

## DCS Installation Requirements for PrintFleet

The DCS should be installed on an existing networked operations or print server to collect and transmit device data. If no server is available, the DCS can be installed on a single networked computer that will remain powered 24 hours a day, 7 days a week.

**Data Collection will stop during times when the system is powered off resulting in an interruption of historical data.**

The following requirements must be met before installing the PrintFleet Data Collector Service (DCS).

### Network Requirements:

- TCP/IP configured
- Port 443 (HTTPS), port 80 (HTTP), or port 21/20 (FTP) must be open for automatic transmission of collected data
- Port 161/udp should be opened on the machine hosting the DCS
- TCP Port 35 should be opened on computers where DCS 4.0 and Local Print Agent are installed

### System Requirements:

- Operating system: Windows XP, or Windows Server 2003, Server 2008, Windows 7, or Windows Vista\* ([special instructions for installation](#))
- Network card: 100 mbit or higher (system must have only one active network card)
- RAM: 512MB or higher
- Microsoft .NET Framework 2.0 SP2 or 3.5 SP1 or higher
- Internet connected browser

### Important:

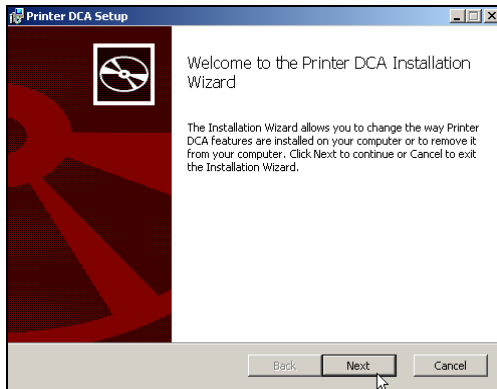
- Do not install the DCS on a laptop
- If you plan to use the DCS to collect data via a VPN, please be aware that due to the extended transmission, **there is a risk of data loss**.
- Do not install on a server that also runs SNMP applications such as “WebJet Admin”, “Insight Manager”, and “IBM Tivoli” as transmission conflicts may occur.

## Installing the PrintFleet DCS for Networked Machines

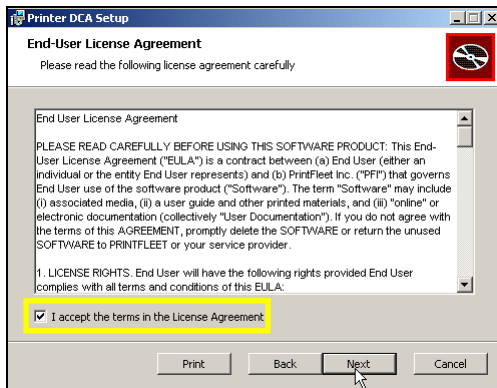
1. Download and install the DCS via the link in the website.
2. On the **Administration** menu click **DCA Install**.
3. Double-click the filename *Printer DCA 4.x.x.x.msi* installation file.



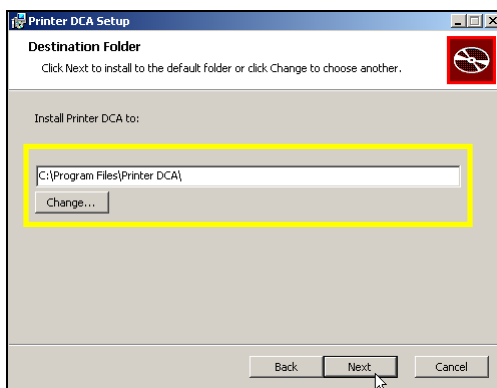
1. The Printer DCA Installation Wizard is launched. Click **Next** to continue.



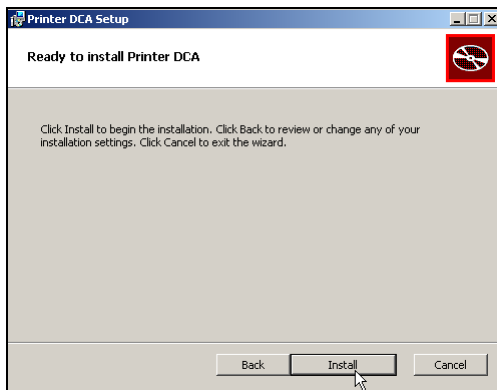
2. Read through the End-User License Agreement, check **I accept the terms in the License Agreement** and select **Next** to continue. If you do not accept the terms, the installation process will not continue.



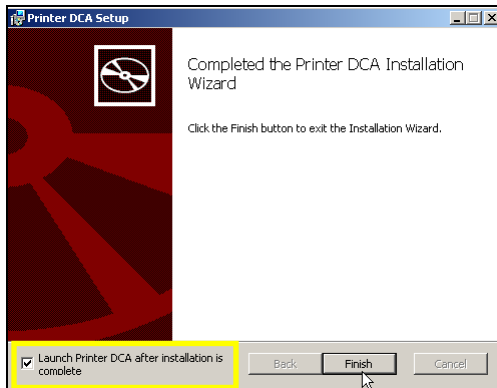
3. In the Destination Folder screen, either leave the default folder displayed, or enter a new destination folder. Click **Next** to continue.



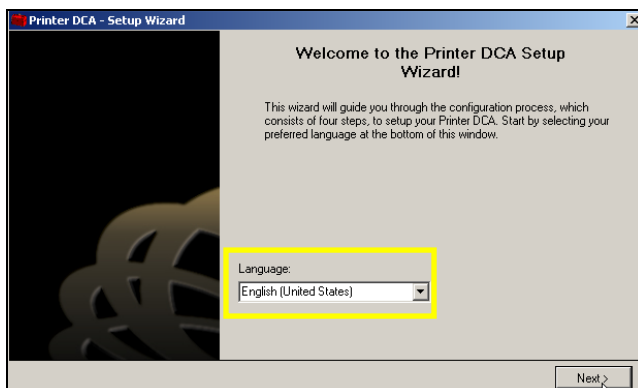
4. In the Ready to Install Printer DCA screen, click **Install** to begin installation or click **Cancel** to exit.



5. In the Completed the Printer DCA Installation Wizard, leave checked or uncheck **Launch Printer DCA after installation** and select **Finish**.



6. In the Welcome to the Printer DCA-Setup Wizard, select the language from the drop down list and select **Next**.



7. In the Printer DCS Activation screen, enter the following:
  - Enter the Server information for the server that the DCS will be sending information to in the **Server** box. (**dcsl.portalmps1.com**)
  - Enter the PIN code in the **PIN Code** box.
  - Optionally, if the location is using a proxy server that you want to configure at this point (you will also be able to do so after installation), click **Show Proxy Configuration**.
  - Click **Next**

Activation

Your DCA has not yet been activated. Please input your activation credentials. You may close this window if you wish to skip activation

Server: dcsl.portalmps1.com

PIN Code: ACEE-0488

Activate

8. In the Scan Settings screen, you will be shown a list of preconfigured IP ranges that will be added to your default DCS network scan. This can be changed after installation is complete if necessary. Click **Next**.

Printer DCA - Setup Wizard

Scan Settings

The following scan ranges have been pre-configured to match your network settings. You can edit these ranges after the setup is complete by opening the Printer DCA and navigating to the "Scan" tab.

Scan Ranges:

- 10.1.10.1-10.1.10.254
- 10.1.20.1-10.1.20.254
- 10.1.31.1-10.1.31.254
- 10.1.32.1-10.1.32.254
- 10.22.10.1-10.22.10.254
- 10.25.10.1-10.25.10.254

Step 2 of 4

< Back Next >

9. In the Intelligent Updates screen, you will be given the option to disable Intelligent Updates. It is recommended that **Allow Intelligent Updates** remains selected unless there is a strong reason to turn it off. Click **Next**.

Printer DCA - Setup Wizard

Intelligent Updates

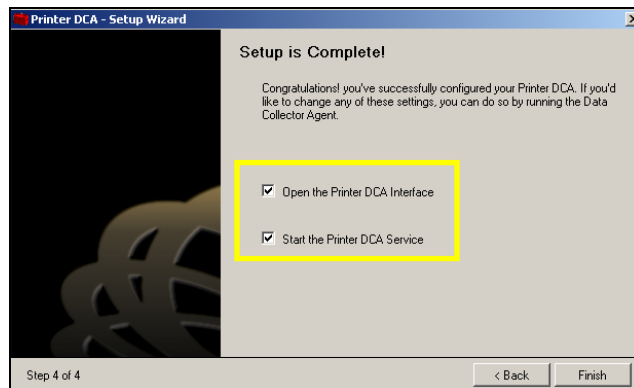
Intelligent updates allow your server to send commands to this Data Collector Agent to notify it that an update is available. This option is strongly recommended.

Allow Intelligent Updates

Step 3 of 4

< Back Next >

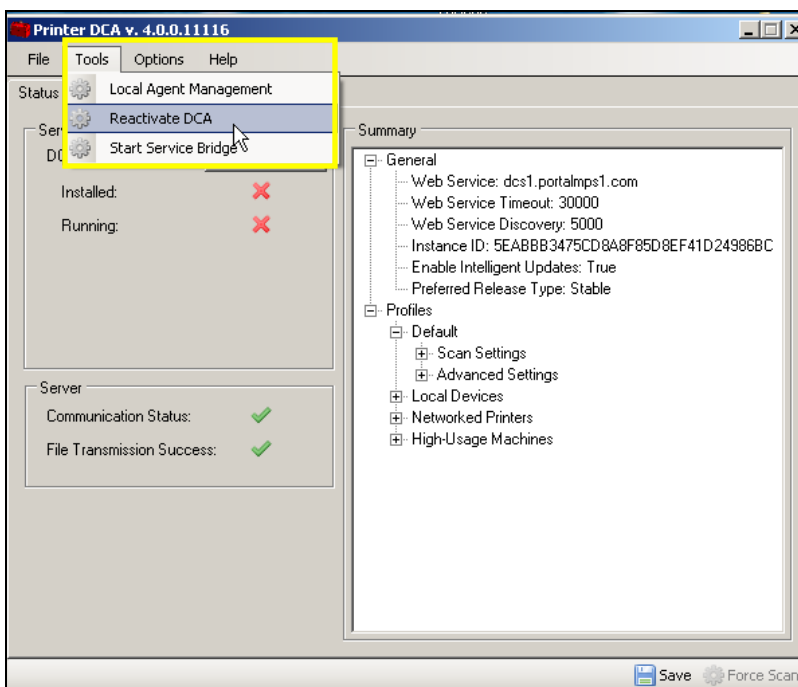
10. In the Setup is Complete screen, by default, the **Open the Data Collector Agent Interface** and **Start the Data Collector Agent Service** are both selected. Optionally, you can turn off one or both of these options. Click **Finish**.



At some point over the life of the DCS installation, you may need to reactivate it, for example, if you were given an activation code with an expiry date, or if you need to redirect the DCS to a new server. You can enter a new activation code from an existing DCS installation.

#### To reactivate the DCS:

1. On the **Tools** menu, click **Reactivate DCA**
2. If you are redirecting the DCS to a new server and/or port, enter the new information in the **Server** box.
3. Enter the new activation code in the **PIN Code** box.
4. Click **Activate**



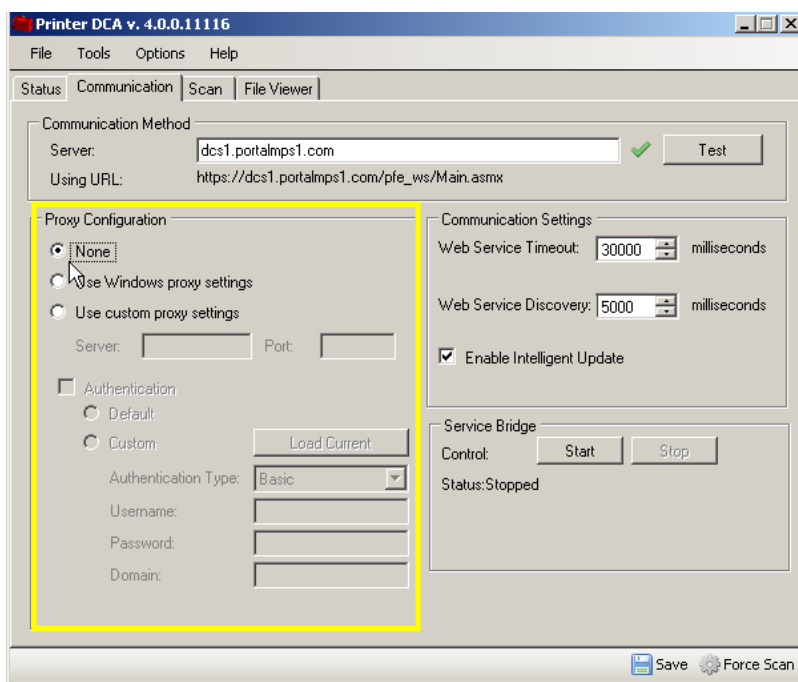
During the DCS installation, the DCS will attempt to establish basic communication with the central server using either HTTPS (default) or HTTP (secondary). Proxy settings can also be configured during installation, or at any time afterwards. If communication with the server is successful during installation, it is not necessary to change the communication method, port, or proxy settings.

## Configuring Communication Settings

If a network being scanned with a DCS uses a proxy server, you can configure the DCS to use the proxy settings, which will allow the DCS to scan the network.

### To use a manual proxy configuration

1. Under the **Communication** tab of the DCS, in the **Proxy Configuration** area, click to select one of the following: **Use Windows proxy settings** (no other configuration required), **Use custom proxy settings**, or **None** (to disable proxy settings).
2. If you have selected **Use custom proxy settings**, enter the server and port information in the **Server** and **Port** boxes, respectively.
3. If the proxy server requires authentication, click to select the **Authentication** check box, and then do one of the following:
  - Click to select **Default** to use the authentication currently being used on the computer installed with the DCS.
  - Click to select **Custom**, and then enter username, password, and domain information in the **Username**, **Password**, and **Domain** boxes, respectively, or click **Load Current** to populate the fields with the current authentication being used by the computer installed with the DCS.
4. In the **Communication Method** area, click **Test** to verify the settings are working.
5. Click **Save**.



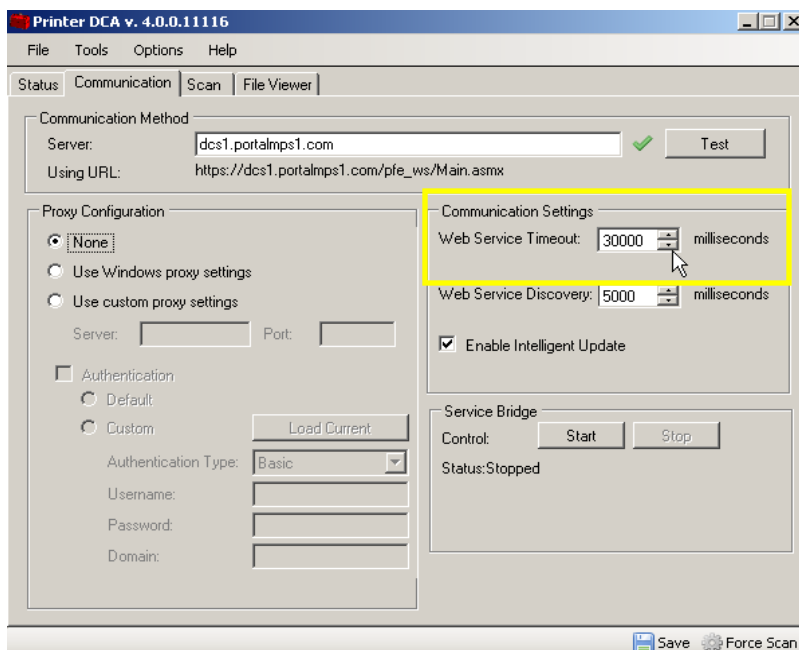
### Changing the web service timeout

The web service timeout determines the maximum time that will be allowed for communication between the DCS and the central server. By default, the web service timeout is 30,000 milliseconds; if necessary, the timeout can be increased or decreased at any time.

### To change the web service timeout:

1. Under the **Communication** tab, in the **Communication Settings** area, enter or select the desired timeout in the **Web Service Timeout** box controls transmission timeout.
2. Click **Save**.

The Web Service Discovery Timeout controls the initial connection to the server and the auto-selection of http/https.

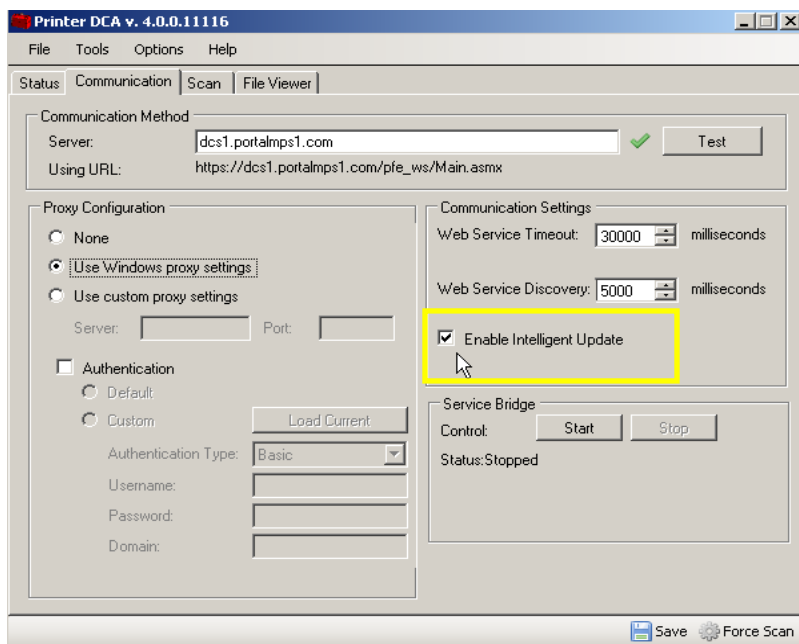


### Enabling Intelligent Update

When Intelligent Update is enabled, as an administrator, you can remotely update and perform other remote actions on the DCS.

#### To enable Intelligent Update:

1. Under the **Communication** tab, in the **Communication Settings** area, click to select the **Enable Intelligent Update** check box.
2. Click **Save**.



## Enabling a Service Bridge

A Service Bridge allows a service technician to create a private, secure connection between a service technician and a specific networked printing device, with the DCS acting as a proxy. Once the bridge is established, the service technician can use a special (private) IP address to directly access the device as if they were on site. The technician can view the embedded web page of the device, perform an SNMP scan, update firmware, etc.

For additional security, an access code must be generated from the central server. This code must then be entered into the applicable DCS.

### On the service technician's computer:

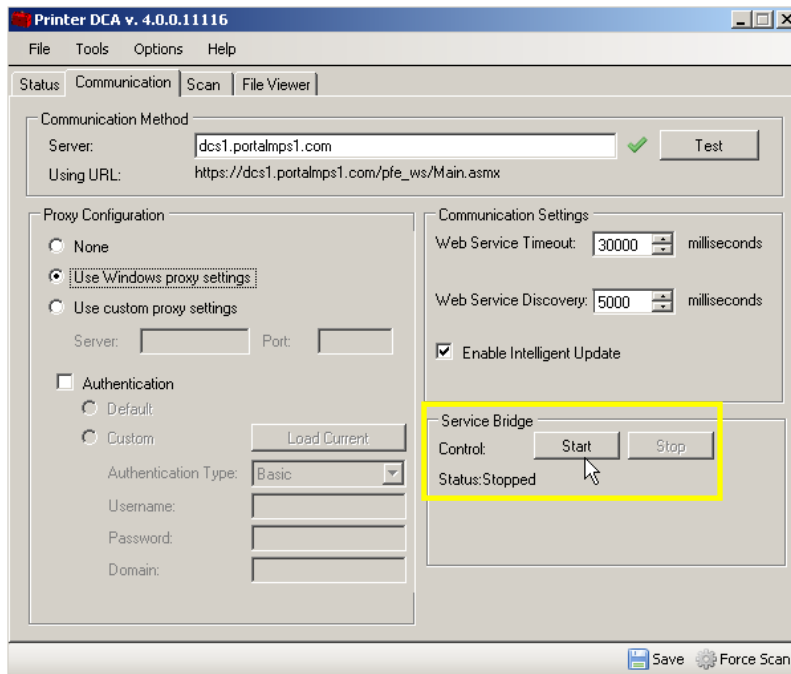
1. The PFO user selects a Device to connect to (the Target Device) and goes to its Details page.
2. The PFO user clicks Device's IP Address shown on the page and selects **Service Bridge** option. The **Service Bridge** option is available for network devices only.
3. If the browser does not support the Click Once feature, download the PrintFleet Service Bridge Client's zip file from <http://PFE Server URL/Downloads/ServiceBridge Client x.x.x.xxxxx.zip>. Extract the zip and run the application. For browsers that do support the Click Once feature, you are prompted to run the PrintFleet.PFE.ServiceBridge.Client application (if not installed).
4. When the PFE URL is displayed, the PFO user can make changes to values or accept default and select OK.
5. The PrintFleet DCS Service Bridge dialog is displayed. If prompted to Download Driver, download the TAP driver and install. When the VPN Connection states Success, a PIN will be generated.
6. Leave this VPN Connection dialog open for the duration. The service technician gives this PIN to the DCS user for their use.

### To enable a Service Bridge from the DCS:

1. Do one of the following:
  - On the **Tools** menu, click **Start Service Bridge**.
  - Under the **Communication** tab, in the **Service Bridge** area, click **Start**.
2. In the **Enter Service Bridge PIN** box, enter the access code generated on the central server and click **Ok**. The **Status** field in the **Service Bridge** area will indicate when the connection has been established.
3. Enter the Remote IP value into your browser; the device's embedded web page is displayed.

### To end the connection:

1. The service technician can close the PrintFleet DCS Service Bridge VPN Connection Success dialog.



### Configuring Network Scan Settings

The DCS network scan settings determine how the DCS collects information from the internal network, and provides options for transmitting the information to the central server. Scan profiles can be used to configure multiple types of network scans that will run independently, for example, you might want different scan and transmission settings for networked and local devices. Network scan settings are independent of communication settings, which specify how the DCS will communicate with the central server, and if and how the central server can communicate with the DCS and/or a specific device on the network.

### Managing Scan Profiles

You can use profiles to configure multiple types of network scans. For example, you might want to scan networked devices every hour, and local devices once a day—these would be two different scan profiles. You might also want a different scan profile for one or two high priority devices that you want to scan more frequently.

Depending on your environment, you might have multiple uses for scan profiles, or you might not need more than one. When you first install the DCS, you will have one scan profile called Default.

### To create a new scan profile:

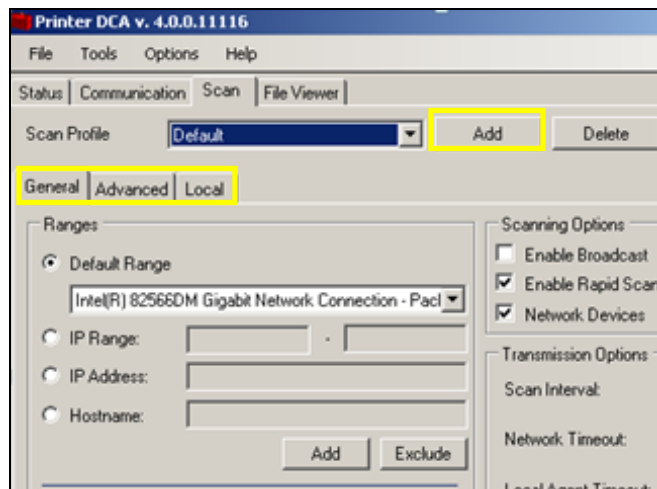
1. Under the **Scan** tab, beside **Scan Profile**, click **Add**.
2. In the **New Profile** dialog box, enter a name to associate your new profile with, and click **Ok**.
3. Configure all settings under the **General**, **Advanced**, and **Local** tabs that apply to the new profile, or copy setting from another profile.
4. Click **Save**.

### To edit an existing scan profile:

1. Under the **Scan** tab, select the profile you want to edit from the **Scan Profile** list.
2. Edit settings as applicable under the **General**, **Advanced**, and **Local** tabs.
3. Click **Save**.

### To delete a scan profile:

1. Under the **Scan** tab, select the profile you want to delete from the **Scan Profile** list.
2. Beside **Scan Profile**, click **Delete**.
3. In the Delete Profile? Dialog box, click Yes.



### Specifying which devices to scan

The DCS only scans the IP addresses and/or hostnames specified in each scan profile. When the DCS is first installed, it selects a default set of IP addresses to scan based on either Active Directory or, if that is not available, the primary network card on the system installed with the DCS. These IP addresses are automatically added to the Default scan profile. If the default set of IP addresses captures all the devices on the network that you want to scan, and you do not want multiple scan profiles, you do not have to further specify the devices for the DCS to scan.

If, however, you want to adjust the devices included in the default scan, or if you have more than one scan profile, you will need to further configure which IP addresses and/or hostnames to include. Single IP addresses, ranges of IP addresses, and hostnames can all be used to specify devices to include or exclude from a network scan. There are two general purposes for excluding a device or range of IP addresses from a network scan: (1) to specifically not collect information from a device or set of devices; or (2) to remove IP addresses that you know do not have printing devices on them to create the most efficient scan range (shorter network scan time).

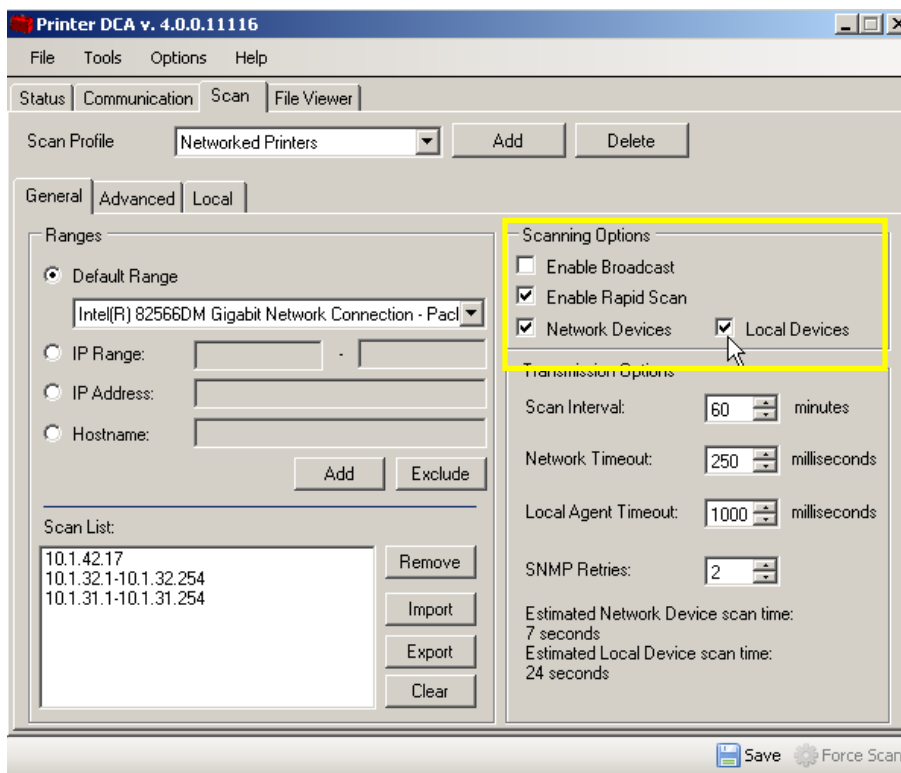
### Enabling Scanning of Network and/or Local Devices

You must enable at least one of network or local device scanning for the DCS to collect data. For local device scanning to work, you must also have Local Print Agent installed on computers connected to the local devices you want to scan.

If you have created separate profiles for networked and local devices, you will enable network device scanning in one, and local device scanning in the other.

### To enable scanning of network and/or local devices:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list.
2. Under the **General** tab, in the **Scanning Options** area, do one or both of the following:
  - Click **Network Devices** to enable scanning of networked printing devices.
  - Click **Local Devices** to enable scanning of locally connected printing devices.
3. Click **Save**.



### Enabling Rapid Scan

Rapid Scan allows the DCS to use multithreading, which significantly decreases the time it takes for the DCS to complete a network scan.

### To enable Rapid Scan:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list.
2. Under the **General** tab, in the **Scanning Options** area, click **Enable Rapid Scan**. See above caption.
3. Click **Save**.

The number of threads can be controlled on the **Advanced** tab. Defaults to a reasonable value for the current system.

## Setting the Scan and Transmission Interval

The scan interval determines how often the DCS will scan the network and transmit the collected information to your destination server. The default scan interval is 30 minutes.

It is generally not useful to set a scan interval for more than every 30 or 60 minutes. For example, new information is posted to the website every 10 minutes, but new alerts are generated approximately every 30 minutes.

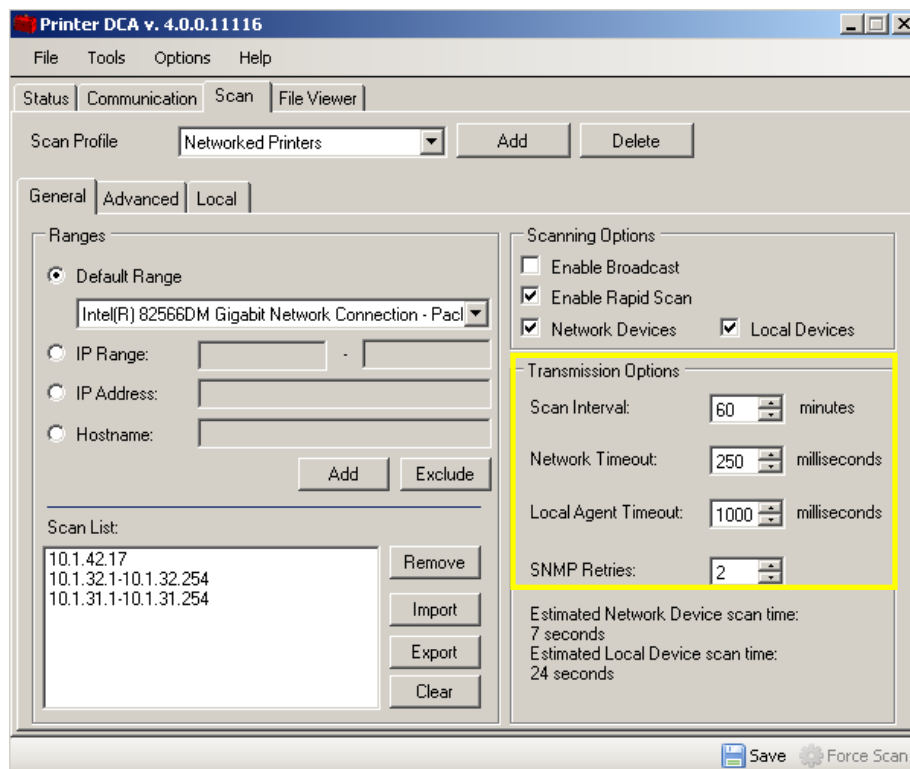
## Setting the Network Timeout

The network timeout is the amount of time that the DCS will wait for a networked device to respond back with its information. The default network timeout is 250 milliseconds.

The network timeout only needs to be adjusted if the DCS is not collecting complete information from networked devices. If, when you perform a DCS scan, certain data fields which should be populated are reporting no information; you may need to increase the network timeout to 500 or 1000 milliseconds. However, the higher the network timeout is set, the longer the DCS scan will take. There may be other reasons that the DCS is not collecting complete information, for example, the device may not store a specific data field (toner levels, etc.).

### To change the network timeout:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list.
2. Under the **General** tab, in the **Transmission Options** area, type or select the desired network timeout, in milliseconds, in the **Network Timeout** box.
3. Click **Save**.



## Setting the Local Print Agent Timeout

The Local Print Agent timeout is the amount of time that the DCS will wait for the Local Print Agent application to respond back with information from a locally connected device. The default Local Print Agent timeout is 10,000 milliseconds per system. Local device collection takes substantially longer than networked device collection because of the extra step needed to go through the connected computer via the Local Print Agent application.

The Local Print Agent timeout only needs to be adjusted if the DCS is not collecting complete information from locally connected devices. There may be other reasons that the DCS is not collecting complete information, for example, the device does not store a specific data field (toner levels, etc.), or a Local Print Agent is not installed on the computer connected to the local device.

### To change the Local Print Agent timeout:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list.
2. Under the **General** tab, in the **Transmission Options** area, type or select the desired Local Print Agent timeout, in milliseconds, in the **Local Print Agent Timeout** box.
3. Click **Save**. See caption above.

## Setting the Number of SNMP Retries

The number of SNMP retries entered in the DCS settings is the number of times the DCS will attempt to get information from a device that is responding with incomplete or no information. Increasing the number of SNMP retries may increase the completeness of a DCS scan, but will also increase the amount of time it takes to complete a network scan.

### To change the number of SNMP retries used:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list.
2. Under the **General** tab, in the **Transmission Options** area, type or select the desired Local Print Agent timeout, in milliseconds, in the **Local Print Agent Timeout** box.
3. Click **Save**. See caption above.

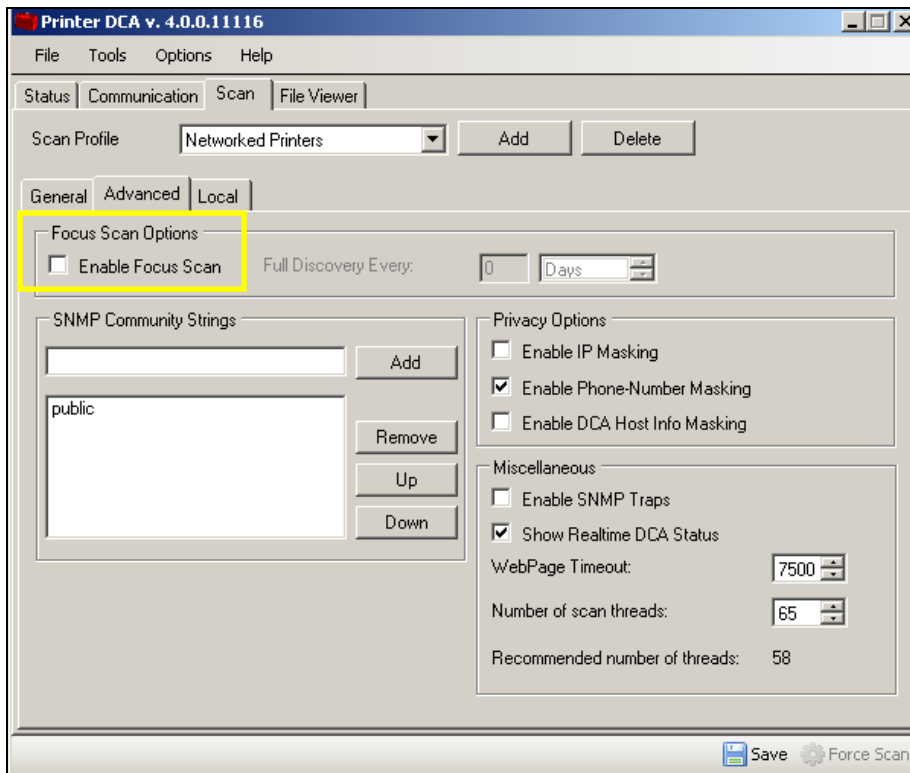
## Using Focus Scans

Without using Focus Scan, the DCS will scan each IP address, IP range, and hostname specified in the scan range settings every time the DCS performs a full network scan. Using Focus Scan, you can specify a periodic interval for the DCS to perform a full network scan, and the scans performed between the intervals will scan only devices found during the previous full network scan.

Using Focus Scan can decrease the amount of total time and bandwidth that the DCS occupies, particularly on large networks, while ensuring that new or relocated document output devices are discovered on a periodic basis.

### To enable Focus Scan:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list.
2. Under the **Advanced** tab, in the **Focus Scan Options** area, click to select the **Enable Focus Scan** check box.
3. Specify how often you want a full network scan to run by selecting either **Days**, **Hours**, or **Minutes** from the list, and entering a number for the interval beside **Full Discovery Every**. For example, if you enter 5 and select Days, a Focus Scan will run once every five days.
4. Click **Save**.



### Storing SNMP Community Strings

Community strings act as passwords on networked devices that limit access via SNMP. Since the DCS uses SNMP to collect data from devices, any custom community strings on printing devices put in place by network administrators can be manually entered in the DCS to allow it SNMP access to the device. Most devices have a community string of public, and the DCS stores a community string of public by default.

#### To store community strings in the DCS:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list.
2. Do one or more of the following under the **Advanced** tab, in the **SNMP Community Strings** area:
  - To add a community string, type an applicable community string in the text box, and click **Add**. Repeat as necessary.
  - To remove a community string, click to select a previously entered community string, and then click **Remove**.
  - To reorder the list of community strings, click to highlight a community string, and then click either the **Up** or **Down** button. Repeat as necessary. When the DCS encounters a device using a community string during the network scan, it will attempt to use the first community string listed, then the next, etc., until it is successful or it runs out of community strings to attempt.
3. Click **Save**. See caption above.

## Masking Private Data

For privacy reasons, the following types of information that the DCS collects can be masked in the transmission file to the central server:

- IP addresses of devices included in the network scan
- Telephone numbers collected from devices (masked by default)
- DCS host system information (IP address, MAC address, subnet, etc.)

### To mask private information in DCS transmission files:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list.
2. Under the **Advanced** tab, in the **Privacy Options** area, do one or more of the following:
  - Click to select the **Enable IP Masking** check box to mask device IP addresses.
  - Click to select the **Enable Phone-Number Masking** check box to mask telephone numbers collected from devices (masked by default).
  - Click to select the **Enable DCA Host Info Masking** check box to mask DCS host system information.
3. Click **Save**. See caption above.

## Managing Local Devices With Local Print Agent

There are three steps that must be taken to collect local printer data using the DCS:

1. Add the IP addresses/ranges of computers connected to local printers to the DCS network scan.
2. Enable the local device scanning option.
3. Install Local Print Agent on computers connected to local printers (instructions follow).

Local Print Agent allows the DCS to obtain information directly from locally connected printing devices. The Local Print Agent application must be installed on each computer connected to a local printer that you want to collect information from. Ideally, Local Print Agent will be installed on all computers at any location where you want to collect local printer information. This will allow you to collect information from new local printers as soon as they are connected.

There are three methods to install Local Print Agent:

- Manual installation from the local printer host computer
- DCS push tool installation (manual and automated)
- Third party push tool installation

In environments that do not allow push installation tools, you may be required to manually install the Local Print Agent application on each computer connected to a local printer.

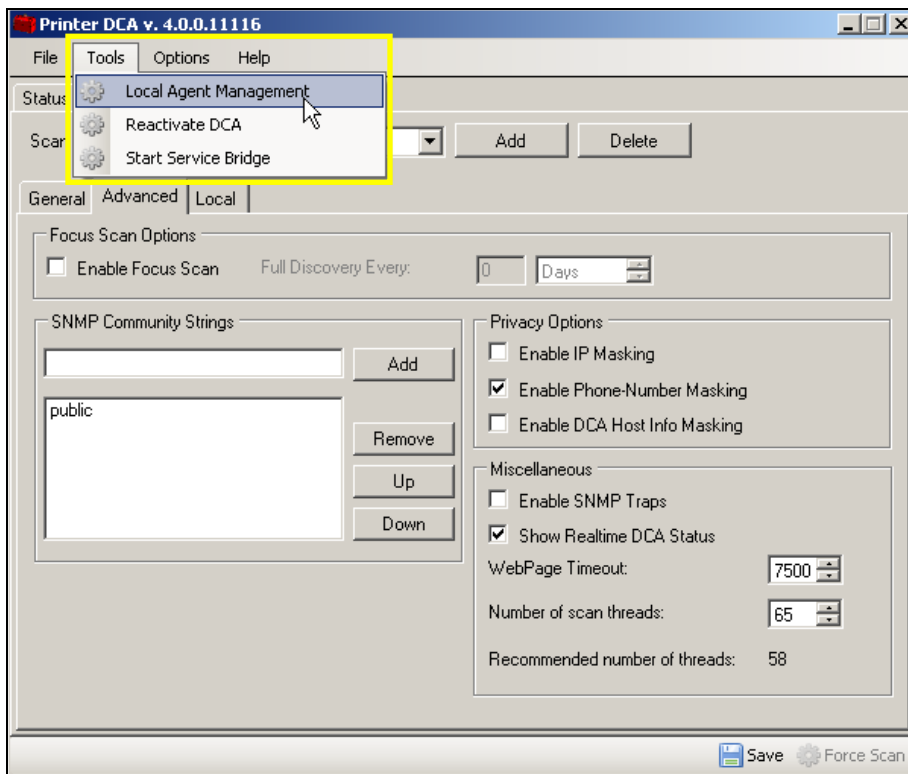
### To install Local Print Agent manually from the local printer host computer:

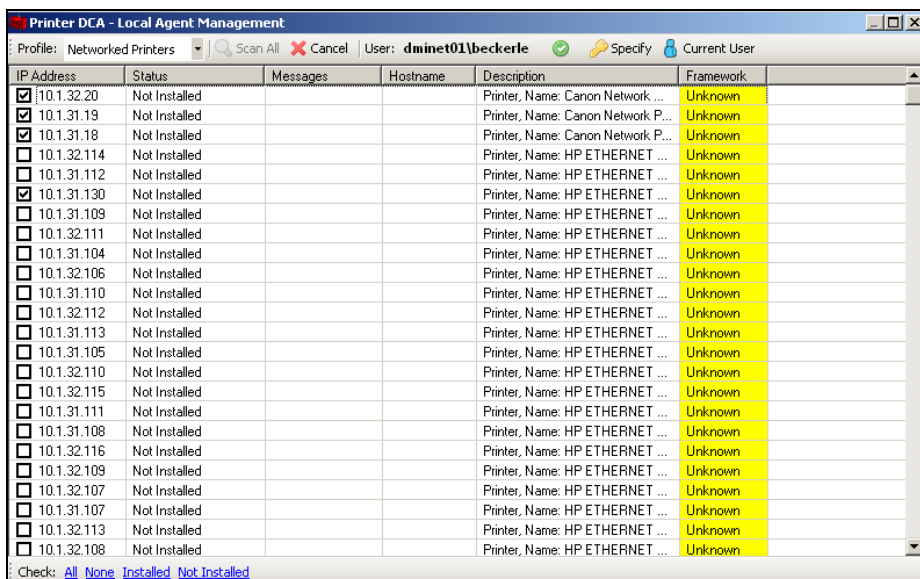
- Run the Local Print Agent.msi file on the computer you want to install Local Print Agent on. The installation file is found by default in: program files\Printer DCA\Support folder. The installation file can be copied to a USB drive, CD, etc. for portability.

The DCS has an embedded push install utility specifically for Local Print Agent. In addition, you can schedule periodic push installs to your entire DCS scan range to ensure that Local Print Agent gets installed to any new computers on the network.

**To push install Local Print Agent from the DCS:**

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list.
2. On the **Tools** menu, select **Local Agent Management**.
3. Click **Scan All**. This will scan all IP addresses included in the selected scan profile.
4. Under the IP Address column, click to select the check boxes beside each IP address belonging to a computer you want to install Local Print Agent on. Optionally, click **All**, **None**, **Not installed**, or **Installed** to automatically select a set of IPs.
5. If you are not currently logged onto the computer as an administrator, in the **Credentials** area, click **Change**. Enter the local administrator credentials (for the target OS) in the **Username**, **Password**, and **Domain** boxes, and then click **Ok**.
6. Click **Install**.



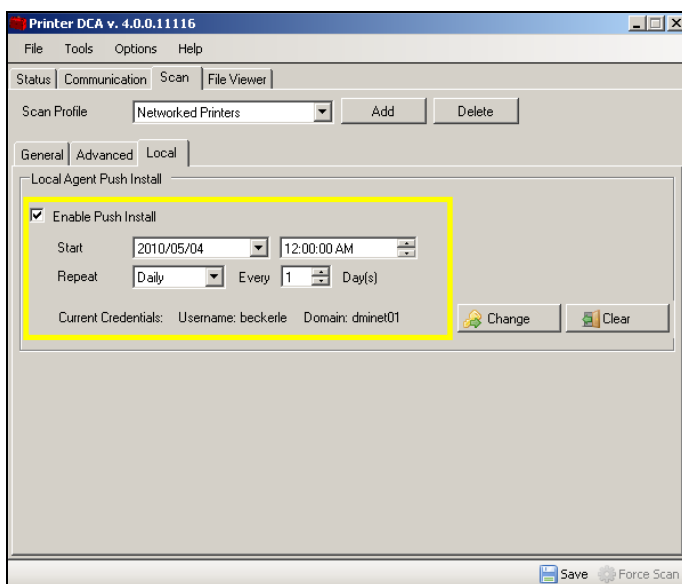


IP Address	Status	Messages	Hostname	Description	Framework
<input checked="" type="checkbox"/>	10.1.32.20	Not Installed		Printer, Name: Canon Network ...	Unknown
<input checked="" type="checkbox"/>	10.1.31.19	Not Installed		Printer, Name: Canon Network P...	Unknown
<input checked="" type="checkbox"/>	10.1.31.18	Not Installed		Printer, Name: Canon Network P...	Unknown
<input type="checkbox"/>	10.1.32.114	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.31.112	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input checked="" type="checkbox"/>	10.1.31.130	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.31.109	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.32.111	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.31.104	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.32.106	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.31.110	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.32.112	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.31.113	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.31.105	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.32.110	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.32.115	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.31.111	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.31.108	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.32.116	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.32.109	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.32.107	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.31.107	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.32.113	Not Installed		Printer, Name: HP ETHERNET ...	Unknown
<input type="checkbox"/>	10.1.32.108	Not Installed		Printer, Name: HP ETHERNET ...	Unknown

### To schedule regular push installs using the DCS:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list.
2. Under the **Local** tab, select the Enable Push Install check box.
3. In the Change Push Install Credentials screen, enter the credentials of the user that belongs to the local administrator group on the target OS.
4. Beside Start, select a start date and time for the automated push install.
5. Beside Repeat, select the interval you want to perform the push install at.
6. Click **Save**.

If the environment already uses a third party push installation tool, you can use that to push install the Local Print Agent.msi file. The installation file can be found in the Printer DCA\support folder on the system installed with the DCS (its default location). Refer to the user guide for the third party push installation tool for further instructions.



Printer DCA v. 4.0.0.11116

File Tools Options Help

Status | Communication | Scan | File Viewer

Scan Profile: Networked Printers [Add] [Delete]

General | Advanced | Local

Local Agent Push Install

Enable Push Install

Start: 2010/05/04 12:00:00 AM

Repeat: Daily Every 1 Day(s)

Current Credentials: Username: beckerle Domain: dminet01 [Change] [Clear]

[Save] [Force Scan]