AT&T Cabling Systems

CablingGuard™ V5 Prerequisites

July 2019

AT&T

Version Control – Version 2019-07-10

Table of Contents

1.0 Welcome 3

2.0 Site Environmental and Power Requirements 3

3.0 Technical Skills and Access Requirements 3

4.0 CABLINGGUARD™ Server Requirements 4

4.1 Hardware 4

4.2 Operating system 5

5.0 CABLINGGUARD™ Application, Server and Scanner Licenses 6

6.0 Additional Software 7

6.1 Microsoft SQL Server 2016 Express Database 7

6.2 Microsoft .NET Framework V4 7

6.3 SAP Crystal Reports 7

6.4 Java 7

7.0 Configure Web Client 8

7.1 Silverlight Installation and Configuration 8

8.0 Configure Network Environment 11

8.1 Access Control 11

8.2 Switch and Device Configuration 11

8.3 CABLINGGUARD™ Discovery Engine 11

9.0 Proceed to Installation Guide 11

1.0 Welcome

This document describes items required to install and operate CABLINGGUARD™ V5 on a Microsoft Windows Server 2016 operating system including:

- Technical skills
- CABLINGGUARD™ Server (hardware, operating system, disk space)
- CABLINGGUARD™ Software (database, runtimes, applications)
- Web Client
- Network Environment

Consult with the *"CABLINGGUARD™ V5 Installation Guide"* for detailed installation instructions.

2.0 Site Environmental and Power Requirements

The environmental and power requirements for installation of the CABLINGGUARD™ server are defined by the hardware implemented by the end user. The CABLINGGUARD™ Scanner data sheet lists the scanner's environmental and power requirements.

3.0 Technical Skills and Access Requirements

AT&T recommends both familiarity in Microsoft Operating systems and LAN networking. Installation of the CABLINGGUARD™ License Server, CABLINGGUARD™ Application Server Software, and other software required to support CABLINGGUARD™ will require System Administrator access on the server. Knowledge and understanding of configuring Microsoft Internet Information Server (IIS), LAN ports, and granting access permissions to users and directories will be useful for the installation process. Administrator access to configure protocols on network equipment may also be required.

4.0 CABLINGGUARD™ Server Requirements

The CABLINGGUARD™ Server consists of a MS-Windows server operating system with MS-SQL Express database, MS-IIS, SAP Crystal Reports, Java Runtime, CABLINGGUARD™ Application software, and CABLINGGUARD™ License Manager Software.

Prior to installing CABLINGGUARD™, confirm that the designated machine meets the following requirements:

- Root partition with at least 50 GB free
- One network interface configured with an address that can be resolved on the network

4.1 Hardware

Server Hardware Guidance

AT&T recommends use of multi-core servers (especially if users specify a significant number of automatically generated reports). As an option, CABLINGGUARD™ does run in virtualized environments that conform to the listed configurations.

Minimum System Requirements

Supported processors: AMD® Athlon, AMD Opteron, AMD Phenom, Intel Xeon, Intel Core Duo, Intel i5/i7 or better.

RAM: 2 GB Minimum

Recommended Configuration (for Optimal Performance)

Supported processors: AMD Phenom or Intel Core i7

RAM: 4 GB Minimum

4.2 Operating system

The process of installing and configuration of CABLINGGUARD™ on a server requires administrator permissions.

CABLINGGUARD™ supported operating system include:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2016 (1607 or later) - Recommended

The operating system must be fully updated with all Microsoft patches.

Consult with the *"CABLINGGUARD™ V5 Installation Guide"* for appropriate configuration of operating system features.

5.0 CABLINGGUARD™ Application, Server and Scanner Licenses

The CABLINGGUARD™ Application is available from the AT&T Technical Support.

The CABLINGGUARD™ system requires two types of license files, both of which must be activated for the CABLINGGUARD™ system to operate:

- CABLINGGUARD™ Application License – authorizes the application to run on a specific server and the quantity of data channels the system can monitor.
- Scanner License – authorizes the CABLINGGUARD™ server to communicate with the specific scanner. One scanner license is required for each scanner.

CABLINGGUARD™ server and scanner license files are unique for each server and scanner. These licenses are available from AT&T Technical Support.

6.0 Additional Software

MS-SQL Server Express, SAP Crystal Reports, Microsoft .NET Framework V4, Java, and CABLINGGUARD™ application software are required to support a CABLINGGUARD™ Server. Best Practices suggest not installing additional software on the CABLINGGUARD™ Server to avoid unknown interactions.

6.1 Microsoft SQL Server 2016 Express Database

CABLINGGUARD™ uses Microsoft SQL Server 2016 Express as the backend database. MS-SQLExpress 2016 Express is available free from Microsoft. MS-SQL Server 2016 Express supports up to two CPUs, 2GB RAM and 10GB of disk space. MS-SQL Server 2016 Express requires .NET Framework V4. Install the .NET framework as shown in the *"CABLINGGUARD™ V5 Installation Guide"*.

CABLINGGUARD™ uses the MS-SQL Server 2016 Express SQL network service. *"CABLINGGUARD™ V5 Installation Guide"* lists the configuration changes required to configure MS-SQL Server 2016 Express correctly.

6.2 Microsoft .NET Framework V4

CABLINGGUARD™ requires the .NET framework V4. The standalone installer is available on Microsoft website.

6.3 SAP Crystal Reports

The CABLINGGUARD™ Server Application requires installation of both the 32-bit and 64-bit versions of SAP Crystal Reports developer version for Microsoft Visual Studio. Software version 13.0.20 is supported. Download the latest 32 and 64 bit support pack redistributable installation packages (.msi files) from SAP website.

https://origin.softwaredownloads.sap.com/public/site/index.html

6.4 Java

CABLINGGUARD™ requires both x86 and x64 versions of Oracle Java 6 Update 24 or newer. Download the current version of the x86 and x64 Java installer packages.

7.0 Configure Web Client

Access to the CABLINGGUARD™ Application requires a web browser from a MS-Windows computer connected to the same network as the CABLINGGUARD™ Server.

Web browsers options include:

- Microsoft Internet Explorer v7 or greater (v9 or newer recommended)
- Mozilla Firefox v3.6 or greater (v7 or newer recommended)

AT&T recommends that each computer have 2GB of RAM and a two-button mouse for the best user experience.

The computer web browser must have the MS-Silverlight add-on installed. Silverlight Version 5 is required on the web client. Download Silverlight from Microsoft website.

7.1 Silverlight Installation and Configuration

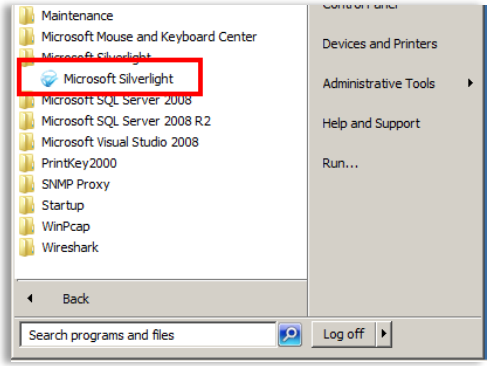
Download and Install Silverlight Version 5 plugin from Microsoft. After installation is complete, check for updates from Microsoft.

Configure Silverlight to optimize performance with the CABLINGGUARD™ application. The configuration changes that follow may affect other programs or applications that use Silverlight.

Select Programs from the start screen.

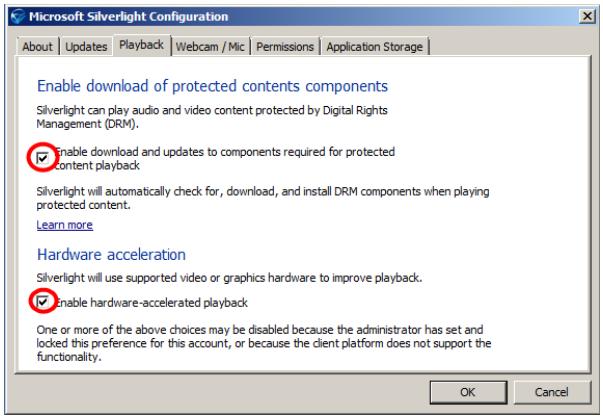
Click on the Microsoft Silverlight Folder.

Click on Microsoft Silverlight.



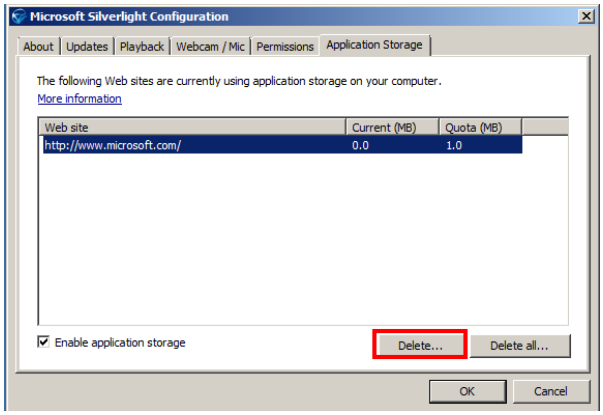
Disable DRM and Hardware Acceleration

Click on the Playback Tab. Uncheck both options for DRM and hardware-accelerated playback.

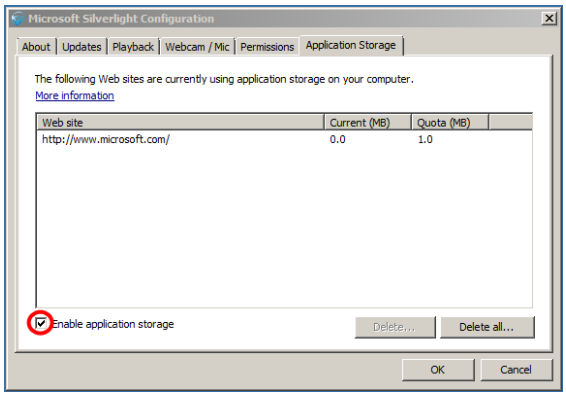


Optional: Disable Application Storage

Click on the Application Storage Tab. Click on web sites to highlight them. Click on the delete button.



Disable Application Storage by unchecking the Enable Application Storage check box.



Click OK and exit the configuration page.

8.0 Configure Network Environment

For the best user experience, the CABLINGGUARD™ GUI requires a stable and consistent network communications between the CABLINGGUARD™ Server, CABLINGGUARD™ Scanner(s), and the user's web browser. High latency or high packet loss connections may interrupt communication between the server and the user interface.

8.1 Access Control

The installation process may require administrator access to network devices. In day-to-day operation, the CABLINGGUARD™ discovery engine requires all devices have SNMPv2 enabled and a RO (Read Only) community string matching the community string set in the CABLINGGUARD™ Server application.

8.2 Switch and Device Configuration

The CABLINGGUARD™ Server requires all switches have Machine Name and IP address assigned to the appropriate VLAN. Typical switch configuration parameters include VLAN, HostName, IP address, and Gateway.

Firewalls and other network devices between the CABLINGGUARD™ Server and CABLINGGUARD™ Scanners (or any CABLINGGUARD™ monitored device) must be configured to permit CABLINGGUARD™ communications services (HTTP, DNS, SNMP, ICMP).

8.3 CABLINGGUARD™ Discovery Engine

CABLINGGUARD™ discovery utilizes DNS to resolve Machine Names. Each Machine Name on the network must be unique.

The CABLINGGUARD™ Discovery engine requires access to standard SNMP port TCP/161 of each switch to determine IP address of device(s) connected to the switch.

The CABLINGGUARD™ discovery engine requires access to standard SNMP ports of the connected device to retrieve the machine name and description of the devices connected to the work area outlet.

9.0 Proceed to Installation Guide

For a new installation of CABLINGGUARD™, proceed to the *"CABLINGGUARD™ V5 Installation Guide"*.