr>
<tr>
<td>Auto Refresh (seconds)</td>
<td>The settings here specify the time, in seconds, that the event log refreshes. If you select manual from the right-click menu, the page refreshes only when you select refresh from the right-click menu.</td>
</tr>
<tr>
<td>Generate Popup</td>
<td>Select this option to display PCoIP overlays (alerts) on the Sentral Console.</td>
</tr>
<tr>
<td>Filter</td>
<td>Enter text in this field to display only log events that contain the text you enter.</td>
</tr>
</tbody>
</table>
19: Generating Reports
You can generate various reports about devices in your Sentral environment. From Sentral Console, you can generate the reports shown below:

Table 24. Sentral device-related reports

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection History</td>
<td>This report details every user connection to a host in the Sentral environment.</td>
</tr>
<tr>
<td>Inventory</td>
<td>This report details all of the components in host devices (physical hosts and VMs). Details include hardware components, BIOS, network IDs, installed applications, running processes, and more.</td>
</tr>
<tr>
<td>Reports Scheduler</td>
<td>This report details all scheduled Inventory Reports.</td>
</tr>
<tr>
<td>Alerts</td>
<td>This report details all deployed alerts.</td>
</tr>
<tr>
<td>Equipment History</td>
<td>This report details all equipment history records on Sentral devices. Equipment history records are text records Sentral users can add to devices for any user-defined record-keeping tasks.</td>
</tr>
<tr>
<td>Device Accessibility</td>
<td>This report details the communication protocols that various devices use in your Sentral environment.</td>
</tr>
<tr>
<td>Profile Status</td>
<td>This report details the Client Profiles on clients and any synchronization issues.</td>
</tr>
</tbody>
</table>

The sections below show how to create each report.

19.1: Connection History
The Report – Connection History screen (available from the Alerts screen) shows a history of host usage. The Host Agent sends connection events, shown in this screen, when users log in to a host’s operating system. Events are not generated if a user is already logged in to a host when a session is established, or if a session is established and a user does not log in to the operating system.

1. From the main menu, click Reports > Alerts.
2. Right-click an empty area of the screen and select Connection History to display the Report – Connection History screen.
3. You can create a report for one or more devices:
   - To include all devices: Right-click an empty portion of the screen and select Export Report.
To include specific devices: select one or more devices (create a multiple selection using CTRL+Click), right-click your selection, and select Export Selected Reports.

If Sentral displays an error message, ensure the device(s) are accessible and are discovered.

4. Select a location to save the file, and enter a file name. Select a file format (.XML, .CSV, or .MIF) for the report.

5. Click Save, and then click OK to close the confirmation dialog box.

Sentral saves the report in the location you specified.

19.2: Inventory Report

The Inventory report details all of the components in host devices (physical hosts and VMs). The list below shows the items listed in an inventory report.

- Computer summary
- Memory
- Motherboard
- Processor
- BIOS
- Network
- Asset Management
- Drives
- Installed Applications
- Operating System
- Running Processes
- Video
- Horizontal Resolution
- Vertical Resolution
- Number of Colors
- Refresh Rate

The steps below show how to schedule and create an inventory report for a host device.

1. From the main menu, select Reports > Inventory.

2. Select the device rows to include in the reports.

3. Right-click your selection and select Schedule Time to display the Date Time Management screen.

4. Click the spin boxes to specify a date and starting time in the future to create a report.

   **NOTE:** To create a report, you must specify a date in the future. This release does not support generating reports from a future date; however, future releases will support this feature.

5. From the toolbar, click Save ( ). Sentral displays the Reports - Inventory screen again.

6. Ensure that at least one of the selected devices remains highlighted. Right-click the selection and select Schedule Report. Click OK to close the confirmation dialog box.

7. Ensure that at least one of the selected devices remains highlighted. Right-click the selection and select Export Report.

   If Sentral displays an error message, ensure the host is accessible, discovered, and contains a Host Agent.
8. Select a location to save the file, and enter a file name. Then select a file format (.XML, .CSV, or .MIF) for the report.

9. Click Save. Click OK to close the confirmation dialog box.

Sentral saves the report in the location you specified.

19.3: Report Scheduler
As noted above, when users create Inventory reports they must schedule (or specify a date and time) to create the report. Sentral uses a report scheduler to manage this schedule.

The Report Scheduler screen (available from the Alerts screen) shows Inventory Reports that Sentral created in the past and any reports that are schedule to run in the future.

1. From the main menu, click Reports > Alerts.

2. Right-click an empty area of the screen and select Scheduler Report to display the Reports - Scheduler Log screen.

3. Select a row containing a scheduled report. From the right-click menu, you can clear the selected report or clear all reports.

19.4: Alerts Report
Create and deploy alerts to computing resources to monitor them. Alerts fire, or trigger, when a device meets one or more specified conditions (see 20: “Sentral Alerts” below for more information about alerts). From the Reports – Alerts screen, you can generate reports about deployed alerts that have fired.

1. From the main menu, select Reports > Alerts to display the Reports – Alerts screen.

2. Select the devices to include in the report.

3. Right-click the selection and select Export Report.

   If Sentral displays an error message, ensure the device(s) are accessible and are discovered.

4. Select a location to save the file, and enter a file name. Then select a file format (.XML, .CSV, or .MIF) for the report.

5. Click Save. Click OK to close the confirmation dialog box.

Sentral saves the report in the location you specified.
19.5: Equipment History
You can generate a report that details all of the equipment history notes saved on host devices. See 14.13: “Recording Device-Related Information (Equipment History)” above for more information about equipment history.

1. From the main menu, select Reports > Equipment History to display the Reports - Equipment History screen.

2. Right-click an empty portion of the screen and select Export Report.
   
   If Sentral displays an error message, ensure that the device(s) are accessible and discovered.

3. Select a location to save the file, and enter a file name. Then select a file format (.XML, .CSV, or .MIF) for the report.

4. Click Save. Click OK to close the confirmation dialog box.

Sentral saves the report in the location you specified.

19.6: Device Accessibility
This report details the communication protocols (RDP or PCoIP) that devices in your Sentral environment use. The steps below show how to generate a Device Accessibility report.

1. From the main menu, select Reports > Device Accessibility to display the Reports – Device Accessibility screen.

2. You can create a report for one or more devices:
   
   • To include all devices: right-click an empty portion of the screen and select Export Report.
   
   • To include specific devices: select one or more devices (create a multiple selection using CTRL+Click or SHIFT+Click), right-click your selection, and select Export Selected Reports.

   If Sentral displays an error message, ensure that the device(s) are accessible and discovered.

3. Select a location to save the file, and enter a file name. Then select a file format (.XML, .CSV, or .MIF) for the report.

4. Click Save. Click OK to close the confirmation dialog box.

Sentral saves the report in the location you specified.

19.7: Profile Application Status
This report details the application of Client Profiles to devices in Sentral groups. (See 14.8: “Configuring Endpoints Using Client Profiles” above for information about Client Profiles.) The steps below show how to generate a Profile Application Status report.
1. From the main menu, select **Reports > Profile Status** to display the Reports – Profile Application Status screen.

2. You can create a report for one or more devices:
   - **To include all devices**: Right-click an empty portion of the screen and select **Export Report**.
   - **To include specific devices**: select one or more devices (create a multiple selection using CTRL+Click or SHIFT+Click), right-click your selection, and select **Export Selected Reports**.

   If Sentral displays an error message, ensure that the device(s) are accessible and discovered.

3. Select a location to save the file, and enter a file name. Then select a file format (.XML, .CSV, or .MIF) for the report.

4. Click **Save**. Click **OK** to close the confirmation dialog box.

   Sentral saves the report in the location you specified.
20: Sentral Alerts

Alerts allow a host (blades and VMs) to report an abnormal condition such as low disk space or an overheating system. You can deploy Alerts to hosts only, because the Host Agent provides the health and status reporting capabilities. You can create alerts to perform actions on hosts.

For example, you can create an alert to email an administrator if a host reaches a certain temperature. The list below shows attributes on a host that alerts can monitor, and actions that alerts can take (alerts can include any combination of the items listed below).

NOTE: Depending on your blade model and chassis configuration, not all functions listed below are available.

Table 25. The monitoring and alerting functions available for customized alerts

<table>
<thead>
<tr>
<th>Monitoring functions</th>
<th>Alerting functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free memory</td>
<td>Send email</td>
</tr>
<tr>
<td>Disk space</td>
<td>Shut down host</td>
</tr>
<tr>
<td>Installed applications</td>
<td>Restart host</td>
</tr>
<tr>
<td>Free virtual memory</td>
<td>Run a script</td>
</tr>
<tr>
<td>Voltage</td>
<td></td>
</tr>
<tr>
<td>Fan speed</td>
<td></td>
</tr>
<tr>
<td>Blade temperature</td>
<td></td>
</tr>
<tr>
<td>Blade fan speed</td>
<td></td>
</tr>
<tr>
<td>Blade voltage</td>
<td></td>
</tr>
</tbody>
</table>

After you create an alert, you must deploy the alert to each host or host group that contains hosts you want to monitor. Sentral does not monitor hosts until you explicitly deploy the alert to the host or host group. Be sure to see 9.14.2: “Additional Alert (Email) Configuration Options” above for information about configuring alert-related evaluation, triggering, and email settings from the Sentral Configuration screen.

The Health & Status > Alerts submenu enables you to:

- View alerts
- Configure alerts
- View deployed alerts

20.1: Viewing Alerts

To view alerts that trigger on a host device, perform the following steps:

1. From the main menu, click Health & Status > Alerts > View Alerts to display the Reports - Alerts screen.

   This screen shows any existing alerts on host devices. Alerts trigger when a device meets one or more specified thresholds and sends an alert to Sentral. If the screen is blank, no
alerts occurred on host devices. Note that this might be because an administrator has not deployed any alerts to host devices.

2. To see if any alerts have been created and deployed to hosts, right-click an empty space and select View Deployed Alerts.

3. Optionally, select and right-click an alert to manage the alert (for example, clear the alert).

20.2: Creating Alerts
This section includes important information about creating alerts and shows how to create different types of alerts.

Be sure to see 9.14.2: “Additional Alert (Email) Configuration Options” above for information about configuring alert-related evaluation, triggering, and email settings from the Sentral Configuration screen.

20.2.1: About Alerts That Monitor Multiple Conditions
You can create alerts that monitor more than one host condition. Note that all of the conditions must be met before Sentral performs the specified action. For example, suppose you create an alert that:

- Is triggered when host temperature is greater than or equal to 50 degrees Celsius
- Is triggered when host fan speed is less than or equal to 1,000 RPM
- Shuts down a host when it meets the specified thresholds.

Sentral does not shut down the host until it meets both conditions.

If you want to cause multiple actions to occur, you can select several items to evaluate before saving an alert. If you want to specify several Evaluate conditions, select a Monitor value and an Evaluate value for each of the conditions. For example, you cannot check for a condition of Memory $\geq$ 100 MB and $\leq$ 200 MB. In this example, you need to establish a separate entry for each condition: one condition being Memory $\geq$ 100 MB and another condition being Memory $\leq$ 200 MB. The conditions must all be true for the alert to trigger. To set an either/or condition, deploy distinct alerts, one for each condition. Then when any of the conditions is true, the corresponding alert triggers.

20.2.2: About Evaluation Parameters
With one exception, values for the Evaluate parameter are numeric and can include decimal places. For the Installed Applications parameter, the value is a string that must exactly match the spelling of the application as shown in Windows Add/Remove Programs (note that the spelling must be the same, but capitalization does not matter).
Be sure to see 9.14.2: “Additional Alert (Email) Configuration Options” above for information about configuring alert-related evaluation, triggering, and email settings from the Sentral Configuration screen.

20.2.3: Using the Shutdown and Restart Actions in Alerts
The Actions panel includes Shutdown and Restart items. If an alert deploys a shutdown or restart, you can abort the action using a DOS command prompt. When you receive a notification that a shutdown is in progress, you have 30 seconds by default (configurable to other values) to open a command prompt and enter the `shutdown -a` command to abort the shutdown.

20.2.4: Creating a New Alert
Before creating an alert, be sure to read the import information about alerts in the previous sections. This section shows how to create an alert.

1. From the main menu, click Health & Status > Alerts > Configure Alerts to display the Health and Status – Configure Alerts screen.

2. Select an item to monitor in the Monitor panel, shown below (if you are selecting Script, see the following section for instructions).

![Monitor panel](image)

Table 26. The Monitor panel

If Sentral displays the Monitor Input dialog box, make the selection that is appropriate for your alert.

If you need to change the Monitor item, click Cancel ( ![Cancel](image) ) from the toolbar to return to the Monitor panel.

3. Double-click an item in the Evaluate panel. From the Evaluate Input dialog box, specify a threshold value for the alert. Click OK to accept the value, or click Cancel to start over.
Table 27. Selecting an item in the Evaluate panel and entering a value

4. Optionally, add additional items to monitor by repeating step 2 and step 3.

5. Select an item in the Action panel:
   - If you select Email, Sentral displays the Enter email address dialog box. Enter the email address to receive the alert notification. Click OK.
   - You can select more than one action. Multiple actions execute in the order specified. Since the alert processes on the computer where the actions execute, the Shutdown and Restart actions prevent any further actions from occurring.

6. Type a name for the alert in the Name text box.

7. From the toolbar, click Save ( ). Sentral saves the alert and lists it in the upper portion of the screen.

   **NOTE:** You must deploy an Alert to activate it. Sentral does not activate the Alert until you deploy it to a host. See 20.3: “Deploying Alerts” below for more information.

Be sure to see 9.14.2: “Additional Alert (Email) Configuration Options” above for information about configuring alert-related evaluation, triggering, and email settings from the Sentral Configuration screen.

**20.2.5: Using Scripts in Custom Alerts and in Automated Actions**

Sentral enables you to write scripts to monitor your Sentral environment and to perform scripted actions when hosts meet conditions that you specify. Scripted alerts (like pre-configured Alerts), consist of the following elements:
- **Monitor**—any script (MS-DOS batch file) you write that monitors an OS-level event, state, condition, or other attribute. The output of the monitor script must be a string.

- **Evaluate string**—specify the evaluate string in the Sentral Health and Status - Alerts screen, as shown in the following steps. Sentral compares the monitor script’s output with the evaluate string. When the values are equivalent, or true, Sentral executes the action script that you specify.

- **Action**—any script (MS-DOS batch file) you write that performs an OS-level action, such as shutting down a host or any other logical action.

The following steps assume that you have a good understanding of how to write MS-DOS batch files. Perform the following steps to create monitor and action scripts:

1. Open a text editor, such as Notepad, in which to write your monitor script.
2. Write a script (batch file) that satisfies your monitoring criterion or criteria and save the file.

   **NOTE:** Ensure that you save the batch file using UTF-8 encoding.

   As shown in the following pseudocode example, you can use the `ECHO` command for your script output. In this example, if the variable `a` is equal to a particular value, the script uses the `ECHO` command to output that value as a string. Sentral compares the evaluation string that you specify in step 7 below with the output of the monitor batch file. If the comparison is true, Sentral executes the action script.

   **Example 2. Monitor.bat pseudocode**

   ```bash
   ECHO OFF
   IF %a% == 1 ECHO 1
   IF %a% == 2 ECHO 2
   IF %a% == 3 ECHO 3
   ```

3. Create the action script in a similar fashion and save the file.

   **NOTE:** Ensure that you save the batch file using UTF-8 encoding.

   The following pseudocode example shows an action script that starts notepad.exe and opens a welcome.txt file on the C:\ drive.

   **Example 3. Action.bat pseudocode**

   ```bash
   ECHO OFF
   Start NOTEPAD.EXE C:\WELCOME.TXT
   ```

4. From the main menu, click **Health & Status > Alerts > Configure Alerts** to display the Health and Status – Configure Alerts screen.
5. Double-click **Script** in the Monitor area to display the Open dialog box. Browse to the script (batch file) to use as the monitor action.

6. Select the appropriate script and click **Open**.

7. From the Evaluate area, double-click **String** to display the Evaluate Input text box. Specify a value in the text box. When the output of the monitor script is the same as the value you specify here, Sentral triggers, or executes, the action script.

8. From the Action area, double-click **Script** to display a dialog box. Browse to the action script to use and select the file.

9. In the **Name** text box, specify a name for the alert and then click Save ( ).

10. Deploy the alert to a single computer, to a group of computers, to a virtual machine, or to a group of virtual machines. See 20.3: “Deploying Alerts” below for information about deploying alerts.

    After deploying the alert to one or more hosts, Sentral executes the action script (batch file) when the alert is triggered on the target host. For more information about configuring alerts and alert notifications, see 9.5.1: “More about TLS in Sentral” and 9.14.2: “Additional Alert (Email) Configuration Options.”

    The examples in this section are basic. Following standard batch file scripting conventions, you can perform nearly any coordinated monitoring and action function appropriate for your environment. Contact ClearCube Support or a ClearCube Partner for more information about batch file scripting.

20.3: Deploying Alerts

This section assumes you have created an alert as shown in 20.2.4: “Creating a New Alert” above. The steps below show how to deploy an Alert.

1. From the main menu, click **Health & Status > Alerts > Configure Alerts** to display the Health and Status – Configure Alerts screen.

2. Select and right-click an alert. Select one of the following deployment choices:
   - Deploy to Physical Machine Group
   - Deploy to VM Group
   - Deploy to Physical Machine
   - Deploy to VM

    Sentral displays the appropriate Health & Status – Deploy screen. The screen lists all available devices or groups.
3. Select a group or devices to receive the alert. With your keyboard and mouse, CTRL+Click or SHIFT+Click to select multiple devices, or press CTRL+A to select all devices.

4. Right-click your selection and select **Deploy Alert** (the menu option might be slightly different depending on your selection).

5. Click **OK** to close the confirmation dialog box.

Be sure to see 9.14.2: “Additional Alert (Email) Configuration Options” above for information about configuring alert-related evaluation, triggering, and email settings from the Sentral Configuration screen.

### 20.4: Viewing Deployed Alerts

This section shows how to view deployed alerts.

1. From the main menu, click **Health & Status > Alerts > View Deployed Alerts** to display the Health & Status – View Deployed Alerts screen.

2. This view shows all alerts that have deployed to hosts. The table below shows each field in the View Deployed Alert screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name entered in the Name field of the Configure Alerts screen.</td>
</tr>
<tr>
<td>Description</td>
<td>This is the formulaic description of the alert’s Evaluate and Action items. The Configure Alerts screen’s Description field shows this value.</td>
</tr>
<tr>
<td>Device ID</td>
<td>The computer name of the device to which the alert is deployed.</td>
</tr>
<tr>
<td>Device Type</td>
<td>This is the type of host to which the alert is deployed (physical host or VM).</td>
</tr>
<tr>
<td>Deployment Time</td>
<td>The time Sentral deployed the alert to the host device.</td>
</tr>
<tr>
<td>Action</td>
<td>This lists the action or actions that the alert performs when triggered.</td>
</tr>
<tr>
<td>Deployment Status</td>
<td>This shows if Sentral deployed the alert to the host device successfully.</td>
</tr>
<tr>
<td>Mute</td>
<td>This shows if the alert is muted. If an alert is muted, it is not monitoring the host device. To toggle the mute setting, select <strong>Mute Selected Alerts</strong> or <strong>Un-Mute Selected Alerts</strong> to change the mute status.</td>
</tr>
</tbody>
</table>
20.5: Modifying Alerts

The following sections show how to modify alerts that monitor one or more host conditions.

20.5.1: Modifying Alerts that Monitor a Single Condition

This section shows how to modify an alert that monitors a single condition on a host device (physical host or VM).

**NOTE:** Modifying an alert does not cause a host to activate it. Changes do not take effect until you deploy the alert to a host.

1. From the main menu, click **Health & Status > Alerts > Configure Alerts** to display the Health and Status – Configure Alerts screen.

2. From the upper portion of the screen, select and right-click an alert to modify (you can modify one alert at a time). Select **Modify Alert**. Sentral displays the existing alert configuration in the lower portion of the screen.

3. Select a new **Monitor** item, a new **Evaluate** item, or both. If you are modifying a Monitor item that is already in the alert, you must select it before selecting the Evaluate item. If you select a new item in the Evaluate area, specify a new value in the dialog box and then click **OK**.

4. Optionally, to specify an additional action for the alert to perform, click **Next Item (➡️)** in the toolbar and then select an action.

5. Sentral displays the Action Input dialog box. If you are specifying a new email address, type the address and click **OK**. If you are selecting the Shutdown or Restart action, leave the dialog box empty and click **OK**.

6. From the toolbar, click **Save (📝)** and then click **OK** to close the confirmation dialog box. You can see the description of the updated alert in the Description column located in the upper part of the screen.

7. Deploy the alert as shown in 20.3: “Deploying Alerts” above.

20.5.2: Modifying Alerts that Monitor Multiple Conditions

This section shows how to modify an alert that monitors more than one condition on a host device (physical host or VM).

1. From the main menu, click **Health & Status > Alerts > Configure Alerts** to display the Health and Status – Configure Alerts screen.

2. From the upper portion of the screen, select and right-click an alert to modify. Select **Modify Alert**. Sentral displays the existing alert configuration in the lower portion of the screen.
3. From the toolbar, click **Next Item** (➡️) and **Previous Item** (⬅️) to move between each item, where an item is a grouping of the host condition to monitor and the value that triggers the alert.

4. Change values of existing Monitor items, Evaluate items, or both.

5. Optionally, change one or more alert actions by clicking **Next Item** (➡️) until the item in the Action panel is highlighted.

6. Select the new action and click **Save** (💾).

7. Deploy the alert as shown in 20.3: “Deploying Alerts” above.

**20.6: Removing Alerts from Sentral Console**

To remove an alert from the console, perform the following steps:

1. From the main menu, click **Health & Status > Alerts > Configure Alerts** to display the Health & Status – Configure Alerts screen.

2. Select one or multiple alerts. Right-click your selection and select **Delete Alert**.

3. Click **OK** to close the confirmation screen.
21: Client Profile Field Descriptions
The sections below detail all Client Profile fields.

21.1: PCoIP Profile Fields
The table below details all PCoIP Profile fields. For more information about profiles, see 14.8: “Configuring Endpoints Using Client Profiles” above.

Table 28. PCoIP Profile Settings

<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile Information section</strong></td>
<td></td>
</tr>
<tr>
<td>Profile Name</td>
<td>Type a name for the profile.</td>
</tr>
<tr>
<td>Profile Description</td>
<td>Type a description of the profile.</td>
</tr>
<tr>
<td><strong>Session Configuration section</strong></td>
<td></td>
</tr>
<tr>
<td>Session Connection Type</td>
<td>This setting controls how the PCoIP device initiates and receives PCoIP sessions.</td>
</tr>
<tr>
<td>Enable Auto Reconnect</td>
<td>When this property is true, the zero client automatically reconnects with the last connected host when a session is disconnected.</td>
</tr>
<tr>
<td>View Connection Server Address</td>
<td>In a VMware View® environment, this property sets the IP address or FQDN of the View Connection Server.</td>
</tr>
<tr>
<td>View Connection Server Port</td>
<td>When using SSL to communicate with the View Connection Server, the default port is 443. If using firmware 3.x.x and SSL communication is not enabled, the default port is 80.</td>
</tr>
<tr>
<td>Enable View Connection Server SSL</td>
<td>Enables SSL communications with the View Connection Server. This property has no effect on devices using firmware 4.0.0 or greater. This firmware requires SSL communication between clients and the View Connection Server.</td>
</tr>
<tr>
<td>CMS Address</td>
<td>IP Address – In a brokered deployment, this is the connection broker’s IP address or FQDN.</td>
</tr>
<tr>
<td>Auto-Logon Username</td>
<td>Specifies the Auto-Logon username. When Auto-Logon is enabled this is the username sent to the VDM server.</td>
</tr>
<tr>
<td>Auto-Logon Password</td>
<td>Specifies the Auto-Logon username. When Auto-Logon is enabled this is the password sent to the VDM server.</td>
</tr>
<tr>
<td>Auto-Logon Domain</td>
<td>Specifies the Auto-Logon domain name. When Auto-Logon is enabled this is the domain name sent to the VDM server.</td>
</tr>
<tr>
<td>Section/Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use Kiosk Custom Username</td>
<td>Enables kiosk mode support. If kiosk mode is disabled, all other kiosk mode parameters are not used. Kiosk mode is disabled by default.</td>
</tr>
<tr>
<td>Kiosk mode Custom Username</td>
<td>Specifies the “XXX” portion of the custom username of form “Custom-XXX”. This value is only applicable when a custom usernames is desired (enableVdmKioskModeCustomUsernameForm is non-zero).</td>
</tr>
<tr>
<td>Kiosk Mode Password</td>
<td>The password used during login to access a remote desktop.</td>
</tr>
<tr>
<td>Onesign Bootstrap URL</td>
<td>This setting sets the URL for the Imprivata OneSign bootstrap server.</td>
</tr>
<tr>
<td><strong>Network Configuration section</strong></td>
<td></td>
</tr>
<tr>
<td>Enable DHCP</td>
<td>When this property is true, the host or zero client contacts a DHCP server to receive an IP address, subnet mask, gateway IP address, and DNS server. Set these parameters manually when this property is false.</td>
</tr>
<tr>
<td>Static Fallback IP Address</td>
<td>The IP address to use when Static IP Fallback is enabled and DHCP lease acquisition fails.</td>
</tr>
<tr>
<td>Static Fallback Subnet Mask</td>
<td>The subnet mask to use when Static IP Fallback is enabled and DHCP lease acquisition fails.</td>
</tr>
<tr>
<td>Static Fallback Gateway</td>
<td>The gateway address to use when Static IP Fallback is enabled and DHCP lease acquisition fails.</td>
</tr>
<tr>
<td><strong>USB Authorizations Configuration section</strong></td>
<td></td>
</tr>
<tr>
<td>USB authorization applies only to PCoIP sessions. Though the web or CMI interface, the user configures the USB authorization and USB unauthorization tables. The authorization table contains a list of authorized USB devices that are functional during a PCoIP session. The unauthorization table contains a list of unauthorized USB devices that are not functional during a PCoIP session. The two tables define which USB devices are functional. For example, use the USB authorization table to authorize a certain class of USB devices and use the USB unauthorization table to deny specific USB devices within that class.</td>
<td></td>
</tr>
<tr>
<td>Rule Number</td>
<td>This number identifies the USB rule you are creating or removing. Devices generate rule numbers automatically, starting at 1, and increasing sequentially. For example, the second rule is automatically numbered 2.</td>
</tr>
<tr>
<td>Rule Type</td>
<td>This option specifies if the USB authorization is by USB device ID or by USB device class. The selection made here disables options that are not applicable to the rule type.</td>
</tr>
</tbody>
</table>
### Section/Field | Description
--- | ---
Device Class | **For Class-based rules only:** This option specifies the type of USB device authorized.
Sub Class | **For Class-based rules only:** This option specifies the sub-class of USB device. Some device classes do not contain any sub-classes. In this case, the only option you can select here is **Any**.
Protocol | **For Class-based rules only:** This option specifies the protocol that the authorized device uses. This option is not applicable to some device sub-classes. In this case, the only option you can select here is **Any**.
PID | **For ID-based rules only:** Type the authorized USB device’s Product ID (PID) here.
VID | **For ID-based rules only:** Type the authorized USB device’s Vendor ID (VID) here.
Action | The **Action** button dynamically changes depending on your current task. If you are creating a new rule, click **Save** to save the rule. If you select an existing rule, click **Remove** to remove the rule.

#### Discovery Configuration section

Enable SLP Discovery | SLP discovery enables a client to find host cards to which it can connect. Select **True** to enable SLP discovery or **False** to disable it.

#### SNMP Configuration section

Enable SNMP | The device’s SNMP support is enabled when this value is **True**. When **False**, the device does not respond to SNMP queries or generate traps.
SNMP NMS Address | Host cards and zero clients can send SNMP traps to an SNMP Network Management System (NMS). This property configures the IP address or FQDN of the SNMP NMS.
Enable SNMP Cold Start Trap | When this property is **True**, a host card or zero client sends SNMP cold start traps to the SNMP NMS after the device is powered on or reset.
Enable SNMP v1 | When **True**, this setting enables the generation of SNMPv1 traps.
Enable SNMP v2 | When **True**, this setting enables the generation of SNMPv2 traps.
SNMP Community Name | This property sets the SNMP community name the zero client or host card uses.

#### Power Configurations section

Client Power Button Function | This property configures the zero client power button. When **soft power off** is enabled: press zero client power button for less than 4
<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds and remote PC enters soft power off state. When <strong>hard power off</strong> is enabled: press power button for longer than 4 seconds and remote PC enters hard power off state.</td>
<td></td>
</tr>
<tr>
<td>Wake-on-USB Mode</td>
<td>This property configures the Wake-on-USB mode.</td>
</tr>
<tr>
<td>Wake-on-LAN Mode</td>
<td>This property configures the Wake-on-LAN mode.</td>
</tr>
<tr>
<td>Power On After Power Loss Mode</td>
<td>When this property is enabled, the zero client automatically powers on when power is supplied.</td>
</tr>
<tr>
<td>Client Power Down Timeout Seconds</td>
<td>This specifies the time of inactivity (no mouse or keyboard activity) that causes a zero client to power down. The timeout only applies to a device when a PCoIP session is not established. Valid values are 60 to 28800, or use 0 to disable power down.</td>
</tr>
<tr>
<td>Display Topology Configuration section</td>
<td></td>
</tr>
<tr>
<td>Dual Display Zero Client</td>
<td><strong>Horizontal</strong> places displays side-by-side. <strong>Vertical</strong> places one display above the other.</td>
</tr>
<tr>
<td>Quad Display Zero Client</td>
<td><strong>Horizontal</strong> places all displays side by side (display 1 leftmost and display 4 rightmost). <strong>Vertical</strong> places all displays in a column (display 1 topmost and display 4 bottommost). <strong>Boxed</strong> creates a quadrant: displays 1 and 2 on the top row and displays 3 and 4 on the bottom row.</td>
</tr>
<tr>
<td>USB Unauthorized Configuration section</td>
<td></td>
</tr>
<tr>
<td>USB authorization applies only to PCoIP sessions. Though the web or CMI interface, the user configures the USB authorization and USB unauthorization tables. The authorization table contains a list of authorized USB devices that are functional during a PCoIP session. The unauthorization table contains a list of unauthorized USB devices that are not functional during a PCoIP session. The two tables together define which USB devices are functional; for example, use the USB authorization table to authorize a certain class of USB devices and use the USB unauthorization table to deny specific USB devices within that class.</td>
<td></td>
</tr>
<tr>
<td>Rule Number</td>
<td>This number identifies the USB rule you are creating or removing. Rule numbers are assigned automatically, begin at 1, and increase sequentially. For example, the second rule is automatically numbered 2.</td>
</tr>
<tr>
<td>Rule Type</td>
<td>This option specifies if the USB prohibition is by USB device ID or by USB device class. The selection made here disables options that are not applicable to the rule type.</td>
</tr>
<tr>
<td>Device Class</td>
<td><strong>For Class-based rules only:</strong> This option specifies the type of USB device that is unauthorized.</td>
</tr>
<tr>
<td>Section/Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sub Class</td>
<td><strong>For Class-based rules only:</strong> This option specifies the sub-class of USB device. Some device classes do not contain any sub-classes. In this case, the only option you can select here is <strong>Any</strong>.</td>
</tr>
<tr>
<td>Protocol</td>
<td><strong>For Class-based rules only:</strong> This option specifies the protocol that the unauthorized device uses. This option is not applicable to some device sub-classes. In this case, the only option you can select here is <strong>Any</strong>.</td>
</tr>
<tr>
<td>PID</td>
<td><strong>For ID-based rules only:</strong> Type the unauthorized USB device’s Product ID (PID) here.</td>
</tr>
<tr>
<td>VID</td>
<td><strong>For ID-based rules only:</strong> Type the unauthorized USB device’s Vendor ID (VID) here.</td>
</tr>
<tr>
<td>Action</td>
<td>The <strong>Action</strong> button dynamically changes depending on your current task. If you are creating a new rule, click <strong>Save</strong> to save the rule. If you select an existing rule, click <strong>Remove</strong> to remove the rule.</td>
</tr>
<tr>
<td>Security Configuration</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Password that the endpoint uses to compare against the local administrative password.</td>
</tr>
</tbody>
</table>

**21.2: Thin Client Agent Profile Fields**

The table below details all Thin Client Agent Profile fields. For more information about profiles, see 14.8: “Configuring Endpoints Using Client Profiles” above.

*Table 29. Thin Client Agent Profile Settings*

<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Information section</td>
<td></td>
</tr>
<tr>
<td>Profile Name</td>
<td>The name for the profile. Any characters allowed; however, Sentral removes whitespace characters from the beginning of names.</td>
</tr>
<tr>
<td>Profile Description</td>
<td>Enter a description for the Thin Client Agent profile. Any characters allowed; however, Sentral removes whitespace characters from the beginning of descriptions.</td>
</tr>
<tr>
<td>Thin Client Agent Configurations section</td>
<td></td>
</tr>
<tr>
<td>Primary Server</td>
<td>The Primary Sentral Server IP address or hostname.</td>
</tr>
<tr>
<td>Secondary Server</td>
<td>The Secondary Sentral Server IP address or hostname. If there is only a Primary Server, enter the Primary Server’s IP address.</td>
</tr>
</tbody>
</table>
## Section/Field

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>or hostname here.</td>
</tr>
<tr>
<td>The Sentral Server communication port. Default port for Sentral Server is 8080.</td>
</tr>
<tr>
<td>The time (in minutes) after which a thin client sends a heartbeat to the Sentral Server. The default value is two minutes. This value should be at least half the “Thin Client Update Timeout” value shown in the Sentral “Configuration” screen.</td>
</tr>
<tr>
<td>If set to TRUE, the thin client will automatically connect to the allocated device after being disconnected.</td>
</tr>
<tr>
<td>Specifies the number of times to try to reconnect during automatic reconnection.</td>
</tr>
<tr>
<td>The maximum time (in seconds) for each connection attempt. If a connection is not made in this time, another attempt is made (when Auto Connect is TRUE and Max Retries is greater than 0).</td>
</tr>
<tr>
<td>If TRUE, at startup the Thin Client Agent uses the username and password from the configuration to automatically sign in to the remote computer. (To enforce connecting after a disconnection, use the <strong>Auto Connect</strong> setting.)</td>
</tr>
<tr>
<td>If TRUE, during reconnection attempts the Thin Client Agent attempts to connect to the last remote computer to which it connected.</td>
</tr>
<tr>
<td>If a remote device requires login credentials and Auto Login or Auto Connect is enabled, enter the username here.</td>
</tr>
<tr>
<td>If a remote device requires login credentials and Auto Login or Auto Connect is enabled, enter the password here.</td>
</tr>
<tr>
<td>If a remote device requires login credentials and Auto Login or Auto Connect is enabled, enter the Domain name here.</td>
</tr>
<tr>
<td>If TRUE, the Thin Client Agent allows users to enter the hostname of a remote computer.</td>
</tr>
<tr>
<td>If FALSE, the Thin Client Agent does not permit users to close the thin client interface.</td>
</tr>
<tr>
<td>If TRUE, Thin Client Agent stores the remote computer’s IP address or hostname for every session rather than retrieving</td>
</tr>
<tr>
<td>Section/Field</td>
</tr>
<tr>
<td>---------------------------------------</td>
</tr>
<tr>
<td>it from Sentral.</td>
</tr>
<tr>
<td>Username Field</td>
</tr>
<tr>
<td>Password Field</td>
</tr>
<tr>
<td>Domain Field</td>
</tr>
<tr>
<td>Edit Domain</td>
</tr>
<tr>
<td>GUI Startup Time</td>
</tr>
<tr>
<td>Multi Instance</td>
</tr>
<tr>
<td>USB Redirection</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
<tr>
<td>Remote Desktop Protocol Configurations section</td>
</tr>
<tr>
<td>Default Resolution</td>
</tr>
<tr>
<td>Bitmap Cache Persistence</td>
</tr>
<tr>
<td>Redirect Printers</td>
</tr>
</tbody>
</table>
### Redirec COM Ports

<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect COM Ports</td>
<td>Makes COM ports configured on the thin client available in the remote session. 0 – The local COM ports on the thin client are not available on the remote host computer. 1 – The local COM ports on the thin client are available on the remote computer.</td>
</tr>
</tbody>
</table>

### Display Connection Bar

<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Connection Bar</td>
<td>This setting determines if the RDP connection bar displays when in full screen mode. 0 – Do not show connection bar. 1 – Show connection bar.</td>
</tr>
</tbody>
</table>

### Audio Mode

<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Mode</td>
<td>Determines how audio output is handled when the thin client is connected to a remote computer. 0 – Play sounds on the thin client. 1 – Play sounds on the remote computer. 2 – Do not play sounds.</td>
</tr>
</tbody>
</table>

### Audio Capture Mode

<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Capture Mode</td>
<td>Determines how audio input is handled when the thin client is connected to a remote computer. 0 – Do not capture audio from the thin client. 1 – Capture audio input on the remote computer.</td>
</tr>
</tbody>
</table>

### Span Monitors

<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Span Monitors</td>
<td>Determines whether the remote session window spans multiple monitors when connected to a remote computer. 0 – Monitor spanning is not in effect. 1 – Monitor spanning is in effect. <strong>NOTE:</strong> When using Remote Desktop Connection 7, we recommend using the <strong>Use Multimon</strong> option.</td>
</tr>
</tbody>
</table>

### Gateway Usage Method

<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Usage Method</td>
<td>Specifies if and how to use a Remote Desktop Gateway (RD Gateway) server. 0 – Do not use an RD Gateway server. 1 – Always use an RD Gateway, even for local connections. 2 – Use the RD Gateway if a direct connection cannot be made to the remote computer (bypass for local addresses). 3 – Use the default RD Gateway settings. 4 – Do not use an RD Gateway server. <strong>NOTE:</strong> Options 0 and 4 have the same effect, but setting the method to 4 also sets the option for bypassing local addresses in the Remote Desktop user interface.</td>
</tr>
<tr>
<td>Section/Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Gateway Profile Usage</td>
<td>Specifies the RD Gateway authentication method.</td>
</tr>
<tr>
<td>Method</td>
<td>0 – Use the default profile mode as specified by the administrator. 1 – Use explicit settings.</td>
</tr>
<tr>
<td>Video Playback Mode</td>
<td>Enables RDC to use RDP efficient multimedia streaming for video playback. 0 – Do not use RDP efficient multimedia streaming. 1 – Use RDP efficient multimedia streaming.</td>
</tr>
<tr>
<td>Disable Wallpaper</td>
<td>Determines whether the desktop background is displayed in the remote session. 0 – Display wallpaper. 1 – Do not display wallpaper.</td>
</tr>
<tr>
<td>Allow Desktop Composition</td>
<td>Determines whether desktop composition (needed for Aero) is permitted when you log on to the remote computer. 0 – Disable desktop composition in the remote session. 1 – Desktop composition is permitted.</td>
</tr>
<tr>
<td>Disable Menu Anims</td>
<td>Determines if menu and window animation effects occur in the remote session. 0 – Menu and window animation is permitted. 1 – Menu and window animation is not permitted.</td>
</tr>
<tr>
<td>Disable Cursor Setting</td>
<td>Indicates whether cursor blinking is enabled during a Terminal Services session. 1 – Cursor blinking is disabled. 0 – Cursor blinking is enabled.</td>
</tr>
<tr>
<td>Redirect POS Devices</td>
<td>Determines whether Microsoft Point of Service (POS) for .NET devices connected to the thin client are redirected and available in the remote session. 0 – Thin client POS devices are not available in the remote session. 1 – Thin client POS devices are available in the remote session.</td>
</tr>
<tr>
<td>Autoreconnection Enabled</td>
<td>Determines if the thin client automatically reconnects to the remote computer if the connection is dropped (for example, if network connectivity is interrupted). 0 – Do not attempt to reconnect. 1 – Attempt to reconnect.</td>
</tr>
<tr>
<td>Authentication Level</td>
<td>Specifies action to take when server authentication fails. 0 – If server authentication fails, connect without warning. 1 – If server authentication fails, do not connect.</td>
</tr>
</tbody>
</table>
### Section/Field Descriptions

<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 – If server authentication fails, show a warning and allow the user to connect or not. 3 – Server authentication is not required.</td>
<td></td>
</tr>
<tr>
<td>Negotiate Security Layer</td>
<td>Determines if the security level is negotiated or not. 0 – Security layer negotiation is not enabled and the session is started using Secure Sockets Layer (SSL). 1 – Security layer negotiation is enabled and the session is started using x.224 encryption.</td>
</tr>
<tr>
<td>Prompt Credentials Once</td>
<td>Determines whether Remote Desktop Connection prompts for credentials when connecting to a remote computer for which credentials were previously saved. 0 – Use the saved credentials and do not prompt for credentials. 1 – Prompt for credentials.</td>
</tr>
<tr>
<td>Network Auto-Detect</td>
<td>Automatically detects network characteristics and optimizes user experience accordingly. 0 – RDP does not detect any network settings. 1 – RDP automatically detects the best network settings.</td>
</tr>
<tr>
<td>Enable Workspace Reconnect</td>
<td>Enables automatic reconnection if the connection drops.</td>
</tr>
<tr>
<td>Audio Quality Mode</td>
<td>Determines the quality of audio played in the remote session. 0 – Dynamically adjust audio quality based on available bandwidth. 1 – Always use medium audio quality. 2 – Always use uncompressed audio quality.</td>
</tr>
<tr>
<td>Enable CredSSP Support</td>
<td>Determines whether Remote Desktop uses CredSSP for authentication (if available). 0 – Do not use CredSSP, even if operating system supports it. 1 – Use CredSSP if operating system supports it.</td>
</tr>
<tr>
<td>Disable Connection Sharing</td>
<td>Determines if a new Terminal Server session starts each time a remote application connects to the same computer and with the same credentials. 0 – A new session does not start. The user’s currently-active session is shared. 1 – A new login session starts for the remote application.</td>
</tr>
<tr>
<td>Section/Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Smart Sizing        | When resizing the thin client window, specifies if the thin client should scale the content on the remote computer to fit the thin client window.  
0 – Thin client window display does not scale when resized.  
1 – Thin client window display scales when resized. |
| Color Depth         | Specifies the color depth of the remote session. Select 15-bit, 16-bit, 24-bit, or 32-bit.                                                                                                                     |
| Devices to Redirect | Determines which supported plug and play devices on the thin client are redirected and available in the remote session.  
No Devices – Do not redirect any supported plug and play devices.  
* – Redirect all supported plug and play devices, including ones that are connected later.  
DynamicDevices – Redirect any supported plug and play devices that are connected later. |
| Drives to Redirect  | Determines which local thin client disk drives are redirected and available in the remote session.  
No Drives – Do not redirect any drives  
* – Redirect all disk drives, including drives connected later.  
DynamicDrives – Redirect any drives that are connected later. |
| Redirect Smart Cards| Specifies if smart cards are redirected and available in a remote session.  
0 – Smart card on thin client is not available in remote session.  
1 – Smart card on thin client is available in the remote session. |
| Keyboard Hook       | Determines how Windows key combinations are applied when connected to a remote computer.  
0 – Windows key combinations are applied on the thin client.  
1 – Windows key combinations are applied on remote computer.  
2 – Windows key combinations applied on remote computer only when RDP is in full-screen mode. |
| Compression         | Determines whether the connection should use bulk compression.  
0 – Do not use bulk compression.  
1 – Use bulk compression. |
| Use Multimon        | Determines whether the session should use true multiple monitor support when connecting to the remote computer.  
0 – Do not enable multiple monitor support.  
1 – Enable multiple monitor support. |
<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTE:</strong></td>
<td>This option requires Windows 7 Enterprise or Ultimate on the remote computer for full support.</td>
</tr>
</tbody>
</table>
| Enable Superspan           | Enables or disables Superspan. Superspan allows users to navigate remote desktops in full-screen mode without scroll bars when the dimensions of the remote desktop are larger than the dimensions of the current client window. The user can point to the window border, and the desktop view will scroll automatically in that direction.  
0 – Do not use Superspan. The remote session window is sized to the thin client window size.  
1 – Enable Superspan. The remote session window is sized to the dimensions specified in the Default Resolution drop-down menu options in the RDP Configurations section. |
| Gateway Credentials Source | Specifies the credentials used to validate the connection with the Remote Desktop Gateway server.  
0 – Ask for password (Windows Challenge/Response, NTLM).  
1 – Use smart card.  
4 – Allow user to select later.                                                                                                                                                                                                                                           |
| Connection Type            | Specifies predefined performance settings for the Remote Desktop session.  
1 – Modem (56kbps)  
2 – Low-speed broadband (256 kbps – 2 Mbps)  
3 – Satellite (2 Mbps – 16 Mbps with high latency)  
4 – High-speed broadband (2 Mbps – 10 Mbps)  
5 – WAN (10 Mbps or higher with high latency)  
6 – LAN (10 Mbps or higher)  
7 – Auto detect  
When selected, this option changes multiple performance-related settings (themes, animation, font smoothing, etc.).  
This setting is superseded by any changes to the individual settings. See the RPC GUI’s Experience tab for list of individual settings that are affected. |
| Allow Font Smoothing       | This setting determines whether font smoothing is used in the remote session.  
0 – Disable font smoothing in the remote session.  
1 – Permit font smoothing.                                                                                                                                                                                                                                                 |
<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Disable Full Window Drag   | Determines whether window content is displayed when you drag the window to a new location.  
0 – Show the contents of the window while dragging.  
1 – Show an outline of the window while dragging. |
| Disable Themes             | Determines whether themes are permitted when you log on to the remote computer.  
0 – Themes are permitted.  
1 – Disable theme in the remote session. |
| Redirect Clipboard        | Determines whether the thin client clipboard is redirected and available in the remote session, and the same for the remote computer’s clipboard.  
0 – Do not redirect the clipboard.  
1 – Redirect the clipboard. |
| Redirect DirectX           | Determines whether DirectX is enabled for the remote session.  
0 – Do not enable DirectX rendering.  
1 – Enable DirectX rendering in the remote session. |
| Autoreconnect Max Retries  | Specifies the maximum number of times a thin client attempts to reconnect to a remote computer if the connection is dropped (for example, an interruption of network connectivity). The default value is 20. |
| Prompt for Credentials     | Determines if Remote Desktop Connection requests credentials when connecting to a remote computer for which the credentials were previously saved.  
0 – Use the saved credentials and do not prompt.  
1 – Prompt for credentials. |
| Remote Application Mode    | Determines if a remote application program launches when connecting to a remote computer.  
0 – Use a normal session and do not start a remote application.  
1 – Connect and launch a remote application. |
| Use Redirection Server Name| Specifies if a redirection server is allowed.  
0 – A redirection server is not allowed.  
1 – A redirection server is allowed. |
| Bandwidth Auto Detect      | 0 – RDP does not detect any bandwidth settings.  
1 – RDP automatically detects the best bandwidth settings. |
<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Administrative Session       | Connect to the administrative session of the remote computer.  
0 – Do not use the administrative session.  
1 – Connect to the administrative session. |
| Disable CTRL+ALT+DEL          | Determines if you must press CTRL+ALT+DEL before entering credentials after you are connected to the remote computer.  
0 – CTRL+ALT+DEL is required before logging in.  
1 – CTRL+ALT+DEL is not required. You can log in immediately.  
**NOTE:** When disabled, this setting delays Auto-Login until the user presses CTRL+ALT+DEL. |
| Pin Connection Bar            | Determines if the connection bar is pinned to the top of the remote session upon connection.  
0 – Connection bar is not pinned to top of the remote session.  
1 – Connection bar is pinned to top of the remote session. |
| Disable Remote App Caps Check | Specifies whether the remote desktop client should check the remote computer for remote application program capabilities.  
0 – Check the remote computer for remote application program capabilities before logging in.  
1 – Do not check the remote computer for remote application program capabilities.  
**NOTE:** This setting must be set to 1 when connecting to Windows XP SP3, Windows Vista, or Windows 7 computers that have a remote application program. |
| Public Mode                   | Prevents caching of passwords and bitmaps. |
22: Troubleshooting
The sections below provide troubleshooting steps and suggestions.

22.1: Console Response Issues
If Sentral Console does not respond to mouse clicks, you might need to restart Sentral Console. From the Windows operating system Task Manager’s Processes tab, find the javaw.exe process and click End Process.

NOTE: ClearCube recommends exiting the console when you have finished using the console rather than leaving it running.

22.2: Server Performance Is Slow or Server Is Not Responding
Restart Sentral Server (depending on your environment, either ClearCube Tomcat service or IIS Admin Service). From the Windows Start menu Search bar, type services.msc and press Enter). From the Services panel, select the service and click Restart.

Depending on your environment, you might find it necessary to restart the server service on occasion. In addition to restarting the service from Services panel (services.msc), you can automate restarts using Windows Task Scheduler (for example, restart the service on a daily basis).

22.3: Sentral Errors and Messages
If you encounter Sentral errors, turn on logging (as described in 11: “Server Log and Settings” above) and send ClearCube server logs.

## 23: Important Account Information

Use the table below to record important Sentral-related account information.

<table>
<thead>
<tr>
<th>Sentral Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
</tr>
<tr>
<td>Domain</td>
</tr>
</tbody>
</table>

*User Account on Computer Running Sentral Server*

<table>
<thead>
<tr>
<th>User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Domain</td>
</tr>
</tbody>
</table>

**Sentral Account Details**

*Built-in CCT Account*

<table>
<thead>
<tr>
<th>User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Domain (CCT by Default)</td>
</tr>
</tbody>
</table>

*User Account on Computer Running Sentral Console (Local System Account)*

<table>
<thead>
<tr>
<th>User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Domain</td>
</tr>
</tbody>
</table>

**Sentral Database**

<table>
<thead>
<tr>
<th>Database Type (MySQL, MS SQL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Version</td>
</tr>
<tr>
<td>User Name</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>

**Sentral Server ClearCube Tomcat Service Account**

*Not applicable if your deployment uses Internet Information Services (IIS)*

<table>
<thead>
<tr>
<th>User Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td></td>
</tr>
</tbody>
</table>

**Microsoft Internet Information Services (IIS) Account**

*Not applicable if your deployment uses Apache Tomcat*

<table>
<thead>
<tr>
<th>User Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td></td>
</tr>
</tbody>
</table>

**Sentral Email Account**

<table>
<thead>
<tr>
<th>Sender</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver</td>
<td></td>
</tr>
<tr>
<td>SMTP Server</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>SSL</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
</tbody>
</table>

**Sentral FTP Server**

*FTP Server is typically installed on the same computer as Sentral Server.*

<table>
<thead>
<tr>
<th>FTP Host</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP User Name</td>
<td></td>
</tr>
<tr>
<td>FTP Password</td>
<td></td>
</tr>
</tbody>
</table>
This Page is Intentionally Blank