OnGuard® 7.3

Advanced Installation Topics

LENEL
United Technologies

Lenel® OnGuard® 7.3 Advanced Installation Topics
This guide is item number DOC-100, revision 7.025, August 2016

Table of Contents

CHAPTER 1

Introduction

The Advanced Installation Topics Guide focuses on those aspects of the OnGuard installation that are not part of normal procedures. Topics covered include:

- Installing Oracle and SQL Server databases
- How to perform a remote installation
- How to use SNMP with OnGuard
- Ports used by OnGuard
- OnGuard Services

The Installation Guides

Advanced Topic Installation User Guide. DOC-100. A guide that encompasses a variety of advanced topics including Oracle installation and configuration.

Installation Guide. DOC-110. A comprehensive guide that includes instructions for installing the OnGuard software. This guide also includes information on the current SQL Server version and the browser-based client applications

Upgrade Guide. DOC-120. A short and sequential guide on upgrading and configuring an access control system that utilizes SQL or SQL Server Express system.

Enterprise Setup & Configuration User Guide. DOC-500. A guide that includes instructions for installing database software, the access control system Enterprise software, and how to setup complex Enterprise systems.

Minimum Privileges Required by Windows Users

A standard Windows user can perform all OnGuard operations, with the exception of the following tasks that require additional privileges.

Minimum Privileges Required by Windows Users

Component or Program	Task	Required Privileges	Notes
System Administration	Text-based archiving	Standard user requires Write permission on the Archive folder.	
Setup Assistant	Run Setup Assistant	Standard user requires administrator privileges.	
Configuration Editor	View the configuration of the database and License Server	Standard user requires administrator privileges.	
Database Setup	Use Database Setup	Standard user must have a login to SQL Server, and must run Database Setup with administrator privileges. This restriction does not apply if the application.config file is configured to use the Lenel database user.	Map the AccessControl database to the user with the roles: • db_datareader • db_datawriter • db_ddladmin
Form Translator	Allows the use of OnGuard web applications	Standard user requires administrator privileges.	
Universal Time Conversion utility	Convert data to UTC time	Standard user must have a login to SQL Server, and must log into Windows as an administrator. This restriction does not apply if the application.config file is configured to use the Lenel database user.	Map the AccessControl database to the user with the roles: • db_datareader • db_datawriter
Security Utility	Run Security Utility	Standard user requires administrator privileges.	

Minimum Privileges Required by Windows Users (Continued)

Component or Program	Task	Required Privileges	Notes
Web VideoViewer	Play video	Standard user must have a login to SQL Server. This restriction does not apply if the application.config file is configured to use the Lenel database user.	Map the AccessControl database to the user with the db_datareader role.
Web Area Access Manager	Assign and remove access levels to/from cardholders	Standard user must have a login to SQL Server. This restriction does not apply if the application.config file is configured to use the Lenel database user.	Map the AccessControl database to the user with the roles: • db_datareader • db_datawriter • db_executor
Replication Administration	Convert a standard OnGuard server to an Enterprise Master or Regional server	Add Modify permission for the standard user to the ACS.ini file.	
LS Message Broker service		LS Message Broker service is started with the Local System as the logon account.	
LS Site Publication Server service		LS Site Publication Server service has the domain administrator user as the logon account, or Local System if using Lenel Database authentication in the application.config file.	
LS Client Update Server service		LS Site Publication Server service has the domain administrator user or Local System as the logon account.	
LS Event Context Provider service		LS Event Context Provider service has the domain administrator user or Local System as the logon account if using Lenel Database authentication.	

Minimum Privileges Required by Windows Users (Continued)

Component or Program	Task	Required Privileges	Notes
System Management Console	Start and stop services	User launch the System Management Console as administrator.	
License Server	Run as an application	To run License Server as an application, you must run it as an administrator.	
Login Driver	Run as an application	To run Login Driver as an application, you must run it as an administrator.	
OpenAccess	Run as an application.	To run OpenAccess as an application, you must run it as an administrator.	

Database Installation and Configuration

CHAPTER 2

Installing and Configuring Oracle 12c Release 1 Server Software

The following overview and instructions are for the following Oracle 12c Release 1 Server installations:

- Single instance database(s) (no Real Application Cluster [RAC]/grid control)
- Enterprise Edition
- Oracle 12c Release 1 Database Server
- Enterprise Manager Database Express
- Windows Server 2012 R1 64-bit

If your configuration includes any customizations, or a different version of Oracle or Windows, then your procedures will differ from those provided in this chapter. Make adjustments accordingly.

An Oracle 12c Release 1 database-compatible Oracle 32-bit client must be installed on each OnGuard system, regardless of whether it will be an OnGuard server or client, and independent of whether it is also the database server. Oracle 64-bit clients will not work with the OnGuard software.

If you are using Windows 7 64-bit or Windows 8/Windows 8.1 64-bit, you might need to run Oracle applications, such as the Net Configuration Assistant, as an Administrator for configuration changes to persist.

If installing on a server with the IP address set to DHCP, then you must first configure a loop-back adapter.

When installing and configuring Oracle Database 12c, do not close any Oracle windows while a program is running. Doing so can result in configuration errors and loss of data. Instead, utilize the Oracle close or cancel buttons.

Oracle 12c Release 1 Server Software Configuration Overview

The following steps are necessary to install and configure Oracle Server for use with OnGuard:

1. Perform pre-installation planning. For more information, refer to Step 1: Pre-Installation Planning on page 12.
2. Install Oracle Database 12c. For more information, refer to Step 2: Install Oracle Database 12c Server Software on page 14.

3. Configure the Database server's Listener and Naming Methods by running the Net Configuration Assistant from the database's Oracle Home. For more information, refer to Step 3: Configure the Live Database Home Net Configuration on page 15.
4. Create the Live database. For more information, refer to Step 4: Create the Live Database on page 15.
5. If the Windows Firewall will be enabled on any Oracle client or server, then take the necessary steps to avoid firewall issues. For more information, refer to Step 5: Prevent Firewall Issues on page 17.
6. Perform Step 6: Configure the LISTENER Manually on page 17.
7. Verify that the Live database is accessible from the database home. For more information, refer to Step 7: Verify Live Database Accessibility from the Database Oracle Home on page 18.
8. Verify that the Live database is accessible from the Enterprise Manager. For more information, refer to Step 8: Verify Live Database Accessibility from the Enterprise Manager Database Express URL on page 18.
9. Perform Step 9: Prepare the User Scripts on page 19.
10. Create the Live Database Oracle users. For more information, refer to Step 10: Create the Live Database Oracle Users on page 20.
11. Create the Archival database. For more information, refer to Step 11: Create the Archival Database on page 21.
12. Install and configure the planned Oracle client. For more information, refer to Step 12: Install and Configure the Planned Oracle Client on page 21.
13. Install OnGuard 7.3. For more information, refer to Step 13: Install OnGuard 7.3 on page 21.

Note: Setup Assistant runs automatically after the OnGuard installation completes.

Oracle 12c Release 1 Server Software Installation and Configuration

The following installation and configuration steps are for Oracle 12c Release 1. Steps will vary for other versions of Oracle.

Step 1: Pre-Installation Planning

1. Review the *Oracle Database Installation Guide 12c Release 1 (12.1) for Microsoft Windows* plan and pre-installation sections. Be sure to note:
   - Minimum physical RAM, hard drive space, and software requirements
   - Virtual memory (swap) recommendations
   - IP address requirements (such as that DHCP requires a loopback adapter)
2. Use the Pre-Installation Planning Worksheet on page 13 to specify the planned configuration, including whether the system will archive to text files or to a separate database.

In addition to creating the required Live database, OnGuard provides two options for archiving Events, Events Video Location, Alarm Acknowledgments, User Transactions, Visits Records, and specific event types from the Live database tables. This helps keep the database from growing so large over time that system performance is adversely affected. The archiving options are:

- Archive to text files
- Archive to an Archival database

Note: By default, OnGuard replicates all data that can be archived to the Master server. For this reason, you might wish to Archive to database on the Master server only.

When deciding which Oracle Client to use, consider the Lenel recommendations and restrictions. Go to https://partner.lenel.com/downloads/onguard/software. Once there, select **Compatibility Charts** from the **Choose type of download** menu, and select the Databases chart.

Note: When accessing the **Downloads** section at https://partner.lenel.com, make sure to select the version of OnGuard that is currently installed.

Also review Oracle's *Client/Server/Interoperability Support Matrix for Different Oracle Versions (Doc ID 207303.1).*

Pre-Installation Planning Worksheet

	Sample Database Configuration	OnGuard Live Database	OnGuard Archival Database	Oracle Client
Host Name	SHost.sample .com			
Oracle Base	C:\app\Ouser			
Oracle Home	C:\app\Ouser\ product\12.1.0\ dbhome_1			
Oracle Home User	Sample\Ouser			
Global Database Name	LnlLive.sample .com			
Local Net Service Name (SID)	LnlLive			
Service Name	LnlLive.sample .com			
Port	1521			
Authentication User*	Sample\ AuthUser			

* The specified user must be the same for the Live and Archival database, if present.

Step 2: Install Oracle Database 12c Server Software

1. Launch the Oracle Universal Installer from the Oracle Database 12c Server disc or folder by running setup.exe.

Notes: Patch Sets are now released as part of Oracle full installation packages. To ensure you have an approved version, go to the Lenel web site at: https://partner.lenel.com/downloads/onguard/software. Once there, select **Compatibility Charts** from the **Choose type of download** menu, and then select the Databases chart.

When accessing the **Downloads** section at https://partner.lenel.com, make sure to select the version of OnGuard that is currently installed.

2. The Configure Security Updates window opens. Complete the Email and Password fields, and then click [Next]. You might need to provide Proxy server and port information.
3. The Download Software Updates window opens. If you wish to update the software, select the preferred option, and then click [Next]. Or you can select **Skip software updates**, and then click [Next].

Notes: Updates must be for an approved version of Oracle Database 12c Server. The list of approved versions can be found on the Lenel Web site at: https://partner.lenel.com/downloads/onguard/software. Once there, select **Compatibility Charts** from the **Choose type of download** menu.

When accessing the **Downloads** section at https://partner.lenel.com, make sure to select the version of OnGuard that is currently installed.

4. If you chose to update the software, the Apply Software Updates window opens. Select the appropriate option for applying all updates, and then click [Next].
5. The Select Installation Option window opens. Select **Install database software only**, and then click [Next].
6. The Grid Installation Options window opens. Select **Single instance database installation**, and then click [Next].
7. The Select Product Languages window opens. Use the arrow buttons to move the desired languages to the right pane, and then click [Next].
8. The Select Database Edition window opens. Select **Enterprise Edition**, and then click [Next].
9. In the Specify Oracle Home User window, select the windows account to run the Oracle services. Oracle recommends using a non-Administrator Windows user. Click [Next].
10. The Specify Installation Location window opens. Modify the Oracle Base to match the Oracle Base specified for the Live database in Step 1: Pre-Installation Planning on page 12, and then click [Next].
11. The Prerequisite Checks window opens, followed by the Summary window.
    a. Verify that the requirements are met, as shown in the Summary window.
    b. Click [Install]. The installation progress is shown in the Install Product window.

Note: The installation process might take several minutes or more, depending on your system resources.

12. The Finish window opens. Click [Close].

Step 3: Configure the Live Database Home Net Configuration

1. Start the ***Net Configuration Assistant*** from the database Oracle Home.
   For more information, refer to “Using OnGuard on Supported Operating Systems” in the Installation Guide.
2. The Net Configuration Assistant Welcome window opens.
   a. Confirm that the **Listener configuration** radio button is selected.
   b. Click [Next].
3. The Listener window opens.
   a. Select the **Add** radio button.
   b. Click [Next].
4. The Listener Name window opens.
   a. Confirm that the **Listener name** is `LISTENER`.
   b. If using a non-Windows Built-in user, then enter the Oracle Home User password.
   c. Click [Next].
5. The Select Protocols window opens.
   a. Confirm that **TCP** is a selected protocol.
   b. Click [Next].
6. The TCP/IP Protocol window opens.
   a. Select the **Use the standard port number of 1521** radio option.
   b. Click [Next].
7. The More Listeners window opens.
   a. Confirm that the **No** radio button is selected.
   b. Click [Next].
8. The Listener Configuration Done window opens. Click [Next].
9. The Oracle Net Configuration Assistant: Welcome window opens.
   a. Select the **Naming Methods configuration** radio button.
   b. Click [Next].
10. The Select Naming Methods window opens.
    a. In the **Available Naming Methods** list, select **Easy Connect Naming**.
    b. Click the right arrow button.
    c. Repeat steps a and b for **Local Naming**.
    d. Click [Next].
11. The Naming Methods Configuration Done window opens. Click [Next].
12. Click [Finish].

Step 4: Create the Live Database

1. Start the **Database Configuration Assistant** from the database Oracle Home.
   For more information, refer to “Using OnGuard on Supported Operating Systems” in the Installation Guide.
2. The Database Operations window opens.
   a. Verify the **Create Database** radio button is selected.
   b. Click [Next].

Note: The **Configure Database Options**, **Manage Pluggable Databases**, and **Delete Database** options are enabled only if you have an existing database.

3. The Creation Mode window opens.
   a. Select the **Advanced Mode** radio button.
   b. Click [Next].
4. The Database Template window opens.
   a. Select the **Custom Database** radio button.
   b. Click [Next]

Note: Selecting a template that does not include datafiles gives you full control to specify and change additional database parameters.

5. In the Database Identification window, specify the **Global Database Name**.
   a. Type `LnlLive.<fully qualified domain>` or just `LnlLive` (depending on whether your database server is in a domain or part of a workgroup) in the **Global Database Name** field.
   b. Click [Next].

Note: The Oracle System Identifier (SID) populates automatically with the first 12 alphanumeric characters.

6. The Management Options window opens. Select the **Configure Enterprise Manager (EM) Database Express** check box and then click [Next].
7. The Database Credentials window opens. Type the administrative password(s) you would like for the different accounts, enter the **Oracle Home User Password**, and then click [Next].
8. On the Network Configuration window, select the Listener configured previously and then click [Next].
9. The Storage Locations window opens. Choose the storage, recovery, and file locations, and then click [Next].

Note: The Enable Archiving recovery option is *not* related to the new OnGuard database archiving feature.

10. The Database Options window opens.
    a. Deselect all database components.
    b. Click [Next].
11. The Initialization Parameters window opens. Leave the default settings on the **Memory**, **Sizing**, **Character Sets**, and **Connection Mode** tabs, and then click [Next].
12. The Creation Options window opens. Ensure the **Create Database** check box is selected, then select the **Customize Storage Locations** button.
    a. In the Customize Storage window, rename the following tablespaces per the following table.
    b. Select the tablespace to rename.
    c. Enter the new tablespace name in the **Name** field.
    d. Update the **Size** field, entering the new size.
    e. Click [Apply] before selecting the next tablespace to modify.
    f. Click [OK] when done with all modifications.

The following table identifies the necessary tablespace names and recommended minimum sizes.

Old Tablespace names	New Tablespace names	New Size (MB)	Notes
USERS	LENEL_DATA	50	
TEMP	LENEL_TEMP	• 100 on General tab • 50 on Options tab, after selecting **Uniform**	Select **Uniform** on Options tab, not **Automatic**.
SYSTEM	SYSTEM	50	De-select **Use Automatic Segment Space Management**.
UNDOTBS1	UNDOTBS1	50	

Note: You can specify other names in the **Name** field. If you do, you must set the **defDataSpace** variable to the new **Name**. For more information, refer to Step 9: Prepare the User Scripts on page 19.

13. After Create Options configuration is complete, click [Next].
14. The Pre Requisite Checks window opens. If the checks pass, then it automatically transitions to the Summary window. Confirm the configuration, and then click [Finish].
15. The Progress Page is shown. This might take over 5 minutes depending on system resources.
16. Upon completion, the Database Configuration Assistant window opens and shows key information. Write down the **EM Database Express URL**, and then click [Exit].
17. From the Progress Page, click [Close] as long as all steps have a **Finished** status. Otherwise investigate and resolve the issue.

Step 5: Prevent Firewall Issues

Note: The following steps are only required if your Oracle server or client firewalls are enabled.

1. Open the Oracle LISTENER TCP port (typically 1521) for inbound and outbound traffic.

   For more information, refer to “Using OnGuard on Supported Operating Systems” in the Installation Guide.
2. To resolve port redirection issues, see Oracle Metalink Note 361284.1 and implement one of the options presented.

Step 6: Configure the LISTENER Manually

1. Open a Command Console window with Administrator privileges.

   For more information, refer to “Using OnGuard on Supported Operating Systems” in the Installation Guide.
2. In the Command Console window, navigate to the Live database Oracle Home’s Bin folder.
3. Run the following command: `lsnrctl start LISTENER`.

a. When prompted for the Oracle Home User's password, enter the password and then press <Return>.
b. To create and start the LISTENER's window service might take several minutes or more depending on your system resources.
c. When done the system should indicate "The command completed successfully.
d. Open Services and set the OracleOraDB12Home1TNSListener service to Automatic Startup type.

For more information, refer to "Using OnGuard on Supported Operating Systems" in the Installation Guide.

4. Restart the Live database host server.

Step 7: Verify Live Database Accessibility from the Database Oracle Home

1. Start the ***Net Configuration Assistant*** from the database Oracle Home.
For more information, refer to "Using OnGuard on Supported Operating Systems" in the Installation Guide.
2. The Net Configuration Assistant: Welcome window opens.
   a. Select the **Local Net Service Name configuration** radio button.
   b. Click [Next].
3. The Net Service Name Configuration window opens.
   a. Select the **Test** radio button.
   b. Click [Next].
4. The Select Net Service Name window opens.
   a. Select the Live Database's Local Net Service Name (SID) from the drop-down.
   b. Click [Next].
5. The Connecting window opens. Click [Change Login].
6. The Change Login dialog opens.
   a. Type the SYSTEM username and password (the same username and password that you set the password for in Step 4: Create the Live Database on page 15).
   b. Click [Next].
7. After successfully testing the service, click [Next].
8. Click [Finish].

Step 8: Verify Live Database Accessibility from the Enterprise Manager Database Express URL

1. Browse to the Enterprise Manager Database Express URL using Internet Explorer.
   a. You might need to edit the Internet options to add the site to the Local Intranet zone.
      For more information, refer to "Using OnGuard on Supported Operating Systems" in the Installation Guide.
   b. If you are presented with a warning regarding the website's security certificate, then allow the browsing to continue.
   c. If you do not have Adobe Flash Player installed or enabled (Windows 8/Windows 8.1/ Windows Server 2012 feature Desktop Experience), then you will be notified and presented with the "Get Flash" link.

For more information, refer to “Using OnGuard on Supported Operating Systems” in the Installation Guide

d. Login as the System user.

2. Confirm that the Live database is online and started.
3. Configure the DEFAULT profile.
   a. Select **Security > Profiles** and select the **DEFAULT** profile.
   b. Select **Actions > Alter Profile**.
   c. Set **Expire in (days)** to **Unlimited**.
   d. Set **Number of failed login attempts to lock after** to **Unlimited**.

Note: This is not a good long-term practice, but is useful prior to installing OnGuard and before the Login Driver is synchronized with the database.

   e. Click [OK].
4. Log out of Enterprise Manager.

Step 9: Prepare the User Scripts

IMPORTANT: Restricted user configuration allows you to avoid granting the Lenel and/or Windows Authenticated users the DBA role. This ensures that OnGuard Oracle users can only execute OnGuard functionality and not database-level administration tasks, such as backups and restores. This makes the Oracle database more secure. In fact, the restricted users will not be allowed to login to the Enterprise Manager Database Express.

1. Create a local folder on the Database server.
2. If restricting the Lenel user or configuring a Windows Authenticated user, then copy the <Path to OnGuard installation disc>\program files\OnGuard\DBSetup\New\RestrictedUserRole.ora to the local folder on the Database server.
3. Copy the <Path to OnGuard Install Disc>\program files\OnGuard\DBSetup\New\LenelUser.ora to the local folder on the Database server.
4. Edit the local copy of the LenelUser.ora file as described in the remarks in the file.
   a. If you chose not to use the LENEL_DATA and/or LENEL_TEMP tablespace names, then you must change the LENEL_DATA and/or LENEL_TEMP references on the CREATE USER line to match the tablespace names configured previously when creating the database. Contact your database administrator for details.
   b. If restricting the Lenel user, then comment out the GRANT line with DBA specified and un-comment the @@RestrictedUserRole.ora and the GRANT line with LENEL_RESTRICTEDUSER_ROLE specified.
   c. If you need to change the default LENEL password of “Secur1ty#”, then modify the CREATE USER line to reflect the desired password.
   d. Save and exit.
5. If you are NOT planning on using a Windows Authenticated user for application.config (Database Setup and OnGuard Web Applications), then continue to Step 10: Create the Live Database Oracle Users on page 20. Otherwise copy the <Path to OnGuard Install Disc>\program files\OnGuard\DBSetup\New\WindowsUser_Authentication.ora to the same local folder on the Database server as the LenelUser.ora script was placed.
6. Edit the local copy of the WindowsUser_Authentication.ora file as described in the remarks in the file.

a. If you chose not to use the LENEL_DATA and/or LENEL_TEMP tablespace names, then you must change the LENEL_DATA and/or LENEL_TEMP references on the CREATE USER line to match the tablespace names you configured previously when creating the database. Contact your database administrator for details.

b. If *not* restricting the Lenel user, then un-comment the @@RestrictedUserRole.ora line.

c. Replace “WindowsUser” references with Live Database Authentication User with an "OPS$" prefix.

d. Save and exit.

Step 10: Create the Live Database Oracle Users

1. Open a Command Console window.

   For more information, refer to “Using OnGuard on Supported Operating Systems” in the Installation Guide.

2. Change directory to the local folder with the modified scripts.

3. Start SQLPlus connecting as the Oracle System user to the Live database’s Local Net Service Name.

   For more information, refer to “Using OnGuard on Supported Operating Systems” in the Installation Guide.

   For example, `sqlplus system/<password>@<Local Net Service Name>`.

   IMPORTANT: You must be logged in as the System user, using the same password set on the Database Credentials window in Step 4: Create the Live Database on page 15.

4. Verify that Oracle connects properly. You should see “Connected to” in the console.

5. From the SQLPlus SQL prompt, run the following: `@@local folder path\LenelUser.ora`.

6. Verify there were no errors. You should see output similar to the following:

   ```
   "User created."
   "Role created." (IF Lenel user restricted)
   "Grant succeeded."  (Approximately 23 of these IF Lenel user restricted)
   "Commit complete." (IF Lenel user restricted)
   "Grant succeeded."
   "Commit complete."
   ```

7. If *not* configuring Windows Authentication, then skip to Step 11: Create the Archival Database on page 21.

8. At the SQL prompt, run the following: `@@WindowsUser_Authentication.ora`.

9. Verify there were no errors. You should see output similar to the following:

   ```
   "User created."
   "Grant succeeded."
   "Commit complete."
   ```

10. Exit SQL.

Step 11: Create the Archival Database

Notes: The following steps are only required if you plan to Archive to a database.

By default, OnGuard replicates all data that can be archived to the Master server. For this reason, you might wish to Archive to database on the Master server only.

If you plan to archive to an Archival database, then create the Archival database by performing the following steps *after* creating the Live database. References to the Live database or its settings should be replaced with the Archival database or its settings.

1. Repeat Step 4: Create the Live Database on page 15 to create the Archival database, but:
   a. Change the Database name to LnlArch.<fully qualified domain> or just LnlArch (depending on whether your database server is in a domain or part of a workgroup) in the Global Database Name field, or whatever you specified in the table entry for OnGuard Archival Database's Global Database Name in Step 1: Pre-Installation Planning on page 12.
   b. Use the same listener created for the Live database.
2. Repeat Step 7: Verify Live Database Accessibility from the Database Oracle Home on page 18.
3. Repeat Step 8: Verify Live Database Accessibility from the Enterprise Manager Database Express URL on page 18.
4. Repeat Step 10: Create the Live Database Oracle Users on page 20.

Note: Utilize the same local folder and scripts that were modified for the Live database.

5. The Archival database is now ready for use.

For detailed information about the Live and Archival databases, refer to the Archives Folder chapter in the System Administration User Guide.

Step 12: Install and Configure the Planned Oracle Client

Oracle client software is required on every planned OnGuard server and OnGuard client that will connect to the Live and, if present, Archival database.

Install and configure the planned Oracle client.

For detailed information about Oracle Client 12c, refer to Chapter 3: Installing and Configuring Oracle 12c Release 1 Client Software on page 23.

Step 13: Install OnGuard 7.3

Install the OnGuard 7.3 software.

For detailed information about installing OnGuard, refer to the Installing OnGuard 7.3 chapter in the OnGuard 7.3 Installation Guide.

Note: If Windows single sign-on is used for database authentication, log in as the Windows (domain or local) user specified during the Oracle user creation.

CHAPTER 3

Installing and Configuring Oracle 12c Release 1 Client Software

IMPORTANT: If you are using Windows 7, you might need to run Oracle applications, such as the Net Configuration Assistant, as an Administrator for configuration changes to persist.

Oracle 12c Release 1 Client Installation and Configuration

Step 1: Install Oracle 12c Release 1 Client

IMPORTANT: If installing the 64-bit version of Oracle Database, you must also install the 32-bit version of the client tools or OnGuard will not work properly.

1. Launch Oracle Universal Installer from the Oracle Client 12c Release 1 disc or folder by running setup.exe.

Notes: Patch Sets are now released as part of Oracle full installation packages. To ensure you have an approved version, go to https://partner.lenel.com/downloads/onguard/software. Once there, select **Compatibility Charts** from the **Choose type of download** menu, and then select the Databases chart.

When accessing the **Downloads** section at https://partner.lenel.com, make sure to select the version of OnGuard that is currently installed.

2. The Select Installation Type window opens.
   a. Select the **Administrator** radio button.
   b. Click [Next].
3. If the Download Software Updates window opens, and if you wish to update the software, select the preferred option, and then click [Next]. Or you can select **Skip software updates**, and then click [Next].

Notes: Updates must be for an approved version of Oracle Client 12c Release 1. The list of approved versions can be found on the Lenel Web site at: https://partner.lenel.com/

downloads/onguard/software. Once there, select **Compatibility Charts** from the **Choose type of download** menu

When accessing the **Downloads** section at https://partner.lenel.com, make sure to select the version of OnGuard that is currently installed.

4. If you chose to update the software, the Apply Software Updates window opens. Select the appropriate option for applying all updates, and then click [Next].
5. The Select Product Languages window opens. Move the desired languages to the right pane using the arrow buttons, and then click [Next].
6. The Specify Oracle Home User window opens. Select the windows account to run the Oracle services. Oracle recommends using a non-Administrator Windows user. Lenel recommends using the same Oracle Home User as the Live database you will be connecting to. Click [Next].
7. The Specify Installation Location window opens. Modify the Oracle base to match the Oracle Base specified for the Live database *if* this Oracle client host is also the Oracle Live Database host. Otherwise accept the defaults, and then click [Next].

Note: This recommendation should be acceptable even if the Oracle client and Oracle database are different versions because the Software location should reflect a differentiating version sub-directory as well as a unique home name.

8. The Summary window opens.
   a. Verify that the settings meet the desired configuration.
   b. Click [Install].
9. The Install Product window opens, showing the progress of the installation. The installation process might take several minutes or more depending on your system resources.

Note: The installer wizard window closes if installing the Oracle Client on a Windows Server 2012 R2 workstation that also has the Oracle Server installed. The Oracle Client cannot be installed on a Windows 8.1 64-bit workstation without the Oracle Server.

10. The Finish window opens. Click [Close].

Step 2: Prevent Firewall Issues

Note: The following sub-steps are only required if your Oracle Server or Client firewalls are enabled.

1. Open the Oracle LISTENER TCP port (typically port 1521) for Inbound and Outbound traffic.

   For more information, refer to “Using OnGuard on Supported Operating Systems” in the Installation Guide.
2. To resolve port redirection issues, see Oracle Metalink Note 361284.1 and implement one of the options presented.

Step 3: Add Local Net Services Name(s)

1. Start the Net Configuration Assistant from the client Oracle Home.

   For more information, refer to “Using OnGuard on Supported Operating Systems” in the Installation Guide.
2. The Net Configuration Assistant Welcome window opens.
   a. Confirm the **Local Net Service Name configuration** radio button is selected.

b. Click [Next].

3. The Net Service Name Configuration window opens.
   a. Select the **Add** radio button.
   b. Click [Next].
4. The Service Name window opens.
   a. Enter the Live database's Global Database Name.
   b. Click [Next].
   c. Verify TCP is selected and then click [Next].
   d. Enter the Live database's Host Name, accept the default standard port of 1521, and then click [Next].
   e. Select the **Yes, perform a test** radio button, and then click [Next].
   f. Select the **Change Login** radio button.
   g. Enter the Live database's System User and Password.
   h. Observe the details, which should indicate that the test was successful.
   i. Click [Next].
   j. Accept the default Net Service Name, which should match the Live database's Local Net Service Name (SID), and then click [Next].
   k. Select the **No** radio button, and then click [Next].
5. The Net Service Name Configuration window opens. Click [Next].
6. If an Archival Database is utilized, then repeat steps 2 through 5, replacing the Live Database settings and references with the Archival Database settings. Otherwise, continue to step 7.
7. Select the **Naming Methods configuration** radio button.
   a. Click [Next].
8. The Select Naming Methods window opens.

Note: If the client host is also a database host, then these setting might already be present.

   a. In the **Available Naming Methods** list, select **Easy Connect Naming**.
   b. Click the right arrow button.
   c. Repeat steps 8a and 8b for Local Naming.
   d. Click [Next].
9. The Naming Methods Configuration Done window opens. Click [Next].
10. Click [Finish].

Advanced Installation Topics

CHAPTER 6

Transparent Data Encryption

Transparent data encryption (TDE) performs real-time I/O encryption and decryption of the database and database log files. (Standard OnGuard log files are not encrypted.)

The encryption uses a database encryption key (DEK), which is stored in the database boot record for availability during recovery. The DEK is a symmetric key secured by using a certificate stored in the master database of the server or an asymmetric key protected by an EKM module. TDE protects data "at rest," meaning the data and log files. It provides the ability to comply with many laws, regulations, and guidelines established in various industries.

For detailed information, refer to "Understanding Transparent Data Encryption" http://msdn.microsoft.com/en-us/library/bb934049.aspx.

IMPORTANT: TDE does not provide encryption across communication channels. For more information about how to encrypt data across communication channels, refer to "Encrypting Connections to SQL Server" http://msdn.microsoft.com/en-us/library/ms189067.aspx.

Enabling TDE

To utilize TDE for the OnGuard database, the system should have Windows Server 2012 R2 or Windows Server 2012 and SQL Server 2012 or SQL Server 2014 installed.

To enable TDE, refer to the section, "Using Transparent Database Encryption" in the article, "Understanding Transparent Data Encryption" http://msdn.microsoft.com/en-us/library/bb934049.aspx.

Note: Encryption is CPU intensive. Therefore, servers with high CPU usage will suffer performance loss.

Backing up a TDE Protected Database

To back up a TDE protected database, refer to step 2 of the section, “To create a database protected by transparent data encryption” in the article, “Move a TDE Protected Database to Another SQL Server” http://msdn.microsoft.com/en-us/library/ff773063.aspx

When enabling TDE, you should immediately back up the certificate and the private key associated with the certificate. If the certificate ever becomes unavailable or if you must restore or attach the database on another server, you must have backups of both the certificate and the private key or you will not be able to open the database.

Moving a TDE Protected Database

For information on moving a TDE protected database to another SQL server, refer to http://msdn.microsoft.com/en-us/library/ff773063.aspx.

If you need to move the database, the database can be attached or restored on another SQL server.

Attach the Database to Another SQL Server

1. Detach the TDE protected database by using Management Studio. In Object Explorer, right-click the database, point to tasks, and then select **Detach**.
2. Move or copy the detached database files from the source server to the same location on the destination server.
3. Move or copy the backup of the server certificate and the private key file from the source server to the same location on the destination server.
4. Create a database master key on the destination instance of SQL Server.
5. Recreate the server certificate by using the original server certificate backup file. The password must be the same as the password that was used when the backup was created.
6. Attach the database that is being moved by using Management Studio. In Object Explorer, right-click the database, and then select **Attach**.

Restore the Database on Another SQL Server

1. Back up the TDE protected database by using Management Studio. In Object Explorer, right-click the database, point to tasks, and then select **Backup**.
2. Move or copy the backup database file from the source server to the same location on the destination server.
3. Move or copy the backup of the server certificate and the private key file from the source server to the same location on the destination server.
4. Create a database master key on the destination instance of SQL Server.
5. Recreate the server certificate by using the original server certificate backup file. The password must be the same as the password that was used when the backup was created.
6. Restore the database that is being moved by using Management Studio. In Object Explorer, right-click the database, and then select **Restore**.

CHAPTER 7

Remote Installation of OnGuard

• WARNING! • These features should only be used for client installations. Lenel does not recommend or support centralized installation or upgrading of servers because servers require additional care and attention.

Automatic Client Updates

The Client Update Server allows the OnGuard server workstation to automatically update client workstations. When a client workstation opens an application in OnGuard, the application detects that the software version does not match the database. The application then allows the user to either cancel the login or update the client software. This functionality only exists for applications that are part of the OnGuard installation suite.

Two services enable this functionality, one installed on the server workstation (LS Client Update Server service) and another installed on each client workstation (LS Client Update service). These services are only used to update client workstations. Server workstations must still be updated manually. The LS Client Update Server service is not running by default, but the LS Client Update service starts automatically.

IMPORTANT: After enabling the automatic client updates feature, all Security Utility system modifications and license terms are accepted automatically on the client workstation being updated.

Notes: Keep the old license in the License Server so that the out-of-date client can start and check for an update. Once updated, the new client will use the new license.

At startup, Client Update application checks to see if server components are installed on the client workstation. If the application finds any server component other than the Communication Server, then the client update is canceled and the user sees an error message.

For information on troubleshooting automatic client update functionality, refer to Client Update Troubleshooting in the System Administration User Guide.

This functionality only applies to new releases, service packs, and incremental updates where the OnGuard version number has changed.

Service packs always contain the base installation plus the service pack. This enables a client workstation with OnGuard to update directly to an OnGuard service update.

Server Performance Considerations and .MSI File Locations

Remember the following when deciding which workstation should host the LS Client Update Server service:

- The LS Client Update Server service can only be installed on one workstation in the system. Select the server that provides the best download performance to all client workstations in the system.
- The server must download the client installation package in less than 30 minutes, or the download will time out. A network latency of 70 ms or less (round trip), with a packet loss of 5% or less, will allow the client installation package to download in the required time.
- Ping the client workstations from the server workstation you are considering to confirm these performance specifications. If the performance is not adequate, select a different server location, or push the client installation package to the client workstations to prepare for the upgrade.
- The client installation package (**Installation Package.msi** file) is located on the server workstation at the root level of the installed OnGuard directory. On the client workstations, place or push the **Installation Package.msi** file into the \ClientUpdate subdirectory of each client's installed OnGuard directory.
- If using the Automatic Client Update process to install OnGuard on a workstation that does not already have OnGuard, or on a client workstation running a version of OnGuard earlier than 7.3, place or push the **Installation Package.msi** file into the same directory as the other required LS Client Update service application files. For more information, refer to Manual Client Update Workflow on page 34.

Note: When the OnGuard update installation completes, the **Installation Package.msi** file is deleted from the client workstation automatically.

LS Client Update Server service

This server workstation function is configured and enabled using the Client Update form in **System Administration > Administration > System Options**. For Enterprise or Distributed ID installations, these settings are configured on a per-system basis and the information is not replicated. For more information on configuring the LS Client Update Server service, refer to Client Update Form Procedures in the System Administration User Guide.

LS Client Update service

This client workstation service is responsible for installing OnGuard so that users do not need Administrator privileges. The application also communicates with the server-side LS Client Update Server service when downloading and installing update packages.

The LS Client Update service is installed automatically with all supported OnGuard versions. The application can also be run manually on workstations that do not have the OnGuard software installed. Manually running this application requires Administrator privileges.

Automatic Client Update Workflow

The workflow between the LS Client Update Server service and the LS Client Update service is as follows:

Notes: This workflow assumes that the OnGuard server workstation is already installed and configured to run the LS Client Update Server service, as described in Client Update Form Procedures in the System Administration User Guide.

This workflow also assumes that the server and client are running a supported version of the OnGuard software.

1. The client user attempts to login to an application in OnGuard, and then receives a message that the OnGuard installation is out of date, and asks if the user wants to upgrade now or later. If user selects later, the OnGuard application closes.

   If the user selects now, the OnGuard application closes and the LS Client Update service application launches.

Notes: The user always has the option to cancel a client update that is in progress.

If the user cancels while in the download queue (refer to Step 4) and then initiates a client update again, the user is placed at the back of the queue.

If the user cancels while the installation package is downloading and then initiates a client update again, the download continues from where it left off (download is queued if the maximum concurrent downloads is reached, as described in Step 4).

If the user cancels an installation that is in progress, the user can run the installation package again.

2. The LS Client Update service application attempts to reach the LS Client Update Server service location, and displays an error message if unsuccessful.
3. Once the connection is made, the LS Client Update service application requests a download of the OnGuard installation package.

Notes: Before requesting the download, the LS Client Update service checks to see if the installation package (**Installation Package.msi** file) was already placed or pushed onto the client workstation. If so, the process skips to Step 7.

If the download begins but fails (due to timeout, network outage, cancelled by client, and so on), the download will resume from where it left off when the user restarts the download.

4. The LS Client Update Server service either starts downloading the OnGuard installation package (**Installation Package.msi** file) and logs a Download Started transaction in the User Transaction Log, or places the client in the download queue.

   If the maximum number of concurrent client downloads is reached, the LS Client Update service application informs the user of the position in the queue. The server logs a Queued for Download transaction in the User Transaction Log.
5. The LS Client Update service application receives the installation package, and verifies it was not corrupted during transfer.
6. The LS Client Update service application notifies the LS Client Update Server service that the download was successful. The server logs a Download Finished transaction in the User Transaction Log.

7. The LS Client Update service application starts installing the OnGuard client update with no user prompts (unattended installation mode). The client also notifies the LS Client Update Server service to log an Installation Started transaction in the User Transaction Log.

Note: If the installation fails, the user can retry the installation. Users are notified that the installation has failed. After fixing the cause of the failure, the user clicks [Retry].

8. Once the installation is complete, the LS Client Update service application notifies the LS Client Update Server service to log an Installation Finished transaction in the User Transaction Log.
9. The LS Client Update service application deletes the installation package from the client workstation.
10. The LS Client Update service application notifies the user that the installation is complete. The user then closes the application.

Note: To run a detailed report of the client update statistics, refer to Running a Client Update Report in the System Administration User Guide.

Manual Client Update Workflow

The workflow between the LS Client Update Server service and the LS Client Update service is as follows:

Notes: This workflow assumes that the OnGuard server workstation is already installed and configured to run the LS Client Update Server service, as described in Client Update Form Procedures in the System Administration User Guide.

This workflow also assumes that the required LS Client Update service application file was placed manually on client workstations running a supported version of the OnGuard software. The required file is: **Lnl.OG.AutoUpgrade.Client.exe**.

This file can be found on the OnGuard disc, in the **\program files\OnGuard** directory. This same directory also contains the **installation package.txt** file, which describes the purpose and process for using the application file, and which can be distributed to the client workstations along with the application file.

In addition, Microsoft .NET Framework 4.6.1 must be installed before running the LS Client Update Service application manually.

The application file is small enough that it can be easily distributed as an e-mail attachment.

1. The user launches the Lnl.OG.AutoUpgrade.Client.exe application.

Note: The application prompts users who do not have Administrator privileges to provide an administrator's user name and password. The Client Update workflow will not proceed without an administrator's login information.

2. The LS Client Update service application asks the user for the LS Client Update Server service location, and the port to use. For client workstations that do not already have OnGuard installed, the application allows the user to select the **Installation type**:
   - Typical client (all features)
   - Monitoring client
   - Badging and credential client
3. The LS Client Update service application attempts to reach the LS Client Update Server service location, and displays an error message if unsuccessful.

4. Once the connection is made, the LS Client Update service application requests a download of the OnGuard installation package.

Notes: Before requesting the download, the LS Client Update service checks to see if the installation package already exists on the client workstation. If it does, the process skips to Step 8.

If the download begins but fails (due to timeout, network outage, cancelled by client, and so on), the download will resume from where it left off when the user restarts the download.

5. The LS Client Update Server service either starts downloading the OnGuard installation package and logs a Download Started transaction in the User Transaction Log, or informs the user of the position in the download queue.
6. The LS Client Update service application receives the installation package, and verifies it was not corrupted during the transfer.
7. The LS Client Update service application notifies the LS Client Update Server service that the download was successful. The server logs a Download Finished transaction in the User Transaction Log.
8. The LS Client Update service application starts installing the OnGuard client update with the normal user prompts. The client also notifies the LS Client Update Server service to log an Installation Started transaction in the User Transaction Log.

Note: If the installation fails, the user can retry the installation. Users are notified that the installation has failed. After fixing the cause of the failure, the user clicks [Retry].

9. Once the installation is complete, the LS Client Update service application notifies the LS Client Update Server service to log an Installation Finished transaction in the User Transaction Log.
10. The LS Client Update service application deletes the installation package from the client workstation.
11. The LS Client Update service application notifies the user that the installation is complete. The user then closes the application.

Note: To run a detailed report of the client update statistics, refer to “Running a Client Update Report” in the *System Administration User Guide*.

Manual Unattended Client Deployment

The Manual Unattended Client Deployment method makes use of a compressed OnGuard client installation package for custom unattended deployment initiatives. Specific user-defined parameters are passed to a special package provided within the source media.

IMPORTANT: In order to use this deployment method properly, follow the instructions as provided. Any attempt to alter the installation options or use additional switches can potentially block certain layers of configuration in the product installation, resulting in an incomplete and non-functioning installation.

Manual Unattended Client Workflow

This deployment method consists of the following steps:

1. Obtain the full OnGuard installation source media.
2. From the OnGuard installation source media, browse to **program files** > **OnGuard** > **Installation Package.msi**.

Note: Make sure to locate the **Installation Package.msi** file and not another ,msi file on the source media. The **Installation Package.msi** file is over 500 MB in size and includes the entire client deployment file set.

3. Make a copy of the **Installation Package.msi** file and place the copy elsewhere (for example, the desktop or the root level of a drive).

   The **Installation Package.msi** file is the only file required to stage and deploy unattended clients. No other files are needed from the source installation media.

4. Once the copy of the **Installation Package.msi** file is staged for deployment, specific command line parameters applied to the **msiexe.exe** file can be used to silently deploy client installations. Use the specified parameters as shown in Command Line Parameter Reference on page 36.

Command Line Parameter Reference

IMPORTANT: Do not deviate from the following parameters as certain overrides (such as /**qb** and **/qr** quiet modes) can suppress critical third party and configuration elements necessary for the client to properly install.

Notes: The use of quiet modes is not required because OnGuard has a custom **CLIENTUPDATE** property that controls the user interface suppression levels to deny user intervention, but to allow required configuration to occur.

Only use straight/ambidextrous quotation marks instead of curly/smart quotation marks for parameters. Curly/smart quotation marks are not supported.

To ensure you have the required privileges to fully configure OnGuard, run the **msiexec.exe** file as an administrator by right-clicking on the file and selecting **Run as Administrator.**

Required Command Line Parameter

The following command line parameter must be passed to the **msiexec.exe** file when client installations are deployed.

```
CLIENTUPDATE=\"1\" LICENSESERVER=\"{0}\" LSPORT=\"{1}\"
DSN=\"{2}\" DATABASETYPE=\"{3}\"REBOOT=Suppress
```

- **{0}** is the license server name
- **{1}** is the license server port
- **{2}** is the database server name (this is the name of the server hosing the database that the DSN will point to)
- **{3}** is the database type [SQL]

Optional Command Line Parameters

The following optional command line parameter allows you to select which features to include in the installation. By default, all standard client features are included in the installation and are deployed unless removed by an optional command line parameter. Only use the optional command line parameter when you need to explicitly specify which features to include and exclude.

If you do not specify whether to include or exclude a feature, that feature is deployed based on its default feature level.

```
ADDLOCAL="{A},{C},{E},{G}" REMOVE="{B},{D},{F},{H}"
```

{A…Z} Feature List:

- AlarmMonitoring[1]
- AreaAccessManager[1]
- BadgeDesigner[1]
- DeviceDiscovery[2]
- DeviceDiscoveryService[2]
- FormsDesigner[1]
- IDCredentialCenter[1]
- MapDesigner[1]
- SkyPointIntegrationAdvancedFeatures[2]
- SystemAdministration[1]
- VisitorManagement[1]
- VideoViewer[1]

[1] Features delivered by default in a standard client installation

[2] Features not delivered by default in a standard client installation

Note: Unless you have a specific intent to use the features not delivered by default in a standard client, it is recommended that you do not include them in your custom deployment.

Examples

The following examples show how to execute Unattended OnGuard Client Deployment.

Example 1: A typical unattended deployment from a network location.

```
msiexec /i "\\SomeNetworkLocation\My OnGuard Installer
Folder\Installation Package.msi" CLIENTUPDATE="1"
LICENSESERVER="MyLicenseServer" LSPORT="1" DSN="MySQLDBServer"
DATABASETYPE="SQL" REBOOT=Suppress
```

Example 2: An unattended deployment from a local drive source location with specific features included and excluded.

```
msiexec /i "C:\MyInstall\Installation Package.msi"
CLIENTUPDATE="1" LICENSESERVER="OurServer" LSPORT="1"
DSN="OurServer" DATABASETYPE="SQL" REBOOT=Suppress
ADDLOCAL="AlarmMonitoring,IDCredentialCenter,MapDesigner,SystemAd
ministration"
REMOVE="AreaAccessManager,BadgeDesigner,FormsDesigner,DeviceDisco
very,
DeviceDicoveryService,SkyPointIntegrationAdvancedFeatures,Visitor
Management,VideoViewer"
```

Note: The formatting in Example 2 shows line returns where there are spaces. To see how the formatting would appear in a command prompt, copy Example 2 and paste it into a simple text editor.

CHAPTER 8

VMware

VMware provides a way to create a virtual machine. OnGuard server software and the Communication Server are certified to run on VMware ESXi.

VMware Installation

Installation of VMware ESXi should be performed according to the manufacturer documentation. Be sure the physical server (host) and storage array are listed on the hardware compatibility list for ESXi to meet the minimum requirements.

Also, take into consideration the minimum requirements of the applications that will be installed on the virtual machine (guest).

Virtual Machine Setup

Once installation of ESXi is complete, start the vSphere Client. Using the vSphere Client, connect to the ESXi server and create a new virtual machine.

Creating a New Virtual Machine

1. From the vSphere Client, click ***File > New > New Virtual Machine***. Doing so launches the Create New Virtual Machine wizard.
2. Select the configuration for the virtual machine by defining the operating system, machine name, disk capacity, etc. If needed, some of these settings (for example, memory) may be modified after the virtual machine has been created.
3. Install the operating system.
4. Install VMware Tools.

Note: For more detailed information, refer to the VMware documentation.

5. Once the virtual machine has been created, install OnGuard according to the instructions in the Installation Guide.

Recommended Hardware Configurations

The following are general recommendations and might change depending on the size and scope of the system.

OnGuard VMware configurations

Configuration	RAM	Available Disc Space	CPU Cores
32ES and ADV	8 GB	200 GB with thick provisioning	4
PRO, ENTREG, and ENTMAS	8 GB	200 GB with thick provisioning	4
Client PC	4 GB	200 GB with thick provisioning	2
Video Client	Not supported		

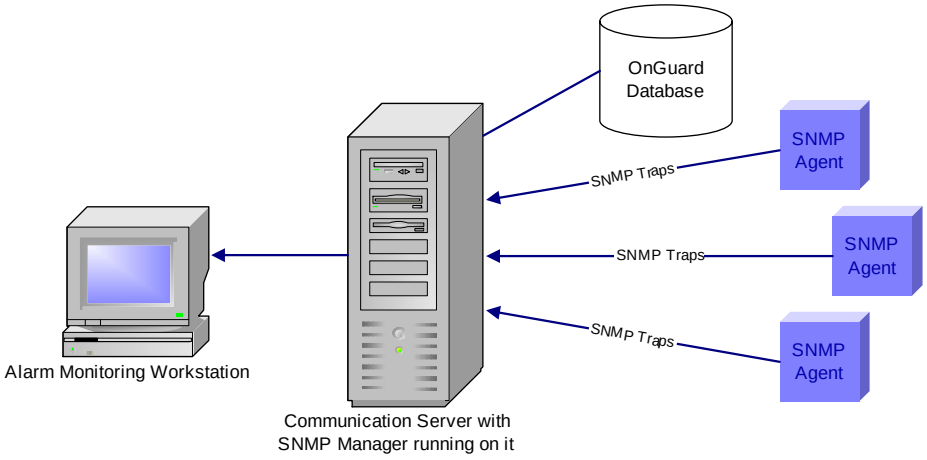
CHAPTER 9

Using SNMP with OnGuard

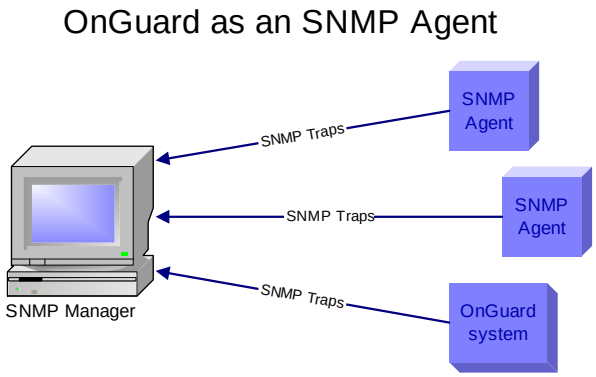
Note: OnGuard only supports SNMPv1 Traps, whether they are sent when OnGuard is configured as an Agent, or if they are received when OnGuard is configured as an SNMP Trap Manager.

SNMP (Simple Network Management Protocol) is used primarily for managing and monitoring devices on a network. This is achieved through the use of get and set requests which access and modify variables on a given device, as well as SNMP traps which are used to notify Managers of changes as they occur. The device which is being managed or monitored is called the *Agent*. The application that is doing the managing or monitoring is called the *Manager*. You can think of a Manager as the coach of a team, and Agents as all the players on the team. The following diagram illustrates how OnGuard can be used as an SNMP Manager:

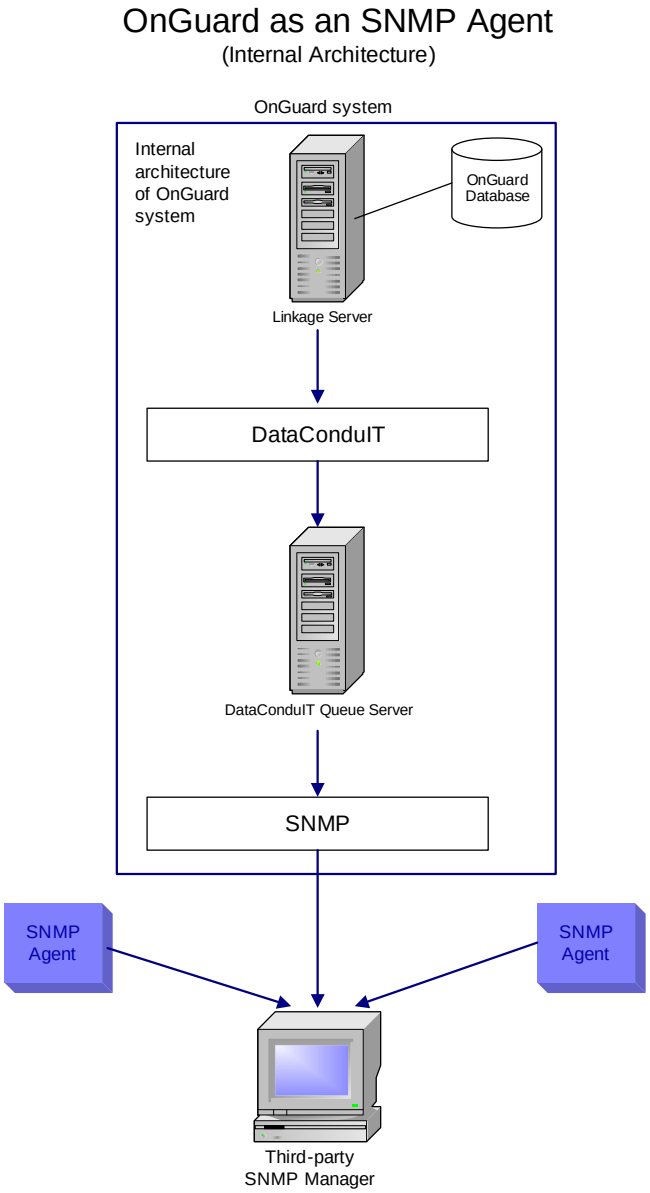
OnGuard as an SNMP Manager



Agents generate *trap messages*, which are sent to a Manager to indicate that something has changed. Trap messages generally contain the system uptime, the trap type, and the enterprise number. OnGuard uses Enterprise specific trap messages to send alarms to SNMP Managers. OnGuard generates trap messages, but does not listen for messages from SNMP Managers. The following diagram illustrates how OnGuard can be used as an SNMP Agent:



Configuring OnGuard as an SNMP Agent requires the use of DataConduIT and the DataConduIT Queue Server, as shown in the diagram that follows.



Why use SNMP with OnGuard? This depends on whether you are using OnGuard as an SNMP Manager or as an SNMP Agent.

OnGuard as an SNMP Manager

When OnGuard is used as an SNMP Manager:

- You can monitor hardware or software applications in OnGuard that you couldn't monitor before without a specific integration.
- If you already have OnGuard installed and are using a third-party application to monitor SNMP traps, you can now move that functionality over to OnGuard and monitor everything in a central location.
- By loading into OnGuard the MIB file for the SNMP Agents you are monitoring, you can customize how the information from the SNMP Agent is displayed in Alarm Monitoring
- Based on the information received and displayed in OnGuard, you can create custom alarm and Global I/O linkages for the trap, as well as take advantage of other existing OnGuard functionality.

To set up OnGuard to function as an SNMP Manager, you must configure an SNMP Manager on a workstation. This is done through System Administration. In addition to configuring the SNMP Manager, you can also load up third party MIB files into OnGuard, which will allow you to customize how SNMP Traps are handled and displayed in the OnGuard software. For more information, refer to the SNMP Managers Folder chapter in the System Administration User Guide.

OnGuard as an SNMP Agent

OnGuard hardware and software events can be reported as SNMP traps to third-party applications with SNMP trap support.

To configure OnGuard as an SNMP Agent, you must configure an SNMP Trap Message queue within the DataConduIT Message Queue configuration in System Administration. You can specify what events you want sent out through this queue (as SNMP Traps) and where you want them sent. For more information, refer to the DataConduIT Message Queues Folder chapter in the System Administration User Guide.

After setting this up, you must load the Lenel MIB file (located in the **SNMP** folder on the OnGuard Supplemental Materials disc) into your SNMP Manager application. For more information, refer to the SNMP Managers Folder chapter in the System Administration User Guide.

Configuring SNMP

The following steps must be completed before you configure OnGuard as either an SNMP Manager or an SNMP Agent:

1. Install the Windows SNMP components. You will need your Windows CD to complete this procedure. For more information, refer to Install the Windows SNMP Components on page 44.
2. Install a license with SNMP support.

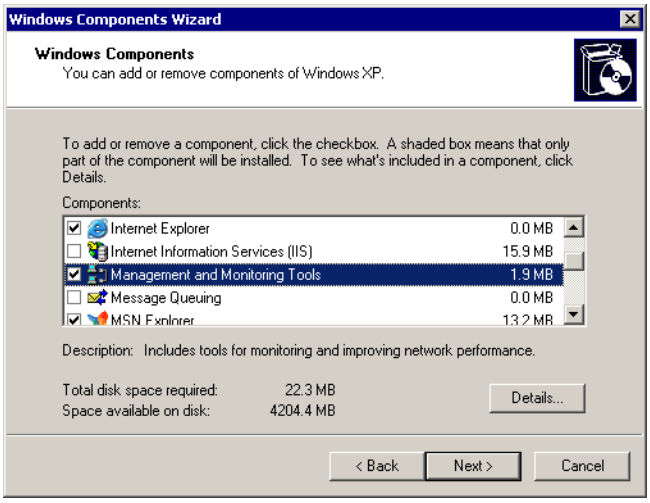
To configure OnGuard as an SNMP Manager, refer to Configuring OnGuard as an SNMP Manager on page 46.

Install the Windows SNMP Components

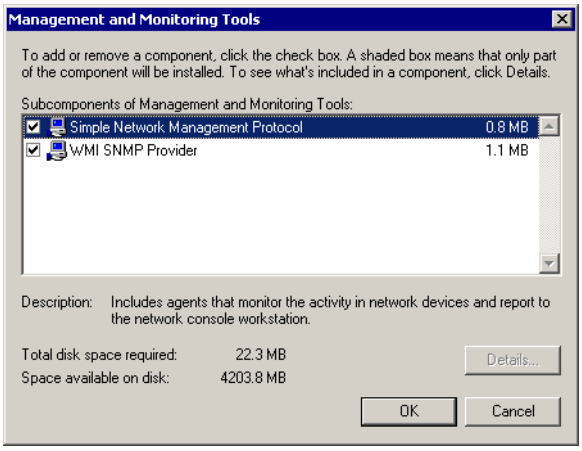
Before configuring an SNMP Manager to run on a Communication Server, the Windows SNMP components must be installed on the Communication Server machine.

IMPORTANT: You will need your Windows CD to complete this procedure.

1. In Windows, open the Control Panel. For more information, refer to "Using OnGuard in the Supported Operating Systems" in the Installation Guide.
2. Double-click "Add or Remove Programs".
3. The Add or Remove Programs window opens. Click "Add/Remove Windows Components".
4. The Windows Components Wizard window opens. Select the **Management and Monitoring Tools** check box.

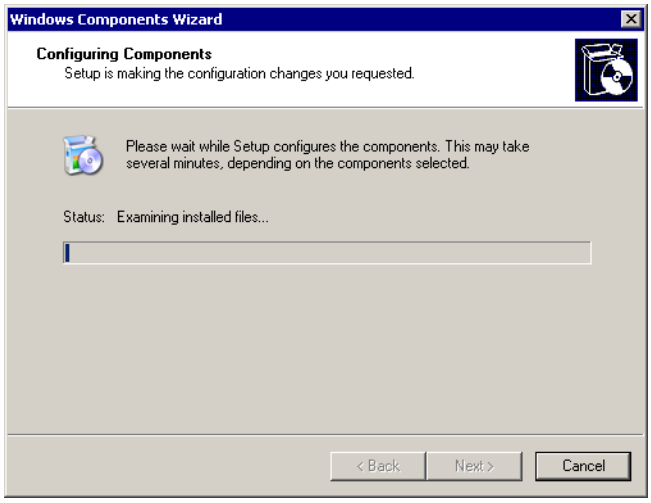


5. Click [Details].
6. The Management and Monitoring Tools window opens. Verify that the Simple Network Management Protocol check box is selected, and then click [OK].

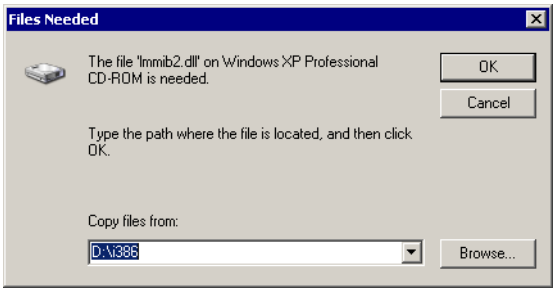


7. Click [Next].

8. The Configuring Components window opens. The status bar is updated as the installation proceeds.



9. When prompted, insert the Windows CD-ROM.
   a. If the Windows autorun screen opens, close it.
   b. If your CD-ROM is the D drive, click [OK].
   c. If your CD-ROM is not the D drive by default, navigate to the correct drive letter of your CD-ROM. Select the **I386** folder, and then click [OK].



10. A message indicating that you have successfully completed the Windows Components Wizard is displayed. Click [Finish].

Install a License with SNMP Support

The following SNMP features in OnGuard are licensed:

- Support for SNMP Managers. If you are licensed to use this feature, “SNMP Managers Support” in the Access Control Options section is set to “true”.
- Number of SNMP trap message queues. The number of queues you are licensed to use is displayed in the “Maximum Number of SNMP Trap Message Queues” setting in the General section of the license.

Configuring OnGuard as an SNMP Manager

Prerequisites:

1. Install the Windows SNMP components. You will need your Windows CD to complete this procedure. For more information, refer to Install the Windows SNMP Components on page 44.
2. Install a license with SNMP support.

To configure OnGuard as an SNMP Manager:

1. Add an SNMP Manager using System Administration. For more information, refer to Add an SNMP Manager on page 46.
2. Add Agents using System Administration. For more information, refer to Add Agents on page 47.
3. Load the MIB file(s). For more information, refer to Load the MIB File(s) on page 48.

Add an SNMP Manager

1. In System Administration, select ***SNMP Managers*** from the ***Additional Hardware*** menu. The SNMP Managers folder opens.
2. On the SNMP Managers tab, click [Add].
3. If segmentation is not enabled, skip this step. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this SNMP Manager will be assigned to.
   b. Click [OK].
4. In the **Name** field, type a name for the SNMP Manager.
5. Select whether the SNMP Manager will be online.
   a. Allow the **Online** check box to remain selected if you want the SNMP Manager to be ready for use. When an SNMP Manager is online, the Communication Server listens for trap messages from SNMP Agents.
   b. Deselect the **Online** check box if the SNMP Manager is not ready for use. When an SNMP Manager is not online, the Communication Server does not listen for trap messages from SNMP Agents.
6. On the Location sub-tab, select the **Workstation** (or server) that the SNMP Manager is or will be running on in order to receive events. The Communication Server must be present on the specified workstation. You can either type the name in the field, or use the [Browse] button to view a list of available workstations.

Notes: You are required to enter the workstation's NetBIOS name. (The NetBIOS name is specified when Windows networking is installed/configured.)

Only one SNMP Manager is allowed to run on each Communication Server. You can have several Communication Servers running with an SNMP Manager on each one and have all Agents in that part of the network configured to report to the local Manager. This would help localize network traffic.

7. Click [OK].

Add Agents

If OnGuard receives an event from an Agent that has not been defined, it will automatically add an Agent for it and have the default name set to the IP address of the Agent. You can then go in and modify the **Name** to whatever you want. On a segmented system, Agents are added to the Manager's segment by default, but they can also be assigned to different segments as well.

To add an Agent manually:

1. In System Administration, select ***SNMP Managers*** from the ***Additional Hardware*** menu. The SNMP Managers folder opens.
2. Click the SNMP Agents tab.
3. Click [Add].
4. In the **Name** field, type a name for the SNMP Agent.
5. In the **IP address** field, enter the IP address of the SNMP Agent.
6. (Optional) In the **Location** field, enter the location of the SNMP Agent.
7. (Optional) In the **Description** field, enter a description of the SNMP Agent.
8. Click [OK].
9. Repeat steps 1-8 for all Agents you wish to add.

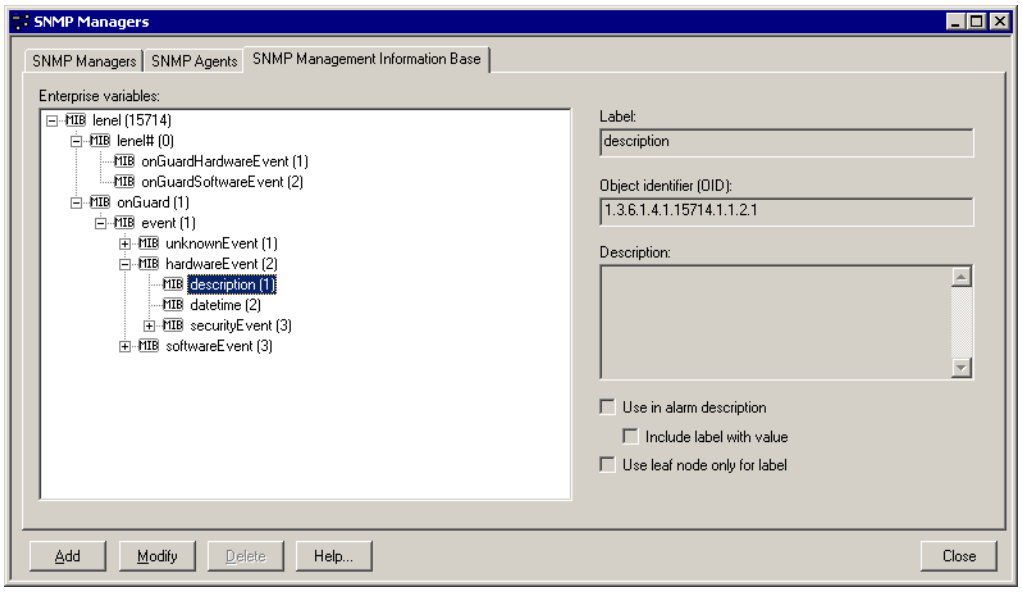
MIB File Overview

SNMP reports its information through the use of variables with name/value combinations. Many of the SNMP variables are designed for network applications or hardware. MIB (Management Information Base) files describe an enterprise's variable structure and allow a user to report hardware-specific information. Inside a MIB file, an enterprise number is specified. Nearly every company that has an application (hardware or software) that reports events has an enterprise number. (Lenel's is 15714). This allows them to control and define all variables under this number.

The enterprise number is used as part of the Object Identifier (OID). A company's enterprise OID is 1.3.6.1.4.1 followed by their enterprise number (1.3.6.1.4.1.15714 for Lenel). MIB files allow labels to be applied to the numbers in an OID. Using the standard MIB files for SNMP, the enterprise OID would be iso.org.dod.internet.private.enterprises followed by the label for the company's enterprise number provided by their MIB file. In this MIB file, you define all other variables that you will be using. These variables are identified by OIDs. The SNMP Trap Messages DataConduIT Message Queue type allows OnGuard to report events through SNMP trap messages. OnGuard uses the **lenel.mib** file to specify the variables to use. For example, one variable in the **lenel.mib** file is 1.3.6.1.4.1.15714.1.1.2.1, which translates to:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).lenel(15714).onGuard (1).event(1).hardwareEvent(2).description(1)

If the **lenel.mib** file is loaded, the variable in the previous example is shown on the SNMP Management Information Base form.



Load the MIB File(s)

The Management Information Base (MIB) file is used to describe an enterprise's variable structure. The Lenel MIB file is located in the **SNMP** folder on the OnGuard Supplemental Materials disc. To load a MIB file into the OnGuard software:

1. Save the MIB file you wish to load to the computer. Remember the location where you save it.
2. If necessary, save any files that contain modules required by the MIB files in the **SNMP-IMPORT-MIBS** folder in the OnGuard installation directory. By default, this is **C:\Program Files\OnGuard\SNMP-IMPORT-MIBS**. The following eight (8) files are installed to that location by default:
   - RFC1155-SMI.txt
   - RFC1213-MIB.txt
   - RFC-1215.txt
   - SNMPv2-CONF.txt
   - SNMPv2-MIB.txt
   - SNMPv2-SMI.txt
   - SNMPv2-TC.txt
   - SNMPv2-TM.txt

Notes: This location can be changed in the **ACS.INI** file by adding the following setting:

[SNMPManager]

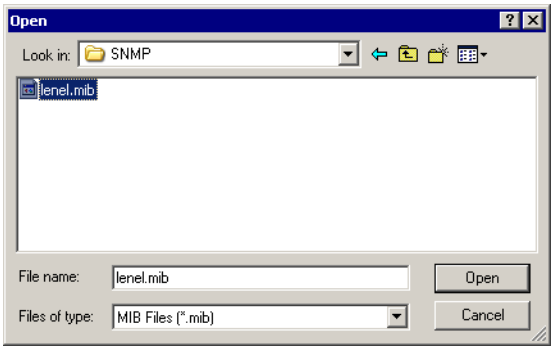
MIBDir="drive:\absolute\path\to\MIB\directory"

To make changes in the **ACS.INI** file on a Windows 7, Windows 8, or Windows 8.1 computer, you must right-click on the **ACS.INI** file and run it as an Administrator.

This directory is processed when a MIB file is loaded in order to load modules that may be imported into the MIB file being loaded. Only files containing imported modules should be saved in this directory. In most cases, the default files in this directory are sufficient. If additional files are required, determine which additional files define the modules imported by the MIB file and place them in this directory.

If a MIB file for an imported module is not present in this directory and the processor encounters an undefined identifier in the MIB file it's parsing, it will log an error to **MIBProcessor.log** in the C:\ProgramData\Lnl\logs directory.

3. In System Administration, select ***SNMP Managers*** from the ***Additional Hardware*** menu. The SNMP Managers folder opens.
4. Click the SNMP Management Information Base tab.
5. Click [Add].
6. The Open window is displayed. Navigate to the MIB file you wish to load, and then click [Open]. In this example, the **lenel.mib** file is being loaded.



7. The MIB file will be processed.
   - If the MIB file is successfully parsed, the results will be displayed in the Enterprise variables listing window. You can expand the items in the tree and look at the defined variables.
   - If the MIB file cannot be parsed, an error will be generated, which is written to the **MIBProcessor.log** file. An error is most likely due to a malformed MIB file or a lack of certain MIB files that are imported by the MIB file you are trying to parse.

Note: After a MIB file has been loaded into OnGuard, the actual file is no longer needed.

Modify an SNMP Management Information Base Variable

1. In System Administration, select ***SNMP Managers*** from the ***Additional Hardware*** menu. The SNMP Managers folder opens.
2. Click the SNMP Management Information Base tab.
3. Expand the items in the Enterprise variables listing window.
4. Click on the variable you wish to modify, then click [Modify].
5. Change the **Label** if you wish.
6. Enter a **Description** for the variable if you wish.
7. Select the **Use in alarm description** check box if the node's information will be used in the alarm description column of Alarm Monitoring. You can have this option set on multiple nodes and for each one that appears in the trap message as a variable, it will be included in the alarm description. The variable name will be discarded.
8. Select the **Include label with value** check box if you selected the **Use in alarm description** check box and if you want to see the variable name with the value.
9. Select the **Use leaf node only** check box if you want the SNMP Manager to ignore anything "higher" than this node in the OID.
10. Click [OK].

SNMP Reports

Reports are run from System Administration or ID CredentialCenter. For more information, please refer to the Reports Folder chapter in the System Administration or ID CredentialCenter User Guide. There are two SNMP-related reports that can be run:

- SNMP Agents - lists all SNMP Agents sorted by segment and name
- SNMP Management Information Base Configuration - lists all MIB data grouped by enterprise

The SNMP Management Information Base Configuration report lists each node's label and OID (Object ID) description. If configured, the following additional options will also be listed:

- Use in alarm description
- Include label with value
- Use leaf node only for label

Configuring OnGuard as an SNMP Agent

Prerequisites:

1. Install the Windows SNMP components. You will need your Windows CD to complete this procedure. For more information, refer to Install the Windows SNMP Components on page 44.
2. Install a license with SNMP support.

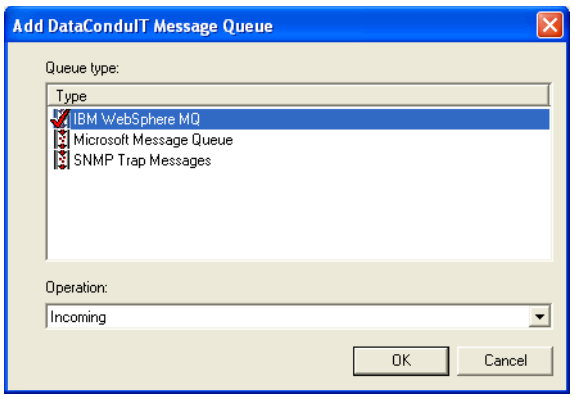
To configure OnGuard as an SNMP Agent:

1. Add a new DataConduIT Message Queue of the type "SNMP Trap Messages" in System Administration. For more information, refer to Add a DataConduIT Message Queue of Type "SNMP Trap Messages" on page 50.
2. Load the Lenel.MIB file. For more information, refer to Load the Lenel.MIB File on page 51.

Note: For more information, refer to the DataConduIT Message Queues Folder in the System Administration User Guide.

Add a DataConduIT Message Queue of Type "SNMP Trap Messages"

1. From the ***Administration*** menu, select ***DataConduIT Message Queues***.
2. On the DataConduIT Message Queues form, click [Add].
3. The Add DataConduIT Message Queue window opens.
   a. Select the "SNMP Trap Messages" **Queue type**.



b. Click [OK].

4. On the General sub-tab:
   a. In the **Queue name** field, type the name of the queue. The name is case-sensitive.
   b. In the **SNMP manager** field, type the name of the queue manager.
   c. Note that the Queue type and Operation that you selected are displayed, but cannot be modified.
5. On the Settings sub-tab:
   a. If you wish to have photo, signature, and fingerprint information sent in messages, select the **Include photos and signature in messages** check box.

Note: Including photo information in the messages makes the size of the message sent much larger.

   b. Select whether a message will be sent when cardholder, badge, visitor, and linked accounts are added, modified, or deleted.
   c. If you wish to have a message sent when an access event occurs, select the **Send a message when access events occur** check box.
   d. If you wish to have a message sent when a security event occurs, select the **Send a message when security events** occur check box.
6. Using the Advanced sub-tab is optional and for advanced users. On the Advanced sub-tab you may:
   a. Type an object event WMI query directly into the **Object event WMI query** textbox.
   b. Type an access and security event WMI query directly into the **Access and security event WMI query** textbox.
7. Click [OK].

Load the Lenel.MIB File

After configuring the SNMP Trap Messages queue, load the **lenel.mib** file into the SNMP Manager so that it knows how to handle and display the variables it receives. The Lenel MIB file is located in the **Support Center\SNMP** folder on the OnGuard Supplemental Materials disc.

If you are using OnGuard as an SNMP agent please refer to the documentation for the third-party SNMP Manager you are using to monitor the OnGuard software.

SNMP Manager Copyright Information

that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2002, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2002, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

CHAPTER 10

Integrating OnGuard with Citrix XenApp

IMPORTANT: To use OnGuard over the Internet, you must have purchased the optional Citrix® XenApp application.

Citrix XenApp Overview

Citrix XenApp provides support in conjunction with Windows Terminal Server for complete access to configure and operate your OnGuard system through a simple Web browser interface.

OnGuard allows for the installation of web server software and, once the server is configured, unlimited clients (based on licensing connections) can attach to the server and run any of the OnGuard applications over the Internet. Virtually any desktop operating system that supports a Web browser can run OnGuard over the Internet. This includes Windows, Macintosh, Unix, Solaris and Linux.

Notes: By default, License Administration loads configuration data from ***C:\Windows\acs.ini***, and Configuration Editor saves changes to this file in this location. When using OnGuard in a Citrix environment, License Administration creates a second acs.ini file in ***C:\Users\<USERNAME>\Windows***. However, Configuration Editor continues to update the acs.ini file located in ***C:\Windows***. If changes are made to the acs.ini file in ***C:\Windows***, License Administration will not load these changes because it loads from the acs.ini file in ***C:\Users\<USERNAME>\Windows***. If changes to the acs.ini file are related to the License Server (for example the license server machine), make sure the changes are made to the acs.ini files in both locations.

Installing Citrix XenApp 7.8 on Windows Server 2012 R2

The basic procedure for installing Citrix XenApp 7.8 on a Windows Server 2012 R2 is:

1. Perform the pre-installation procedures. For more information, refer to Step 1: Perform the Pre-Installation Set-up Procedures on page 56.

2. Install Citrix XenApp. For more information, refer to Step 2: Install Citrix XenApp on the Server on page 56.
3. Configure the License Server. For more information, refer to Step 3: Configure the License Server on page 57.
4. Create a site. For more information, refer to Step 4: Create a Site on page 57.
5. Create the master image. For more information, refer to Step 5: Create the Master Image on page 58.
6. Publish an application. For more information, refer to Step 6: Publish an Application on page 58.
7. Access the applications from the Citrix Receiver Web. For more information, refer to Step 7: Access the Applications from the Citrix Receiver Web on page 59.

Step 1: Perform the Pre-Installation Set-up Procedures

Note: Confirm that the operating system has the latest updates.

1. Add the operating system in domain.
2. Use a clean installation of Microsoft SQL Server as your starting point.
3. Start the Server Manager.

   For more information, refer to “Using OnGuard in the Supported Operating Systems” in the Installation Guide.
4. From the Server Manager, add the following roles and features:
   - IIS:
     - **Web Server > Health and Diagnostics > Logging Tools**
     - **Web Server > Health and Diagnostics > Tracing**
     - **Management Tools > IIS 6 Management Compatibility > select all sub items**
   - Application Server:
     - Keep the features that are selected by default
   - Remote Desktop Services:
     - Remote Desktop Session Host
     - Remote Desktop Licensing
     - Remote Desktop Web Access
5. In the Server Manager:
   a. Click [Configure this local server].
   b. In the Properties section, click **On for IE Enhanced Security Configuration**.
   c. For both Administrators and User, select **Off**.
   d. Click [OK].

Step 2: Install Citrix XenApp on the Server

Notes: When installing Citrix XenApp, you may need an ISO mounting application.

Ensure that your license for Remote Desktop services is current.

Ensure that your license for Citrix XenApp is current. When you obtain this license, ensure that the server name is exactly as specified. The server name is case-sensitive.

1. Run the Citrix installer.

2. On the Citrix menu screen, click [Start] next to **XenApp Deliver applications**.
3. On the XenApp screen, click the **Delivery Controller** link below the **Get Started** heading.
4. On the License Agreement screen, accept the license and then click [Next].
5. On the Core Components screen, keep the default settings as they are and click [Next].
6. On the Features screen, keep the default settings as they are and click [Next].
7. On the Firewall screen, keep the default settings as they are and click [Next].
8. On the Summary screen, click [Install]. When the installation is complete, click [Finish].

Step 3: Configure the License Server

1. Use the web browser to open the Citrix License Administration Console.

   For more information, refer to “Using OnGuard in the Supported Operating Systems” in the Installation Guide.
2. On the top-right area of the window, click [Administration].
3. Log in with the domain user name and password, and then click [Submit].
4. In the left tab, click [Vendor Daemon Configuration].
5. Click [Import License], select the Citrix License File, and then click [Import License].

   When the import is complete, a success message appears. Click [OK].
6. Restart the Citrix license:
   a. Open the Citrix Licensing Service.

      For more information, refer to “Using OnGuard in the Supported Operating Systems” in the Installation Guide.
   b. Right-click **Citrix Licensing** and then click [Restart].
7. Go back to the Citrix License Administration Console. In the top-right area of the console, next to **Administration**, click [Dashboard].

   If everything is correct, you will see your Citrix license along with a Citrix startup license. It should look similar to this:

   – Citrix Start-up License | Server
   – Citrix XenApp Advanced | Concurrent
   – Citrix XenApp Enterprise | Concurrent
   – Citrix XenApp Platinum | Concurrent

Step 4: Create a Site

1. Launch the Citrix Studio.
2. On the Welcome screen, select **Deliver application and desktops to your users**.
3. On the Introduction screen, select **A fully configured, product-ready Site**, enter the **Site name**, and then click [Next].
4. On the Database screen:
   a. Enter the **Database server location**.
   b. Click [Next].
5. On the Licensing screen:
   a. Enter the license server address.
   b. Select the licenses that already exist. For example, **CitrixXenApp Enterprise**.

c. Click [Next].

6. On the Connection screen, select a **Connection type**.
   - If machine management is not used (such as when using physical hardware), select **No machine management**, click [Next], and then go to step 9.
7. If the Network screen appears:
   a. In the **Name for these resources** field, enter the desired name.
   b. Select the network to use.
   c. Click [Next].
8. If the Storage screen appears, select the storage device to use and click [Next].
9. On the Additional Features screen, uncheck the **App-V publishing** check box and click [Next].
10. On the Summary screen, click [Finish].

    The setup takes several minutes to complete.

Step 5: Create the Master Image

1. Launch the XenApp installation: **XenApp_and_XenDesktop7_8.iso**.
2. On the XenApp 7.8 screen, select **Prepare Machines and Images**.
3. On the Equipment screen, select **Create a Master image** and click [Next].
4. On the Core Components screen, click [Next].
5. On the Delivery Controller screen:
   a. Select the **Do it manually** option.
   b. Enter the controller address.
   c. Click [Test connection] and ensure that there are no errors.

      If an error occurs, resolve the error and retest the connection.
   d. Click [Add].
   e. Click [Next].
6. On the Features screen, select all of the features and click [Next].
7. On the Firewall screen, keep the default settings as they are and click [Next].
8. On the Summary screen, click [Install].
9. After the installation is completed, restart the server.

Step 6: Publish an Application

Note: Before installing OnGuard, try publishing Notepad or Calculator to confirm that publishing works correctly.

Create One Machine Catalogs

1. In the Citrix Studio, expand the system tree.
2. Select the **Machine Catalogs** node, then click the **Create Machine Catalog** link on the right-top window. The Machine Catalog Setup wizard opens.
3. On the Introduction screen, click [Next].
4. On the Operating System screen, select **Server OS** and click [Next].
5. On the Machine Management screen:
   a. Select the **Machines that are not power managed** radio button.

   b. Select the **Another service or technology** radio button.
   c. Click [Next].
6. On the Machines screen, click [Add computers] to add local to the list and then click [Next].
7. On the Summary screen, enter the **Machine Catalog name** and click [Finish].

Create Delivery Groups

1. In the Citrix Studio, expand the system tree (if not already expanded).
2. Select the **Delivery Groups** node, then click the **Create Delivery Group** link on the right-top window. The Create Delivery Group wizard opens.
3. On the Introduction screen, click [Next].
4. On the Machines screen:
   a. Select the desired Machine Catalog.
   b. In the **Choose the number of machines for this Delivery Group** field, enter the appropriate value.
   c. Click [Next].
5. On the Users screen:
   a. Click [Allow any authenticated users to use this Delivery Group].
   b. Click [Next].
6. On the Applications screen:
   a. Click [Add].
   b. From the Add options, select **From start menu...**
   c. In the Add Applications from Start Menu screen, select the desired OnGuard application.
   d. Click [OK].
   e. Click [Next].

Note: The applications in the operating system are automatically displayed on this screen. If you already installed OnGuard, the OnGuard applications are automatically displayed. If the application under test is not displayed, add the application by clicking [Add] and then selecting **Manually...**

7. On the Summary screen, enter the **Deliver Group name** and click [Finish].

Step 7: Access the Applications from the Citrix Receiver Web

1. On the CitrixStoreFront, expand the system tree and select the **Receiver for Web** node.
2. Open Internet Explorer and enter the URL displayed in the **Store Web Receiver** section.
3. Log in as the domain user and domain user password and view the published applications.

Reference

CHAPTER 11

Ports Used by OnGuard

IMPORTANT: To make changes in the **ACS.INI** file on a Windows 7, Windows 8, or Windows 8.1 computer, you must right-click on the **ACS.INI** file and run it as an Administrator.

Note: Most of the following ports use the Transport Control Protocol (TCP). Ports 45303, 45307, and 46308 use the User Datagram Protocol (UDP). Port 9111 uses the Hypertext Transfer Protocol (HTTP) protocol.

Port	Function	From (Client)	To (Server)	OnGuard version	Notes/Where port can be changed
80	Web Server (IIS)	Web browser	OnGuard server	Only used with OnGuard 5.12 and later	Used for Web Applications to communicate with the Web Service. Check IIS configuration for the correct port configuration.[4]
135	DCOM Initial Connections	Any DCOM application	Lenel NVR; OnGuard	All OnGuard Versions	Cannot be changed.
443	Web Server (IIS) SSL	Web browser	OnGuard server	Only used with OnGuard 5.12 and later	Used when SSL is utilized for the Web Applications. Port 443 is used for secure web browser communication.[4]
1433	Default port for SQL Server	All client applications and services	Database server		Check SQL Server configuration/ documentation; this can be changed in SQL configuration.
1521	Default port for Oracle	All client applications and services	Database server		Check Oracle configuration/ documentation; this can be changed in Oracle configuration.

Port	Function	From (Client)	To (Server)	OnGuard version	Notes/Where port can be changed
3001	Connected controllers	Communication Server	Connected controllers	OnGuard 5.0 and later	The default port the Communications Server uses to communicate with controllers. Configurable within System Administration.
4001	Communication Server RPC	System Administration; Alarm Monitoring; Area Access Manager; Data Conduit; Data Exchange; Replicator; Config Download Service; Linkage Server	Communication Server	All OnGuard versions	Can be changed in **ACS.INI** [Service] section DriverRpcPort[1]
4002	Global Output Server RPC	Linkage Server	Global Output Server	OnGuard 5.0 and later	Can be changed in **ACS.INI** [Service] section GosRpcPort[1]
4003	Login Driver RPC	Applications and services that login to the OnGuard database	Login driver	OnGuard 5.0 and later	Can be changed in **ACS.INI** [Service] section LoginRpcPort[1]
4004	Communication Server Socket (event reporting)	Alarm Monitoring; Linkage Server	Comm Server	All OnGuard versions	Can be changed in **ACS.INI** [Service] section DriverSocketPort[1]
4005	Linkage Server RPC	System Administration	Linkage Server	OnGuard 5.7 and later	Can be changed in **ACS.INI** [Service] section LinkageServerRpcPort[1]
4006	Video Server RPC	System Administration; Linkage Server	Archive Server	OnGuard 5.7 and later	Can be changed in **ACS.INI** [Service] section VideoServerRpcPort[1]
4009 - 4057	Alarm Monitoring RPC	Communication Server	Alarm Monitoring	OnGuard 5.9 and later	Used for the Guard Tour, Grant-Deny Popup and Failure to Acknowledge/ Forward Alarm features only. One port used per Monitoring instance on a given machine (typically 4009). Can be changed in **ACS.INI** [Service] section AcsmntrRpcMinPort, AcsmntrRpcMaxPort[2,3]

Port	Function	From (Client)	To (Server)	OnGuard version	Notes/Where port can be changed
4059	Replicator	Replicator Administration; LS Replicator Service	Replicator Service	OnGuard 5.9 and later	Can be changed in **ACS.INI** [Service] section ReplicatorSocketPort[1]
4060	Replicator	Replicator Administration; LS Replicator Service	Replicator Service	OnGuard 5.9 and later	Can be changed in **ACS.INI** [Service] section ReplicatorRpcPort[1]
4061	DataExchange	Linkage Server	Data Exchange	OnGuard 5.9 and later	Can be changed in **ACS.INI** [Service] section DESocketPort[1]
4062	DataExchange	Linkage Server	Data Exchange	OnGuard 5.9 and later	Can be changed in **ACS.INI** [Service] section DERpcPort[1]
4065	Replicator	Replicator	ID Allocation Service	OnGuard 6.3 and later	Port used by Replicator and/or Replication Administration to communicate with the ID Allocation Service to allocate additional IDs for pre-allocated objects
4070	HID Edge device communication	Communication Server	HID Edge devices	OnGuard 6.1 and later	Used for bi-directional communication between OnGuard Communication Server and HID Edge devices. Can be changed in the **ACS.INI** file under the [HID VertX] section Listening Port[1]
5671	Used by the LS Message Broker service to transfer incremental credential data, deliver message delivery, for data queuing, and event logging.	OnGuard server	OnGuard server	OnGuard 7.0 and later[5]	Can be changed via the Security Utility. See the Security Utility release notes for more information. When the Security Utility opens, click [More Info] in the disclaimer to view the release notes. This is for SSL traffic.

Port	Function	From (Client)	To (Server)	OnGuard version	Notes/Where port can be changed
5672	Used by the LS Message Broker service to transfer incremental credential data, deliver message delivery, for data queuing, and event logging.	OnGuard server	OnGuard server	OnGuard 7.0 and later[5]	Can be changed via the Security Utility. See the Security Utility release notes for more information. When the Security Utility opens, click [More Info] in the disclaimer to view the release notes. This is for non-secure communication. Either Port 5671 or 5672 may be used. 5671 is the default port.
7007	Communications with SkyPoint Base Server	Communication	Communication	OnGuard 7.0 and later	Used for communication between SkyPoint Base Server and the OnGuard software.
7008	SkyPoint Base Server	Communication	Communication	OnGuard 7.0 and later	Used for communication between SkyPoint Base Server and the OnGuard software.
7654	LS Client Update Server service	Client Update service	Client Update server	OnGuard 7.0 and later	Can be changed in System Administration > Administration > System Options, on the Client Update form.
8032	Used by the LS Site Publication Server (Enterprise or Replicator). This is for binary transaction transfer.	Site Publication server	Site Publication server	OnGuard 7.0 and later	Can be changed via the Security Utility. See the Security Utility release notes for more information. When the Security Utility opens, click [More Info] in the disclaimer to view the release notes.
8048	Used by the OpenAccess REST Proxy	OnGuard server	OnGuard server	OnGuard 7.1 and later	Used for communication between the NGINX web server and OpenAccess REST Proxy.
8049	LS Web Event Bridge service	OnGuard server	Event subscriber	OnGuard 7.2 and later	Used for receiving events using WebSocket through the LS OpenAccess and LS Event Context Provider services.

Port	Function	From (Client)	To (Server)	OnGuard version	Notes/Where port can be changed
8080	Used by the Web Server (NGINX) for OpenAccess	All client applications	OnGuard server	OnGuard 7.1 and later	Can be changed via the Security Utility. See the Security Utility release notes for more information. When the Security Utility opens, click [More Info] in the disclaimer to view the release notes.
	Port for NetDVMS connections	OnGuard	NetDVMS	OnGuard 6.4.500 and later	If port is set to 0 on the NetDVMS form this indicates the default port 8080 will be used. **Note:** NetDVMS-connected devices cannot be hosted on same server as OpenAccess.
8189	License Server	All client applications	License Server	OnGuard 5.7 and later	To change the License Server port: 1. Use the Configuration Editor to change the port number. Refer to the *Configuration Editor* appendix in the *Installation Guide*. 2. The following must be added to the **LicenseServerConfig\Server.properties** file (file content is case-sensitive!): Port=8189 where '8189' is replaced by the desired port number. (This line is not present by default. The whole file is not present by default; it is created when the admin username or password is changed.)
8888	Software License	License Server at customer site	Lenel's public License Admin site	OnGuard 6.1 and later	Port used for online activation and deactivation of software based licensing. This port must be open to activate a software-based (FLEXnet) license.

Port	Function	From (Client)	To (Server)	OnGuard version	Notes/Where port can be changed
9111	Application Server (as a Windows Service)	Web hosted applications	Application Server	OnGuard 5.12 and later	Used for communication with the Application Server service. Lnl.OG.ApplicationServer.Service.exe.config contains the Application Server port configuration. The Web Service web.confg file indicates to the Web Service how to connect to the Application Server (including which port). Uses the HTTP protocol.

Port	Function	From (Client)	To (Server)	OnGuard version	Notes/Where port can be changed
9999	License Administration	Web browser	License Server	OnGuard 5.7 and later	To change the License Administration port, the following must be added to the **LicenseServerConfig\Server.properties** file (file content is case sensitive!): AdminPort=9999 where '9999' is replaced by the desired port number. (This line is not present by default. The whole file is not present by default; it is created when the admin username or password is changed.) **Note:** The License Administration shortcut installed by OnGuard can't be used if the License Administration port has been changed. To access the License Administration after the port has been changed, simply point the browser to http://licenseserver:9999 (where 'licenseserver' is the name of the machine running Licenser Server and '9999' is the port number for License Administration).
10001	Galaxy Ethernet Module	Comm Server	Galaxy panels	OnGuard 5.11 and later	Cannot be changed.
45303	Elevator Terminal Online Status Port	Comm Server	Otis elevator dispatching system	OnGuard 5.12 and later	**ACS.INI** [Otis] section SSOnlineStatusPort. If changed, must be done on workstation running Communication Server. Uses UDP.

Port	Function	From (Client)	To (Server)	OnGuard version	Notes/Where port can be changed
45307	Elevator Dispatching Heartbeat Port	Otis elevator dispatching system	Comm Server	OnGuard 5.12 and later	**ACS.INI** [Otis] section SSHeartbeatPort. If changed, must be done on workstation running Communication Server. Uses UDP.
46308	Elevator Terminal Command Port	Comm Server	Otis elevator dispatching system	OnGuard 5.12 and later	**ACS.INI** [Otis] section SSDECCommandPort. If changed, must be done on workstation running Communication Server. Uses UDP.

[1] To change these ports, the **ACS.INI** settings must be changed on all machines (server and clients).

[2] To change these ports for a given monitoring station, the **ACS.INI** settings only need to be changed on that machine.

[3] Each port in this range is used for the same purpose, and most of these ports are usually unused. This port range is reserved so that multiple instances of Alarm Monitoring can run on one PC in a terminal services environment. Because each instance of Alarm Monitoring running on one PC requires a unique port, the next available port in this range is used.

[4] These ports are used by the LNL-2220 and LNL-3300 when connected to the network.

[5] With OnGuard 7.3 and later, these ports used by the LS Message Broker can be manually configured. For more information, refer to **Message Broker Service host** in the *System Administration User Guide*.

Digital Video Ports

Access to live and recorded digital video is done through a combination of DCOM and network socket connections.

Abbreviations:

- Lenel NVR - Lenel Network Video Recorder
- IVS - IntelligentVideo Server
- IVAS - IntelligentVideo Application Server
- LSVS - Lenel Streaming Video Server
- RM - Remote Monitor
- VV(web) - VideoViewer browser-based client

Port	Function	From (Client)	To (Server)	Protocol
<User>[a]	Live video	Lenel NVR, RM	OnGuard, IVS, VV(web)	UDP/IP or multicast[b]

Port	Function	From (Client)	To (Server)	Protocol
<User>[c]	Live video	OnGuard, IVS, VV(web), RM	Lenel NVR	TCP/IP
DCOM	Setting configuration, querying status, playback control, and recorded video	OnGuard, IVS, VV(web), RM	Lenel NVR	DCOM
DCOM	Setting configuration, querying status	OnGuard	IVS, IVAS	DCOM
<User>[d]	Video processing metadata stream	OnGuard, IVAS	IVS	TCP/IP
DCOM	Video processing event subscription	IVAS	IVS	DCOM
<User>[e]	Streamed RTP live video	LSVS	Any RTP client	UDP/IP or multicast
DCOM	LSVS configuration[f]	LSVS config tool	LSVS	DCOM
6000[g]	Control commands	OnGuard	RM	UDP/IP
6001-7000[h]	Control command response notifications	RM	OnGuard	UDP/IP
80[i]	Live video retrieval and camera control	Lenel NVR	IP Cameras	TCP/IP
21 and ####[j]	In-Camera Storage retrieval	Lenel NVR	IP Cameras	TCP/IP

a. If live video is transmitted in UDP/IP mode, the OnGuard client determines which port should be used. The range of ports can be limited by launching LnrNI utility on the OnGuard client machine and specifying the port range to use under the **Use UDP/IP** check box. If live video is transmitted in multicast mode, the Lenel NVR will choose which port should be used by each channel. The range of ports can be specified by launching the LnrNI utility on the Lenel NVR machine, selecting the "Recorder Network Settings" tab and entering the first multicast port. The actual port number for each channel is defined by adding the first multicast port and the channel number. For example, if the first multicast port is 2000, then channel 1 will use port 2001, channel 2 will be 2002, etc.

b. When Lenel NVR starts for the first time, it will randomly choose a multicast address for use with live video and stores this address in the **LNR.XML** file. If a different address is desired, this value can be changed by editing the LNR/Recorder/Settings/MulticastIP element in the **LNR.XML** file.

This multicast address becomes the base number and similarly to the multicast port actual address for a channel is determined by adding the channel number to this base value. It is important to remember that if multicast video is used in the system, all channels on all Lenel NVRs should be assigned unique multicast port and address values.

c. This port number can be specified by launching the LnrNI utility on the Lenel NVR machine, selecting the "Recorder Network Settings" tab and entering a value for **Recorder TCP/IP Port**.

d. This port number can be specified by launching the LnrNI utility on the Lenel NVR machine, selecting the "IVS Network Settings page and entering a value for **IntelligentVideo Server TCP/IP Port**.

e. The port and multicast address for each channel is chosen by the user through the configuration utility when channels are added to the LSVS.

f. This setting is only required if the user wishes to configure the LSVS from a remote machine. This step is not necessary if the configuration application is launched from the host where the streaming server is installed.

g. This port number must be the same on all remote monitoring and OnGuard client machines in the system. If the user wishes to use a different value, all machines must be updated at the same time. On the OnGuard client, this can be changed by editing the "MonitorUDPPort" registry value under HKEY_LOCAL_MACHINE\Software\Lenel\OnGuard. On RM machines, the same value must be updated in the registry under HKEY_LOCAL_MACHINE\Software\Lenel\RemoteMonitor.

h. This port range can be changed by launching the LnrNI utility on the OnGuard client machine, selecting the "Remote Monitor Network Settings" tab and entering a different port range.

i. Cameras have built-in web servers. Typically they use HTTP port 80, but the user can configure it to use any arbitrary port number. The camera tab in the digital video folder in System Administration allows you to specify which port Lenel NVR will connect to. For more information, refer to the Digital Video Folder chapter in the System Administration User Guide for more information.

j. Currently this is only supported for Sony cameras. FTP protocol is used to retrieve video from In-Camera Storage. By default this protocol uses TCP port 21 to establish the connection. This port can be changed in the camera configuration. FTP protocol also uses a separate TCP/IP connection for actual data transfer and this connection can be established on just about any port. Therefore, using In-Camera Storage through firewalls might cause problems.

DCOM uses TCP port 135 to establish new connections. TCP port 135 must be open on the server. Once a client connects to that port, the Windows DCOM/RPC subsystem determines the type of the actual communications. This type can be either TCP/IP or UDP/IP based on the machine settings. These settings can be changed with the following steps:

1. Run `dcomcnfg` from the command line.
2. Expand to ***Console Root*** > ***Component Services*** > ***Computers*** > ***My Computer***.
3. Right-click on My Computer and select Properties.
4. Select the Default Protocols tab.
5. Select UDP/IP or TCP/IP or both. For each option, the port range can also be limited. If the port range is not limited, DCOM will use any random port between 1024 and 65000. It is recommended to limit the port range for systems using firewalls.

For additional information about DCOM, refer to the Microsoft Windows documentation.

The LnrNI utility is used to configure the ports that should be used for each type of communication. When launched on a client, the LnrNI utility defines the mode that will be used to receive live video from the Lenel NVR. It attempts each type of connection in the order they are listed on the Client Network Settings tab. If the connection is unsuccessful after 3 seconds it will move to the next connection type until all three have been tried: multicast, UDP/IP, and TCP/IP. TCP/IP is the fallback mechanism and cannot be disabled.

The LnrNI utility also determines which network card should be used by the video software if the machine is multihomed, meaning it has different IP addresses due to multiple active network adapters.

CHAPTER 12

OnGuard Services

The following is a table of OnGuard services and those services that run on OnGuard installations.

Note: Configure these services to start automatically if you require the function provided by the service, and if the service does not default to starting automatically.

OnGuard Services

Name	Definition	Number per OnGuard system	Notes
Application Server	Used to provide the application server for the web based applications.	One per server.	Only installed when a custom installation is performed and the Application Server component is selected.
Client Update Server	The Client Update Server is used to automatically update client workstations.	One per server.	Only client workstations are upgraded automatically. Server workstations still require manual updates. By default, this functionality is disabled unless it applies to new releases, service packs, and incremental updates where the OnGuard version number has changed.
Client Update Service	Communicates with the Client Update Server, when client updates are required.	One per client.	Refer to Notes for Client Update Server.

OnGuard Services (Continued)

Name	Definition	Number per OnGuard system	Notes
Communication Server	The OnGuard Communication Server acts as the communication “gateway” for information flow between the OnGuard software and hardware.	You can have multiple communication servers.	Many communication services may be running throughout a region. One communication server can communicate to many field hardware devices, but a hardware device can only communicate to one communication server. It is typically configured to run automatically on the regional server though any regional client can run the communication server.
Config Download Service	The Config Download service is used to propagate configuration changes down to the hardware from the web based applications.	One per server. Must be run on the same machine as the Application Server.	Needed only for the Area Access Manager (Browser-based Client) application.
DataConduIT Message Queue Server	The DataConduIT Message Queue Server is an adapter that works with the DataConduIT Service. It provides an easy way to use/ delegate DataConduIT notifications using queues.	One per server.	Typically installed on the database server.
DataConduIT Service	The DataConduIT Service is a platform for integrating with IT systems, providing access to ID management data, access control events, and real-time notification when changes are made to cardholders and their credentials.	One per server.	DataConduIT must be installed on the same machine as the Linkage Server if you want to receive events through DataConduIT.

OnGuard Services (Continued)

Name	Definition	Number per OnGuard system	Notes
DataExchange Server	The DataExchange Server is used to exchange database information with third party applications.	One per server.	Only one DataExchange server may be running on each regional database and/or master database. It only needs to be running when scheduling to run a DataExchange script.
Device Discovery Service	The Device Discovery Service is used as a proxy service for running remotely (systems in other subnets) all services that the Device Discovery Console cannot otherwise access.	One per server.	You must perform a custom installation and select “Device Discovery Service” in the Standard Applications section.
Event Context Provider	The Communication Server publishes events that are picked up by the Event Context Provider service, which provides additional event details.	One per server.	Events are provided to any event subscriber listening for those events.
Global Output Server	The OnGuard Global Output Server (GOS) is used to send output to any supported output system (including electronic mail and paging) connected to the computer on which the GOS is installed. For e-mail, the GOS communicates to the SMTP Server and for paging it outputs the file to a specified location.	As many as needed.	As many instance of Global Output Server (GOS) can be running on each regional and/or master database.

OnGuard Services (Continued)

Name	Definition	Number per OnGuard system	Notes
ID Allocation	Used to manage pre-allocated IDs across an enterprise installation.	One. Must be run only on the Enterprise Master or Distributed ID Master.	
License Server	The License server controls which features the computer is licensed to use.	One per server.	The OnGuard License Server is typically run on OnGuard servers but can be configured on a separate machine.
Linkage Server	The Linkage Server is responsible for the central processing of various tasks within the Access Control system.	One per server.	Typically runs on the database server.
Login Driver	The login driver allows OnGuard to log in and access the database.	One per server.	The Login Driver service manages the database password (not user passwords) for clients.
LnrCapSvc	Records video from CCTV devices.	One per Lenel NVR.	Must be running in order for the Lenel NVR to connect to video sources and to store information to the disk. It also services live video retrieval requests.
LnrRetrSvc	Retrieves recorded video requested by client.	One per Lenel Lenel NVR.	Manages stored video and stored video retrieval requests. If your storage fills up this service finds which files should be deleted so the capture service has space for new video.
LnrRTPServer	Streams video to RTP clients.	One per Lenel NVR.	This services is a translation layer between the proprietary Lenel NVR video retrieval interfaces and the standard way of transmitting streaming media data.
LpsIVAppServer	Performs processing for IntelligentVideo Applications.	One per IVAS.	This is a host service for all IntelligentVideo applications where each application is implemented as a dynamically linked library module. Currently the only application supported is Facility Utilization.

OnGuard Services (Continued)

Name	Definition	Number per OnGuard system	Notes
LpsIVSAdminSvc	Manages configuration of video analytics events.	One per IVAS.	Must be running in order for the IntelligentVideo Server to work. Runs on the IVS.
LpsRetrSvc	Retrieves metadata associated with video analytics events.	One per IVS.	Services stored processed video metadata retrieval requests. This is used by clients when they are viewing recorded video and want to see overlay images generated by video processing algorithms.
LpsSearchSvc	Performs video analytics processing.	One per IVS + one per OnGuard client + one per Lenel NVR.	Must be installed in order to perform any video searches. Should be run on all machines, servers and clients, that will need to perform video searches.
Message Broker	Provides message delivery and queuing services.	One per Enterprise Master Server, Distributed ID Master Server, Enterprise Regional Server, or Mobile Station.	Requires that Secure Socket Layer (SSL) is running on all Enterprise workstations.
OpenAccess	A platform for integrating with IT systems, providing access to ID management data, logged events, and hardware configuration information. Allows the creation of a client against a REST API to OnGuard through NGINX as the web service that abstracts the AMQP language.	One per server.	Typically installed on the OnGuard server.
PTZ Tour Server	PTZ Tour Server.	One per OnGuard client + one on the OnGuard server.	

OnGuard Services (Continued)

Name	Definition	Number per OnGuard system	Notes
Replicator	Used to distribute and synchronize hardware transactions across all systems in an Enterprise or Distributed ID configuration.	One per Enterprise Region or Mobile Station.	Can be run as a program (Manual start up type) or Automatic. If using as an automatic startup type, you will use OnGuard scheduler when replicating. If manual, you will replicate whenever convenient (This is typical for those using Mobile ID.)
Site Publication Server	This service is used to distribute and synchronize incremental credential data across all systems in an Enterprise or Distributed ID configuration.	One per Enterprise Master Server, Distributed ID Master Server, Enterprise Regional Server, or Mobile Station.	This service is responsible for synchronizing cardholder changes automatically, without a schedule, using the Message Bus. It should run on the same machine as the Replicator or ID Allocation service, and will only start on the specified machine.
Video Archive Server	The Video Archive Server is a system service that is responsible for purging or archiving video data from multiple video servers onto one or more designated storage devices.	Depending on the number of recorders and physical archive servers you have.	A digital video recorder device can only communicate to one Video Archive Server.
Web Event Bridge	Allows event subscribers to receive events using WebSocket.	One per server.	By default, the Web Event Bridge service is configured to locate the REST proxy, which is part of the OpenAccess service, on the same server. If you installed the Web Event Bridge service on a different server than the OpenAccess service, open the Lnl.OG.WebEventBridgeService.exe.config file and edit the proxy from **localhost** to the correct server name.
Web Service	The service hosting NGINX.	One per server	Typically installed on the OnGuard server.

Appendices

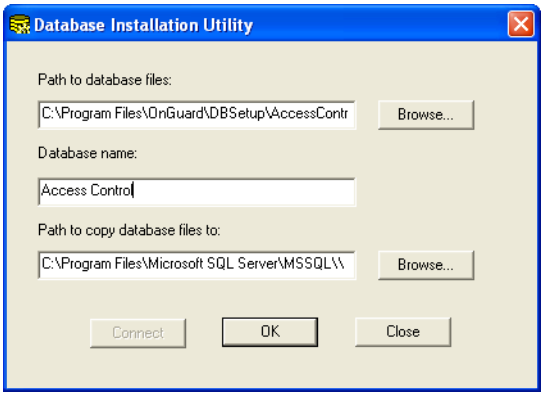
APPENDIX A

Database Installation Utility

The Database Installation Utility is used to attach an SQL Server Express/SQL Server database for use with the OnGuard software. The Database Installation Utility copies the existing database data files (MDF and LDF), attaches the database, and updates the Lenel Data Source Name (DSN) to point to the correct database. It does not create the tables in a new database - Database Setup must be run.

The Database Installation Utility is run automatically at the end of the OnGuard installation when either a new SQL Server Express database or a demo database has been selected. It is also installed on the local machine in the OnGuard installation directory so that it can be run manually after the installation has completed.

Database Installation Utility Window



Database Installation Utility Window Fields

Path to database files

The source data file (MDF) name. When the Database Installation Utility is run automatically during the OnGuard installation, the **Path to database files** and the **Database name** are determined based on the choice of the SQL Server Express or Demo database.

The default empty SQL Server Express database is **AccessControl_Data.mdf**. The OnGuard demo database is **AccessControlDemo_Data.mdf**.

Browse

Click to select the **Path to database files**.

Database name

The name of the database that will be used with the OnGuard software. When the Database Installation Utility is run automatically during the OnGuard installation, the **Database name** and the **Path to database files** are determined based on the choice of the SQL Server Express or Demo database.

Path to copy database files to

The destination directory. The destination directory will always default to the SQL Server Express/SQL Server default data directory, as configured in SQL Server Express/SQL Server and stored in the registry.

Browse

Click to select the **Path to copy database files to**.

Connect

When the Database Installation Utility opens, it attempts to connect to the database for the DSN that is currently specified in the Database section of the Configuration Editor. For more information, refer to the *Configuration Editor* appendix in the *Installation Guide*.

OK

Created or attaches the specified database.

Close

Closes the Database Installation Utility without performing any function.

Database Installation Utility Procedures

Attach an SQL Server Express Database

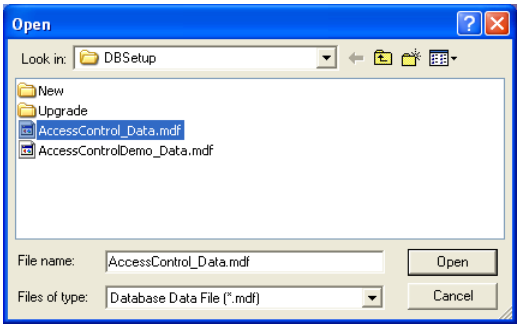
Run the Database Installation Utility by doing the following:

IMPORTANT: To make changes in the **ACS.INI** file on a Windows 7, Windows 8, or Windows 8.1 computer, you must right-click on the **ACS.INI** file and run it as an Administrator.

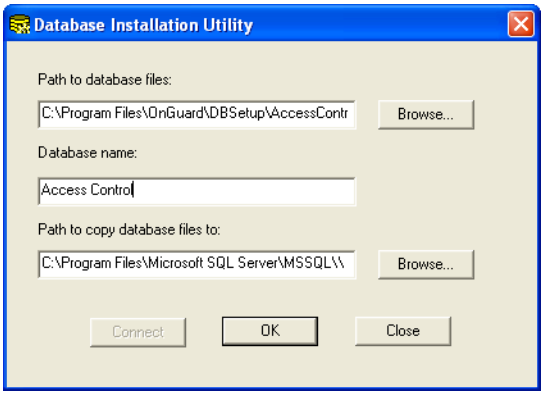
1. In Windows Explorer, navigate to the OnGuard installation directory (**C:\Program Files\OnGuard** by default), and then double-click on the **DatabaseInstallationUtility.exe** file to run it.
2. The Database Installation Utility window is displayed. When the Database Installation Utility opens, it attempts to connect to the database for the DSN that is currently specified in the Database section of the Configuration Editor.
   - If the database connection succeeds, the [Connect] button is grayed out. Proceed to step 3.
   - If the database connection fails, an error message that says, “The DSN selected in your ACS.INI is invalid. Please check your ODBC configuration.” is displayed and the [Connect] button is enabled. If this message is displayed, use the Configuration Editor application to

specify the correct DSN, and then click the [Connect] button. If the connection is successful, the [Connect] button becomes grayed out. Proceed to step 3.

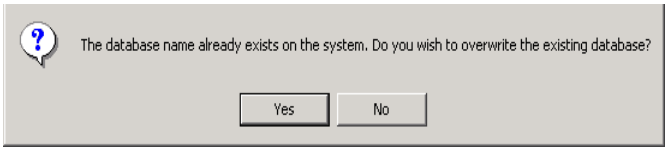
3. Click [Browse...] to choose the path to the database files.
4. The Open window is displayed. Navigate to the **DBSetup** folder in the OnGuard installation directory, select the MDF file that you wish to attach, and then click [Open]. MDF files you may wish to attach include:
   - The default empty SQL Server Express database **AccessControl_Data.mdf**.
   - The OnGuard demo database **AccessControlDemo_Data.mdf**.



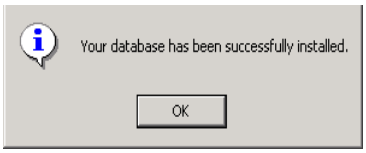
5. In the **Database name** field, type `AccessControl` or any other name you wish to use, as shown.



6. The recommended path is the default path specified in the **Path to copy database files to** field. This default path is where the files would be stored if you were using the SQL Server user interface (which does not come with SQL Server Express) to create a database.
   - If you do not change the default setting in the **Path to copy database files to** field and a database with the name you specified already exists, the database will be overwritten.
   - If you do change the default setting, a new database will be created in that location.
7. Click [OK].
8. If you did not change the default setting, the following message is displayed. Click [Yes].



9. The DSN is updated to point to the database, and a message is displayed that indicates that the database was successfully installed. Click [OK].



10. On the Database Installation Utility window, click [Close].

IMPORTANT: After attaching a database, you must run Database Setup to create the tables in the database.

APPENDIX B

Change the Database Owner in SQL Server Express

Since SQL Server Express doesn't provide an interface for accessing the database engine, use the following procedure to log into the database directly using the ODBC connection created for OnGuard:

1. Open the Run dialog.
   For more information, refer to "Using OnGuard in the Supported Operating Systems" in the Installation Guide.
   Click [Browse…]. Browse to the OnGuard folder and select the '**ACCESSDB.exe**' application. Click [Open] and then [OK] to run this application.
2. From the ***Management*** menu, select ***Datasource > Connect***.
   a. On the Machine DataSource tab, select "Lenel". Click [OK].
   b. You will be prompted for the database "sa" login ID and password. Enter the credentials and click [OK].
   c. The screen will return to the main window.
   d. From the ***SQL*** menu, select ***Statement***. Enter the following statement in the text box:
      ```
      sp_changedbowner lenel
      ```
      Click [OK] when you are ready to execute the statement.
   e. If the command returns highlighted, then it completed without error.
3. Log into any OnGuard application and verify that the change was successful.

APPENDIX C

Manually Creating an ODBC Connection for SQL

The following appendix will detail the manual creation of an ODBC connection for SQL. These instructions are primarily for reference purposes because the OnGuard installation automatically creates the necessary ODBC connection to the database.

If using Windows 7, Windows 8, or Windows 8.1 with UAC turned on, you might receive an error when creating an ODBC with OnGuard applications. This error occurs when you are not running the application as an Administrator. To work around this issue, run the application as Administrator or create the ODBC manually as described in this appendix.

IMPORTANT: When manually creating an ODBC connection you must use the SQL Native Client driver.

Creating an ODBC Connection for SQL

1. Open the ODBC Data Source Administrator window. To do this, navigate to **C:\windows\SysWOW64** and run the **odbcad32.exe** file.
2. The ODBC Data Source Administrator window is displayed. Select the System DSN tab.
3. Click [Add].
4. The Create New Data Source dialog is displayed.
   a. Select **SQL Native Client** from the list view.
   b. Click [Finish].
5. The Create a New Data Source to SQL Server dialog is displayed.
   a. Enter a descriptive Name for the data source.
   b. Enter the name of the machine or virtual machine hosting the database in the **Server** field.
   c. Click [Next].
6. Select SQL Server authentication and enter the **Login ID** and **Password**.

Note: If you select Windows NT authentication it may impact your ability to store credentials in a file as a means of authentication. Selecting SQL Server authentication does not impact your ability to use Windows authentication with the Web applications. Refer to

the Installation Guide for more information about database authentication with the Web applications.

7. Click [Next].
8. Select the **Change the default database to** check box and choose the OnGuard database from the drop-down list.
9. Click [Next].
10. Click [Finish].
11. The ODBC Microsoft SQL Server Setup dialog is displayed.
    a. Click [Test Data Source]. A success message should be displayed.
    b. Click [OK] to exit each of the dialogs.

Updating the DSN in the OnGuard Configuration Files

The ODBC connection information that OnGuard uses to connect to the database is stored in two configuration files. Use the Configuration Editor to ensure that the ODBC connection is configured correctly in these files. For more information, refer to the *Configuration Editor* appendix in the *OnGuard Installation Guide*.

Troubleshooting

If you experience problems connecting to the OnGuard database, check the ODBC connection to be sure that it is configured correctly.

1. From Administrative Tools in Windows, open Data Sources (ODBC).
2. The ODBC Data Source Administrator window is displayed. Select the System DSN tab.
3. Select the DSN used to connect to the OnGuard database from the list view.
4. Verify in the System Data Sources listing window that the DSN driver is SQL Native Client.

Note: If the DSN driver is not SQL Native Client, delete the System DSNand create a new ODBC connection using the SQL Native Client driver. For more information, refer to Creating an ODBC Connection for SQL on page 87.

5. Click [Configure].
6. Verify that the name of the **Server** is correct in the drop-down.
7. Click [Next].
8. Check that the correct method of authentication is selected and verify the credentials if using SQL Server authentication.

Note: If you select Windows NT authentication it may impact your ability to store credentials in a file as a means of authentication. Selecting SQL Server authentication does not impact your ability to use Windows authentication with the Web applications. Refer to the Installation Guide for more information about database authentication with the Web applications.

9. Click [Next].
10. Verify that **Change the default database to** check box is selected and that the OnGuard database is selected in the drop-down.

11. Click [Next].
12. Click [Finish].
13. The ODBC Microsoft SQL Server Setup dialog is displayed.
    a. Click [Test Data Source]. A success message should be displayed.
    b. Click [OK] to exit each of the dialogs.

APPENDIX D

Setting Up & Configuring a Capture Station

The following appendix will show you how to set up and configure a capture station.

Environmental Considerations Affecting Flash & Camera Capture Quality

There are several factors to consider when selecting your capture station environment. Lighting is the most important factor and the most difficult to provide setup instructions for, because every site's capture environment is unique. OnGuard ships with the optimal hardware setting defaults already set. The important items to consider when setting up the capture environment are the flash and camera settings based on environmental considerations.

Setting Up the OnGuard Capture Dialog

You will initially need to set up the OnGuard capture dialog with factory default settings that are appropriate for your capture hardware. Once that is done, you can make minor adjustments to accommodate your specific capture devices and capture environments.

1. Launch the application you'll be using to capture photos/signatures/badge layout graphics.
2. Launch the capture dialog from within that application by selecting the [Capture] button on a form that accesses the Multimedia Capture module.
3. Repeat the following procedure for each outer capture form:
   a. If configuring cardholder photo capture, select the Photo tab. If configuring cardholder signature capture, select the Signature tab. If you are using the BadgeDesigner application, you only have the Graphic tab.
   b. Configuring the capture dialog with settings that are appropriate for your capture hardware is easily done via the factory defaults profile procedure. Use the following procedure to configure capture from sources other than the File Import capture source:
      i. Click [Load Factory Defaults]. The "Load Factory Defaults" dialog will open.

ii. Select the factory defaults profile that most closely matched your capture device. The default capture source (configured on the General Settings form) will be automatically set to the capture source associated with that device. The crop window (configured on the General Settings form) will be automatically set to a size appropriate for the profile you select.

iii. Click [OK].

c. If you want to capture images with the “File Import” capture source:

i. From the capture source drop-down list, select **File Import**.

ii. Click on the File I/O Settings tab.

iii. Set the file import directory to the directory where you store all of your photo files.

iv. Click [Save User Defaults].

d. If you want to capture images with a USB camera or any WDM or TWAIN compliant camera, configure the multimedia capture module for the following settings instead of loading the default settings. If you are using the CAM-24Z704-USB camera skip these steps and refer to Basic Camera Setup (CAM-24Z704-USB) on page 96.

1) From the capture source drop-down list, select **WDM Video**.

2) Click the WDM Video Settings Device tab.

3) Select **USB Video Bus II, Video** from the Device drop-down box.

4) Click [Video Input].

5) The Video Input Properties window displays.

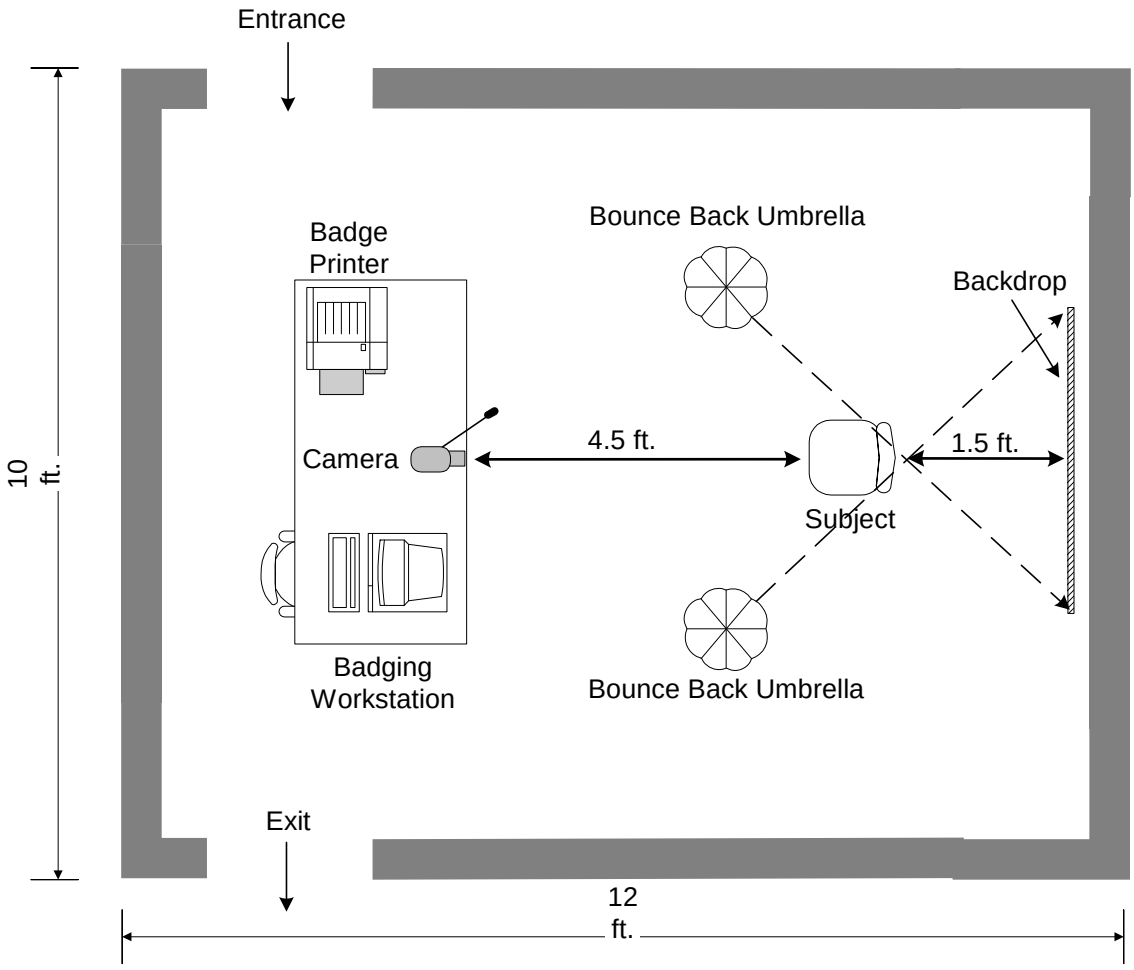
6) Select **1:VideoSVideo In** from the Input drop-down menu.

Capture Station Setup Specifications

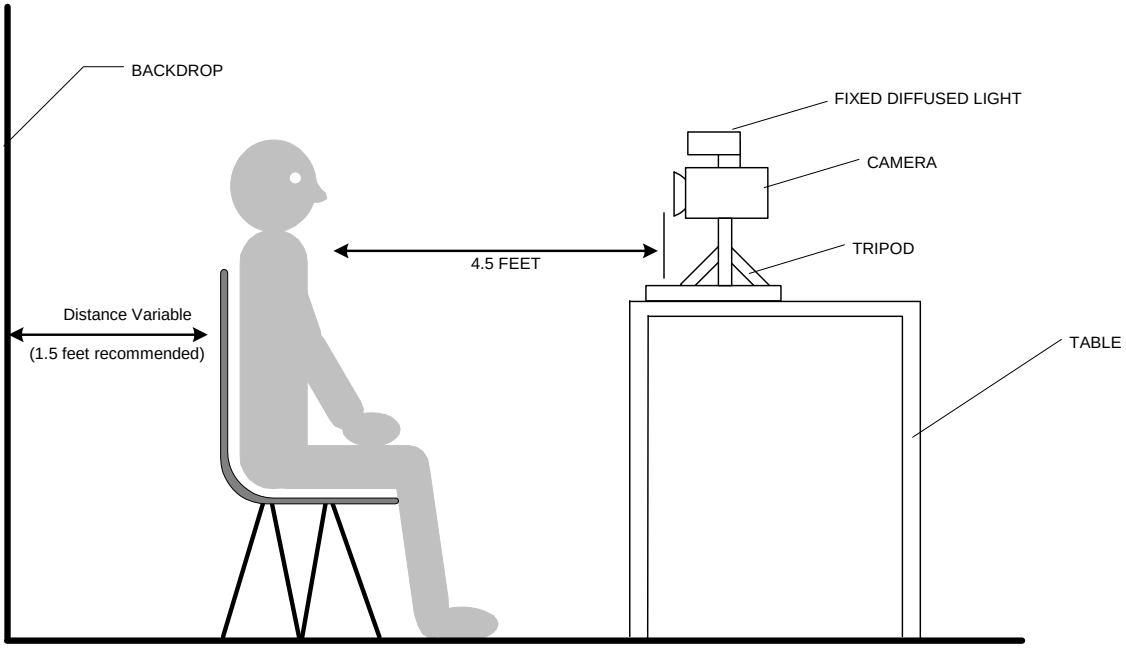
For every capture station the equipment should be setup as close as possible to the following specifications:

The backdrop should be approximately 1.5 feet behind the subject. The camera and flash apparatus should be at least 4.5 feet in front of the subject at an average height (the height should be adjustable for obvious reasons). The capture area requires approximately 10 to 12 feet of floor space with appropriate width.

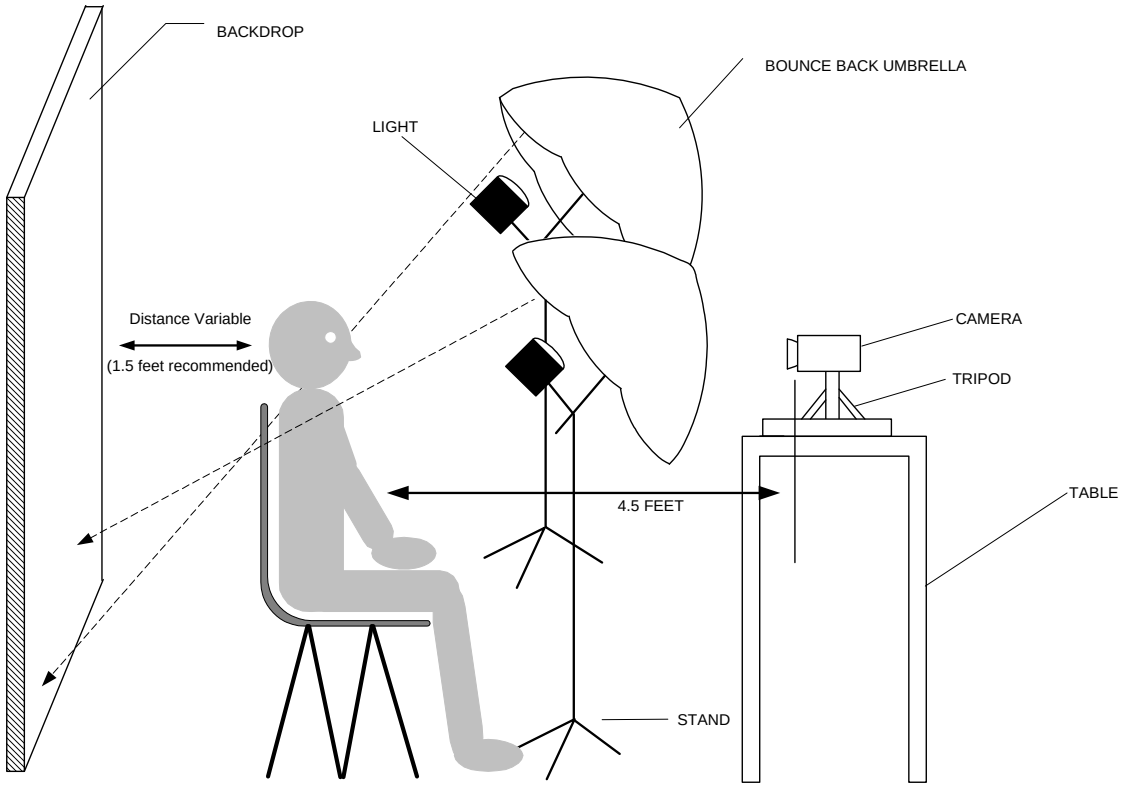
Recommended Badging Room Layout



Final Adjustments for Fixed Diffused Lighting



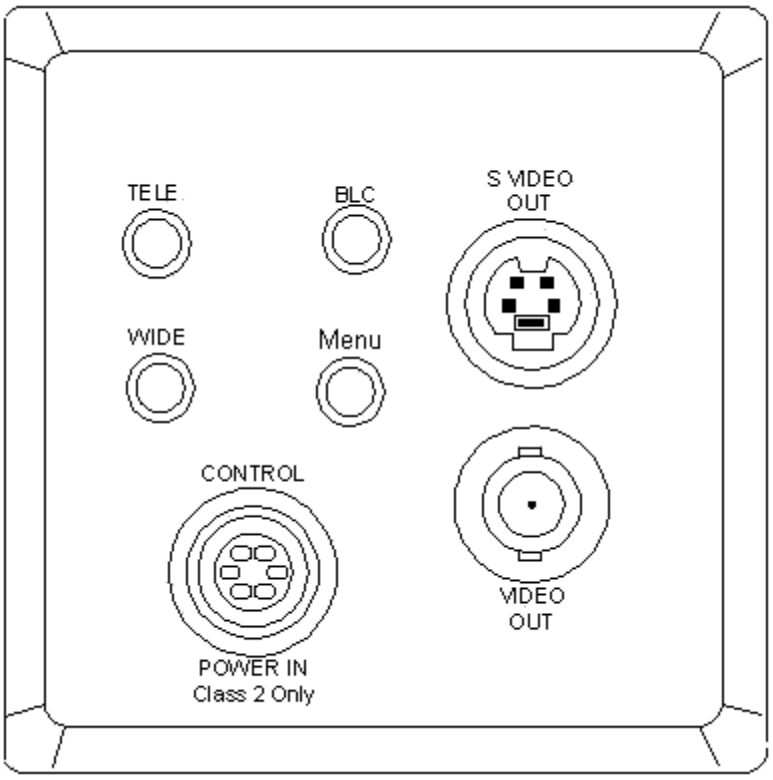
Final Adjustments for Continuous Lighting



Basic Camera Setup (CAM-CCP-500K)

For complete installation setup, see the instruction manual that came with the CAM-CCP-500K.

CCP-500 (Back View)



1. Tele Button – (Telephoto) Press this button to zoom in.
2. Wide Button – (Wide Angle) Press this button to zoom out.
3. BLC – (Back Light Compensation) If you press this button while viewing a backlight subject, the camera will adjust itself to the high contrast lighting.
   - BLC mode is switched between ON and OFF by pressing this button.
   - If you hold the button down for more than 2 seconds and then release, the BLC will change to AUTO BLC mode.
4. Menu – Press to display OSD
   - If you hold the button for more than 2 seconds and then release, OSD will shut off.
5. Power In and Control – Insert the DC power cable here to connect the camera to the DC power source (DC 12V). You can control the Zoom and Focus Lens to use Controller.
6. Video Out terminal - Connect this terminal to the video input terminal or an external input, such as a monitor, TV or VCR.
7. S-Video Out terminal – This is an output terminal for separate Y/C video signals.

The CAM-CCP-500K camera zooms to X32, but the recommended zoom area should be less than X16. This is because the zoom past X16 is digital and the picture captured becomes rough (pixilated). The subject should be within X1 to X12 zoom for optimal results. The subject should nominally fill the pre-sized crop window if adjusted properly. Always leave on “Maintain Aspect Ratio”

To adjust the zoom, set the selector switch to zoom (all the way to the right). Adjust the camera apparatus for the center of the subject. With the arrows located to the bottom left of the rear of the camera, zoom in all the way and then zoom back to determine the approximate center point of the zoom (remember: you do not want to zoom past X12, the halfway point). Then, zoom into the subject until the desired capture frame is attained. The arrows located at the bottom of the camera can be use in one of two manors. If you push and hold the arrow, it will zoom all the way in or out. If you push the arrow button momentarily, it will move in and out incrementally.

Note: Optimally the subject should fill the pre-sized crop window, so no additional cropping adjustments need be made.

Why manual white balance? With light or gray colors the Auto White Balance adjusts incorrectly. That is why the CAM-CCP-500K should be setup for Manual White Balance. It is necessary to White balance the camera to obtain a default white balance setting and is maintained for consistent picture quality.

Basic Camera Setup (CAM-24Z704-USB)

IMPORTANT: The following cameras are meant for client machines and not servers. Windows Server 2012 is not supported.

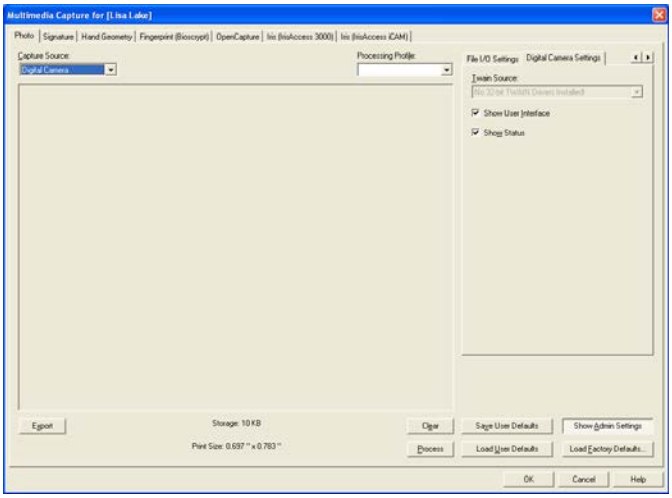
Installation of CAM-24Z704-USB

To install the USB camera simply plug it in, connect the USB cord to the workstation, and install the drivers that come with the camera. For more information refer to the Badging Image Capture Camera User Guide that came with the camera.

Note: Though there is a connection for S-video Out it is strongly recommended that you use the USB connection.

Configuration of CAM-24Z704-USB

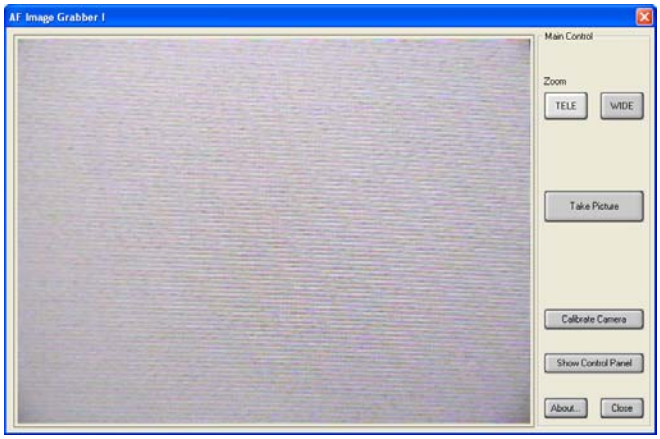
1. Start the application you will be using to capture photos/signatures/badge layout graphics.
2. Launch the capture dialog from within that application by selecting the [Capture] button on a form that accesses the Multimedia Capture module.
3. On the Photo sub-tab of the Multimedia Capture module, select **Digital Camera** from the **Capture Source** dropdown box.
4. On the Digital Camera Settings sub-tab, select **AF Imaging Grabber 1** from the **Twain Source** dropdown box.



IMPORTANT: Make sure that the **Show User Interface** check box IS selected.

Using CAM-24Z704-USB

1. To use, click **Get Photo** on the Multimedia Capture module. The AF Image Grabber 1 control box opens.
2. Click **Take Picture** to take the picture. The AF Image Grabber 1 control box closes and you see the picture on the Multimedia Capture Module screen.
3. Click [OK] and the picture is added to the Cardholder screen.



AF Image Grabber 1

TELE

Zooms in. The camera has a 16:1 optical zoom range along with an 8x digital zoom.

WIDE

Zooms out.

Take Picture

Takes a picture for use in the Multimedia Capture module. When selected the camera image freezes, the LED illuminator turns on, and the image is captured.

Calibrate Camera

Automatically adjusts the camera settings to provide the best quality image under certain lighting conditions. For more information refer to the Badging Image Capture Camera User Guide that came with the camera.

Show Control Panel

Activates the on screen control panel for making adjustments to the captured video image.

Lighting Setup

Professional Continuous Lighting Setup (EHK-K42U-A)

The EHK-K42U-A kit is designed to help eliminate shadows that may appear behind the subject that you are capturing, or under the subject's chin (known as bearding). Most capture environments have adequate light to capture a subject with the CAM-CCP-500K capture kit, but to enhance the colors (more real life), and to eliminate shadows, the capture kit is necessary.

Advanced Setup

After the capture station has been setup, some testing must be performed to determine the optimal illumination settings for image capture. You may have to adjust the lights, drapes, or other elements in the capture environment.

With a test subject, view the live image on the screen with all the room lights on. Set the selector switch on the back of the camera to iris (all the way to the left). With the arrows on back of the camera adjust the iris all the way down, the live image on the screen should become dark if not black. The arrows located at the bottom of the camera can be use in one of two manners. If you push and hold the arrow, it will zoom all the way in or out. If you push the arrow button momentarily, it will move in and out incrementally. While viewing the screen, increase the iris until the subject is visible. Increase the iris a little more, until the screen image is about the same brightness as the real view of the subject. Take a test picture. Label this "test 1, all lights". From here we will adjust the room environments lighting and make minor adjustments to the iris if needed while continuing to save the sample captures at (test 2, test 3 etc.).

Steps to improving capture quality:

1. Turn on all the lights in the room.
2. Open the Capture dialog and center on a test subject with the camera.
3. Adjust the iris all the way down, and then adjust it until the screen image is about the same brightness as the real viewable image.
4. Set the White Balance. (Set the selector switch on the back of the camera to WB. Hold a white piece of paper in front of the camera so there is only white showing on the screen. Using the arrows on the back of the camera adjust the white balance until the image in the capture window is white.)
5. Take a test picture. Save this as a cardholder labeled "Test1: all lights".
6. Turn off all the lights.
7. Take another picture. Save this as a cardholder labeled "Test2: no lights".
8. Continue testing until a desired lighting quality is captured on the screen. Be sure to label each test with a number and a description of what you did. Adjust your environments based on the

environmental considerations below. Continue to take pictures, save them, and use them as references until the best conditions are determined.

Environmental Considerations and Factors Leading to Poor Lighting

Environmental factors to consider when setting up a capture station include:

- Is there a different amount of sunlight entering the area through out the day?
- Is the station next to a window or under a skylight?
- Are the wall colors dark or light or bright colors? If they are light they will reflect more light or change your white balance setup.
- Is the ceiling low or cathedral like? The lower the ceiling the more light will reflect.
- What types of lights are used in the room? Incandescent or florescent (cool white or colored) or direct spots?
- Is there any direct lighting of the subject? Is the room evenly illuminated? Direct lighting will over expose the subject.
- What is the color of reflective shields around the lights? For example, gold reflective surface shields illuminate the subject in yellow highlights.

This is just a partial list of possible factors leading to poor image lighting quality. There may be other features of your site that will affect the image capture that may need to be considered.

Index

UTC Fire & Security Americas Corporation, Inc.
1212 Pittsford-Victor Road
Pittsford, New York 14534 USA
Tel 866.788.5095 Fax 585.248.9185
www.lenel.com
docfeedback@lenel.com

LENEL
United Technologies