Peregrine **Network Discovery**

Release Notes

Version 5.2

Peregrine
S Y S T E M S.

Peregrine Systems, Inc.
3611 Valley Centre Drive San Diego, CA 92130
Tel 800.638.5231 or 858.481.5000
Fax 858.481.1751
www.peregrine.com

Contents

Network Discovery 5.2 Release Notes

Version 5.2 of Peregrine's Network Discovery is a minor release of the product.

These *Release Notes* for version 5.2 have the following sections:

Overview

Network Discovery is a mature, low-impact solution for discovering and managing your network infrastructure. It allows you to address business issues in many areas of the organization and requires only a minimum of administration.

The new version 5.2 implements a host of new features and improvements designed to make deployment and administration even easier than before, while at the same time increasing the core capabilities of the product. Main highlights of the release include:

- With the ability to handle up to 15,000 devices from a single appliance, the number of appliances required to handle a large network is reduced, allowing a further reduction in maintenance and administration costs. When used as an aggregator, information about up to 100,000 devices can be aggregated on a single large appliance. In Basic Discovery mode, a single large appliance can store information for 60,000 devices.

- In order to address the need of global enterprises where information may be discovered in many languages including non-ASCII ones like Japanese and Greek, this version of Network Discovery introduces support for handling all data in UTF-8 format. The result is that data discovered will be stored and displayed correctly, irrespective of the language.

- As part of an ongoing effort to ensure that Network Discovery can run on hardware from your preferred vendor, allowing you to take advantage of standardization and pre-negotiated discounts, Network Discovery 5.2 adds the HP DL360 and HP DL380 platforms to the list of hardware platforms from IBM and Dell supported by previous versions.

The following sections of this document contains a detailed description of all of the new capabilities in this version as well as a list of known and corrected issues and information on how to upgrade from an earlier version.

Terminology

Appliance size

In previous releases, the Peregrine appliance was available in Large and Small versions. With the addition of new hardware platforms, the appliance is now available in Small, Medium, and Large versions. See the *Setup Guide* for more information.

Note: The new platforms available are the "Large" versions, making the previously available platforms "Small" and "Medium."

The recommended values for each appliance size is in the following table:

	Small Appliance 1 CPU, 1GB RAM	Medium Appliance 2 CPUs*, 2GB RAM	Large Appliance 2 CPUs†, 4GB RAM
Regular Appliance			
Devices	4,000	8,000	15,000
Ports	24,000	48,000	90,000
Attributes	560,000	1,120,000	2,100,000
Aggregator Appliance			
Devices	20,000	50,000	100,000
Ports	120,000	300,000	600,000
Attributes	2,800,000	7,000,000	14,000,000
Appliances	10	20	50

* This could be 2 CPUs, or one physical CPU which is equivalent to 2 logical CPUs.
† The large appliance has 2 physical CPUs, which is equivalent to 4 logical CPUs.

There is a new license option: Basic Discovery. If you are using your Peregrine appliance in this mode, the number of devices (scan files) change considerably. For more information on Basic Discovery licenses, see the *Setup Guide.*

The recommended values for each appliance size is in the following table:

	Small Appliance 1 CPU, 1GB RAM	Medium Appliance* 2 CPUs, 2GB RAM	Large Appliance 2 CPUs, 4GB RAM
Devices	20,000	40,000	60,000
Ports	120,000	240,000	360,000
Attributes	20,000	40,000	60,000

  * In order to support 40,000 devices on the Medium appliance, you must have 73GB disks.

Important: If you are using the Desktop Inventory delta scanning feature, the amount of disk space required for scan files doubles because both the enriched scan and the original scan are kept. On appliances where disk space may be fully used, the number of devices to be managed may need to be reduced by half. For example, a large appliance may only be able to support 30,000 devices. Peregrine estimates that an average scan file would be 270 KB.

Reports Database

The Aggregate Database has been renamed the **Reports Database**.

Two of the sub-databases have been renamed:

- Network Inventory (formerly the Network Configuration database)
- Workstation Inventory (formerly the Workstation Configuration database)

For more information, see *Reports Database* on page 16.

Event Filter menu

In the Event Filters menu, there was some inconsistency in the terminology. This has been fixed so that there are only references to "devices" and "lines."

Also, the "Connection" event has been renamed "Moves" to make it consistent with other Network Discovery features.

Port Manager

In the Diagnostics panel, the term "last changed" has been changed to "last moved" to make it consistent with other Network Discovery features.

Logical CPUs

In previous versions, the Network Discovery software and documentation discussed "virtual CPUs." To be consistent with Desktop Inventory, the term "logical CPUs" is used instead.

Peregrine Support

In previous versions, you would allow Peregrine access from 209.167.240.9 (sprocket.loran.com) if you wanted to have customer support access your appliance over the internet. The DNS name has changed to ottongw.peregrine.com. The IP address is the same.

New Features and Visible Improvements

This section has been divided into the following categories:

Hardware Support

Network Discovery 5.2 can be installed on an HP DL360/DL380 server. See the *Setup Guide* for more specific requirements.

How Network Discovery works

There have been a few changes to how the product operates. These changes can be seen throughout the product.

Internal Character Set

The internal character set used to store data is now UTF-8, instead of Latin-1. All web pages and e-mail messages are now generated in UTF-8.

When upgrading, all Latin-1 data in the database will be converted to UTF-8 format. Extended characters (such as Japanese characters) can now be shown on the Network Map and in the Device Manager, Line Manager, Port Manager, and Attribute Manager.

Cisco port labels

There are new port labels for Cisco devices. The new labels can be seen throughout the Network Discovery user interface (Device Manager, Port Manager, Network Map, Alarms Viewer, etc.).

In previous versions, these ports were numbered like all devices (1, 2, 3, etc.). Now, the Cisco naming convention is displayed (for example, "Tu1" for Tunnel 1, or "Fa0/1" for Fast Ethernet 1).

Note: When you upgrade to 5.2, you should wait for a model update in order for the new port labels to be displayed.

Note: You will not lose any port statistics upon upgrading, as only the displayed port label has changed.

New recorded events

There are new events in Network Discovery 5.2:

- All SNMP Set operations done through the appliance are now logged. The new information can be seen in the Events Browser by Admin users.
- When a user logs on or off the Peregrine appliance, it is logged. The new information can be seen in the Events Browser by Admin users.

Note: The maximum number of events stored by Network Discovery has not changed, so fewer network events are stored.

For more information, see the *User Guide*.

New alarm type

Not recently seen devices are now in two categories:

- Scan not recently seen (for devices scanned with Desktop Inventory)
- Network not recently seen (for devices discovered by Network Discovery)

Detecting break faults

In previous versions, Network Discovery would need to be running for at least 24 hours before detecting broken devices in your network. Also, any device had to be seen by the network mapper for at least 24 hours before it could be seen as "broken."

This has been improved, so breaks can be detected even faster, normally within 2 poll cycles of the device being added to the map.

Disaster Recovery License

You can get a disaster recovery license in case your appliance breaks, allowing you to have a standby appliance ready to go. This license will allow you to restore your backup data to a standby appliance. Then, you will be able to use the standby appliance for up to 30 days, while your broken appliance is being repaired.

For more information, see the *Setup Guide*.

Basic Discovery License

Basic Discovery means that Network Discovery will only discover devices on your network. Network Discovery will not monitor those devices.

See the *Setup Guide* and inline help for more information.

Replacing devices in your network

Previous to version 5.1.2, it was likely that your device models would merge if you replaced one device with another, but used the same IP address. You had to manually purge the old device to avoid this. Starting in version 5.1.2, the old device is automatically deactivated, so the new device will have a unique device model.

In version 5.2, when this happens, a new Duplicate IP exception may be recorded. The device will appear in the list at **Status** > **Deactivated Devices**, with the explanation "Duplicate IP."

Using Cisco Discovery Protocol to enhance the discovery process

If Network Discovery cannot access the SNMP information on a device, then Network Discovery will consider the device to be "unmanaged".

If that "unmanaged" Cisco device is connected to another Cisco device that is managed, and the two devices communicate with the Cisco Discovery Protocol (CDP), Network Discovery can obtain some basic information about the "unmanaged" device.

By accessing the CDP information, Network Discovery may be able to assign a more appropriate name and icon to the "unmanaged" device.

"Prime" configuration backups

In previous versions, Network Discovery saved backups of the Prime map configuration for 1 year. Now, the backups are saved for only 4 weeks, to save on disk (backup) space.

Deactivated Devices

In previous versions, you would see property change events in the Events Browser, if someone made a change to a deactivated device (icon, title, tag, priority). This is no longer the case.

Device Model Merging based on NetBIOS Name and NetBIOS Workgroup

In previous versions, Network Discovery merged device models based on MAC and IP addresses. Now, device models can be merged based on NetBIOS Name and NetBIOS Workgroup before trying MAC and IP address. For example, if a laptop changes between built-in ethernet, a docking station and a wireless card, Network Discovery can track the same laptop as its MAC address changes.

Reports Database

There have been several changes to the Reports Database (formerly known as the Aggregate Database).

In previous versions, the dates in the Reports Database Events table were stored in Unixtime. This has been changed so the date is now stored in a date/time field.

In previous versions, the nonvisible ports were not in the Aggregate Port table. Now, if the nonvisible ports have a MAC or IP address associated with them, they will appear in the Reports Database.

Users can now manually refresh their local portion of the Reports Database on demand at **Status** > **Aggregate appliance health**. On a regular appliance (not an aggregator), users can do the same function through **Administration** > **Data Management** > **Update reports database**.

The following tables have been added to the Database Schema:

- AttributeGroupStateSummary
- AttributeRefreshSchedule
- ConnectionEvent
- DBVersion
- ReportStateSummary
- VLan
- VLanObject

The following columns have been added to the Database Schema:

- Appliance.Appliance_DevicesToImport
- Attribute.Attribute_TrashUnixTimeStamp
- Device.Device_LastScanTimeStamp
- Device.Device_LastSeenTimeStamp
- Device.Device_ListenerOperatingSystem
- Device.Device_ListenerPortNumber
- Device.Device_ListenerVersion
- RefreshRate.RefreshRate_ExcludedPeriods
- SWSubComponent.SWSubComponent_LastAccessTimeStamp

The following columns have been changed in the Database Schema:

- Appliance.Appliance_IPv4Address column to Appliance.Appliance_IPAddress
- Event.Event_UnixTimeStamp column to Event.Event_TimeStamp

The following columns have been updated to use the Local Appliance Time instead of the Remote Appliance Time (which is helpful when two appliances are in different time zones):

- Attribute.Attribute_UpdatedDt
- AttributeState.AttributeState_UpdatedDt;Device.Device_FirstFoundDt
- Connection.Connection_LastChangedDt
- Device.Device_UpdatedDt
- Event.Event_TimeStamp
- EventSummary.EventSummary_UpdatedDt
- HourlySummary.HourlySummary_TimeStamp
- HourlySummary.HourlySummary_PeakTime

Also, there have been many changes to the fields in the Desktop Inventory schema, which are also in the Reports Database. For a complete list of these fields, see *Data Collected by the Scanners* in your Desktop Inventory Help menu.

Console Interface

There are two new commands in the console interface:

Command	Explanation
Restore from internal backup	If you have trouble accessing Network Discovery, and need to perform an internal restore, you can now do that from the console interface.
Create temporary account to reset administration password	If the Administrator becomes locked out, and cannot access Network Discovery, he/she can now access Network Discovery through the console interface and create a special account called "lostpassword." This account will allow temporary access to the Network Discovery user interface, so the Administrator can reset his/her password.
	Note: This account will not appear in the list at **Administration** > **Account administration** > **List accounts**.

Home Page

Network Availability graphs are now visible on the Network Discovery Home page. The y-axis of the graphs show only 80-100%. If you want to see the full graphs, open the Device Manager for the Peregrine appliance.

Note: This is not available on Aggregator appliances.

Administration Menu

Aggregator - Remote Appliance Administration

When adding a remote appliance to your aggregator configuration, you can enter an IP address or a DNS name. If you enter a DNS name, it will automatically be converted into an IP address.

In previous versions, you could only enter the IP address.

Write Community Strings

In previous versions, it was not possible to omit the write community string for the Peregrine appliance. Now, can leave the write community string blank. This will disable SNMP Set operations to the Peregrine appliance.

Appliance Administrator E-mail Address

In previous versions, you would have to enter an e-mail address at **Administration** > **Appliance management** > **Appliance administrator e-mail address** in order for Network Discovery to generate any e-mail messages. This functionality has been changed, this field is now optional.

If you do not enter an Administrator e-mail address, e-mails generated by the appliance will have the following "sender" information:

From: Network Discovery at Unknown
<email.address.not.configured@Network.Discovery>

Update Reports Database

This new feature is on the **Administration** > **Data Management** page. In previous versions, the Reports database was only updated once a day. Now, with this new feature, you can update the database whenever you need to.

Send Inventory

This new feature is on the **Administration** > **Data Management** page. You can use this feature to send a series of Add events that will populate the ServiceCenter database with your entire Network Discovery inventory. This is an alternate mechanism to using a Connect-It scenario.

Account Administration

Account names

In previous versions, the maximum number of characters for an account name was 20. This has been reduced to 16 characters due to a limit it the account length for ODBC access.

Note: When upgrading to Network Discovery 5.2, accounts with more than 16 characters will not be removed, but those accounts will not have ODBC access.

There were many account names that were reserved for internal use only. Most of these have been removed, and now the only reserved account names for Network Discovery are "root" and "lostpassword."

Scanner Account

There is a new "Scanner" account type. This account is exclusively used to receive scan files from Desktop Inventory.

If you will be using delta scanning, and transmitting your scan files over HTTP, you will need to setup a Scanner account on the Peregrine appliance. For more information, see *Using Network Discovery with Desktop Inventory and Desktop Administration*.

Account Properties and Capabilities

Account properties have been split into two: Account capabilities and Account properties.

There are new options under Account Properties:

- Default Device Manager statistic
- Default Port Manager statistic
- Default statistic interval
- Default statistic maximum
- Default statistic granularity

Failed Login Attempts

There is a new option so an Administrator can set how many failed login attempts can be recorded by Network Discovery before an account is locked out. If a user account has been locked out, the only way for that account to access Network Discovery again, is to have the Administrator reset the user's password.

Password History

There are two new options:

- Password history
- Delete password history

The password history records all of the passwords used by an account, so that account cannot reuse the passwords. If you use the "Delete password history" feature, you can delete those used passwords, so an account can reuse an old password.

Network Configuration

Users can now import their IPv4 ranges from a CSV file, using the **Administration** > **Network Configuration** > **Import IPv4** ranges command. You can also export your IPv4 ranges to a CSV file by using the **CSV Export** link on the **Network Configuration** page.

System Preferences

Basic Discovery

In previous versions, this feature (**Administration** > **System preferences** > **Appliance services** > **Force Basic Discovery mode**) was called **Network management features disabled**. It has been renamed and the default has been inverted to make consistent terminology.

The default setting is to have **Basic Discovery** turned off (No).

Note: This option is not needed if you have purchased a Basic Discovery license.

Token Ring is active in the network

By turning on the "Token Ring is active in the network" feature (**Administration** > **System preferences** > **Network devices**), Network Discovery will consider non-canonical MAC address formats when mapping your network. This helps Network Discovery create only one device model for every Token Ring device when both Token Ring and Ethernet are mixed in the same network.

Read VLAN tables where appropriate

By turning off the "Read VLAN tables where appropriate" feature (**Administration** > **System preferences** > **Network devices**), Network Discovery will not read VLAN tables in your network devices.

Some devices are configured with default VLANs. In these cases, Network Discovery may trigger traps and fill the device's log files. If you have network devices with default VLANs, you may want to change this setting to "No."

Warning: If you turn this feature off, you should expect to see poor connectivity on the Network Map.

Attribute Export Schedule

There is a new feature (**Administration** > **System preferences** > **Attribute Export Schedule**) so the user can trigger when attribute data should be exported to the Reports Database.

SNMP Character Set

There is a new feature (**Administration** > **System Preferences** > **Network Devices** > **SNMP Character Set**) that allows the user to select the type of characters to expect in the SNMP data from network devices.

By default, Network Discovery will interpret SNMP data as UTF-8. In previous versions, it was interpreted as ISO-Latin-1 (ISO-8859-1). Change this option to revert to the previous behavior.

AutoSequence Number

The AutoSequence Number commands will help you assign an automatically generated number to your scan files. If you enable this function, each new scan file will be given a "hardware" field that will contain this number (**Administration** > **System Preferences** > **Scanned devices**). See the Desktop Inventory *Scanner Generator* documentation for more information.

Orphaned Scan Files

Orphaned scan files are scan files that are no longer associated with a network device. By default, these orphaned scan files will be automatically deleted. If you wish, you can change the setting so the files will be saved (**Administration** > **System Preferences** > **Scan file management**).

Group Processed Scan Files

The Processed Scan File Grouping commands will help you organize your scan files in the processed directory (**Administration** > **System Preferences** > **Scan file management**).

Event Filters

In previous versions, when creating a new event filter, priority 4 was preselected by default. Now, priorities 4, 5 and 6 are pre-selected.

In previous versions, the suffix of "device" or "line" did not appear when choosing the name of an event filter for deletion. This has been fixed.

ServiceCenter Configuration

There are two new features (Administration > System Preferences > ServiceCenter configuration) to help you integrate with ServiceCenter 6:

- Web Tier Host Name
- Web Tier Port

When you set up Host and Port access, you will be able to access ServiceCenter directly by clicking on ticket numbers in the Network Discovery user interface.

Expiry

There is a new level of expiry: Obliteration. If there is space in your license, Network Discovery will keep a record of purged devices until the obliteration interval passes, at which point the device and all associated data will be permanently deleted.

Note: This applies only to the Reports Database.

Number of Explorer Pings

Added support to control the maximum number of explorer pings sent to an IP address (see **Administration** > **System preferences** > **Network devices** > **Number of Explorer Pings**).

XML Enricher

The defaults for "merge priority" have been changed in **Administration** > **System Preferences** > **Scanned Devices.**

Help Menu

In **Help** > **Classifications** > **Device types,** there is a new column to show the icon ID.

In **Help** > **Classifications** > **Hardware fields,** there is a complete list of all Desktop Inventory hardware fields.

Click **Help** > **Configuration options** to see a complete alphabetical list of configuration options and their inline help information.

Reports Menu

Improvements have been made to **Reports** > **Scanned Machine Summary**.

Under **Reports** > **Network Documentation** and **Reports** > **Aggregate Inventory,** there are new Summary and Device/Port Inventory reports for VLANs.

Status Menu

Aggregate Appliance Health

There is now information showing when your Aggregator Appliance is over its license limit.

"Total Devices" in Status Reports

Each of the following Status reports now has a number of "total devices" at the top of the report:

- modelling queue
- active devices
- filtered devices
- deactivated devices
- hidden devices
- forced connections

Deactivated Devices

A new column has been added to this table to indicate why the device was deactivated. Devices will only have this status if they have been deactivated since you installed Network Discovery 5.2.

Download Directory

There is a new script available to help process delta scan files over HTTP: **deltascan.pl.** For more information, see *Using Network Discovery with Desktop Inventory and Desktop Administration.*

There is a new ODBC driver for Windows: **MyODBC-3.51.06.exe**.

There is a new Java Runtime Engine: **j2re-1_4_2_03-windows-i586-p.exe**.

There are new **manager.exe** and **agent.exe** files. The Peregrine Agent has been improved to ensure that all associated security keys are properly removed when it is uninstalled.

Network Map

Update Model

There are three new options in the Update Model menu:

- Configure Scanner (was previously called Run Scanner)
- Run Scanner (which no longer runs the configuration step)
- Enrich XML

Also, the **Retrieve FSF** command has been renamed **Retrieve Scan File.**

It is now possible to perform Update Model functions on multiple devices on the network map. Select the devices, and then click **Object** > **Update Model**.

Visibility

It is now possible to perform Visibility functions (Activate, Deactivate, Hide, Purge) on multiple devices on the Network Map. Select the devices, and then click **Object** > **Visibility**.

Map pop-ups

The pop-ups that appear when you put the cursor over a device icon has changed. The pop-up will now show all ServiceCenter tickets associated with that device, rather than just the tickets associated with the currently selected alarm category.

Port numbers (for real and virtual ports) are now shown in the map pop-up window when the cursor hovers over a line. The pop-up displays port information for the end of the line nearer the mouse, or with the SHIFT key pressed, it displays port information for the end of the line farther from the cursor.

Device Titles

Device titles on the map are now truncated according to the amount of available space, rather than by the number of characters.

Revert

In the Network Map, you can now revert (**File** > **Revert**) your map changes to the point at which you last saved the map configuration.

Save Map Image

You can now save your Network Map window as a jpg or png image file (**File** > **Save Map Image**).

Background Images

The Network Map can now have a background image for each package. This allows you to visually identify where your packages are located (**Configure** > **Background Image**).

Important: You can add your own background images to the image library. If you add images that are larger than 250KB, you may notice the Network Map scrolling slowly.

Alarm-Type Pull-down list

The look of this list has been changed. There is now an alarm state icon associated with each alarm category, representing the highest alarm state for that category in your network.

Configure Menu

There is a new menu in the Network Map, called **Configure**. This menu contains commands relating to layout, packaging, and the look of your map window.

Show All Ports

This command appears in the Configure menu, and when you right-click on a device in the Network Map. When you select **Show All Ports**, a window will appear, showing a list of all the ports on that device, and their connectivity.

Right-click menu on lines

When you double-click on a line, you will automatically open a Line Manager. You can right-click on a line to see other options:

- Open Port (opens the port to which you are closest when you click the line)
- Open Line (opens the Line Manager)
- Open Multiline (opens the Multiple Line Manager)
- Browse Port Events (opens the Events Browser, with this port in context)
- Port Properties (opens the Port Properties dialog)

Promote All

In previous versions, there was an **Unpack** command. This command has been renamed **Promote All** and is under the **Configure** menu.

Device Properties

In previous versions, there were two ways of changing device properties: **My User Properties**, and **System Properties**. **My User Properties** has been removed, and now only Administrator and IT Manager accounts can make changes to the device properties (icon, tag, title, and priority).

Important: If you have accounts that have made changes to **My User Properties**, those changes will be lost when you upgrade to Network Discovery 5.2.

Scale Slider

The slider now has a right-click menu, featuring commands that were previously available on the Network Map:

- Zoom In
- Zoom Out
- Scale to fit Width
- Scale to fit Height
- Scale to 100%

There are two new keyboard shortcuts. To **Zoom In**, press **Ctrl** - (dash). To **Zoom Out**, press **Ctrl** = (equal sign).

Note: If you are using a Japanese keyboard, you can use **Ctrl Shift** - (dash) to **Zoom Out**.

In previous versions, the slider would shrink when the map window was reduced in size. This has been fixed, so when the window is reduced, the slider is hidden.

DNS Query and Listener Ping

These commands now appear in the **Object** > **Diagnosis** menu, and when you right-click on a device, in the **Diagnosis** sub-menu.

Clouds with manual connections

In previous versions, sometimes a cloud icon set by the user would revert to the default when there had been some connectivity changes. This has been fixed. The icon you have selected for the cloud will now remain even if you change its connection information.

Command Confirmation Dialogs

Several commands (such as Visibility commands, Update Model, and Save As Prime) had an "OK" confirmation dialog appear when the command had been run successfully. These have been removed.

Health Panel

You can now use the **File** > **Save Table Data** feature to save selected info into a text file. If you want to select the entire table, click **Edit** > **Select Table**.

Find and Aggregate Find

The Find feature has been rewritten as a Java applet. It works similarly to the old Find feature, but is much easier to use. Some of the terminology has been changed, and some new options have been added:

	Regular Find	Aggregate Find
Easy Find*	✔	—
Device Title	✔	✔
IP Address	✔	✔
MAC Address	✔	✔
Asset Tag	✔	✔
Domain Name*	✔	✔
NetBIOS Name	✔	✔
NetBIOS Workgroup*	✔	✔
Ticket (ServiceCenter Ticket number)*	✔	—
Family	✔	✔
Model	✔	✔
Operating System	✔	✔
Network Function† (in previous versions, this was called "Application")	✔	✔
SNMP Description	✔	✔
SNMP Contact	✔	✔
SNMP Name	✔	✔
SNMP Location	✔	✔
SNMP Serial Number*	✔	✔

	Regular Find	Aggregate Find
DNS Query*	✔	—
NetBIOS Query*	✔	—

  * New in 5.2.
  † Changed in 5.2.

In previous versions, you could Find a specific port. That functionality has change to a new command on the Network Map Object menu, called **Show All Ports.**

Note: If an IP or MAC address is associated with a port, you will see a port listed in your Find results.

Also, there is a new Aggregate Find feature, that lets the user search for devices on all aggregated appliances.

MIB Browser

There are two new features in the MIB Browser.

- **Open Walk** allows you to save all or part of a device MIB to a text file.
- **Save Table Data** allows you to save a particular table from the MIB to a text file.

The MIB Radar feature has been improved, so you can change the refresh rate and view the radar history.

Alarms Viewer

The columns displayed in the Alarms Viewer will be different depending on the alarm type you have chosen.

ServiceCenter ticket numbers now appear in the Alarms Viewer. If you have configured the ServiceCenter access options (**Administration** > **System preferences** > **ServiceCenter configuration**), you can right-click on the ticket number and click **Open Ticket** to access ServiceCenter.

You can now use the **File** > **Save Table Data** feature to save selected info into a text file. If you want to select the entire table, click **Edit** > **Select Table.**

Events Browser

You can now use the **File** > **Save Table Data** feature to save selected info into a text file. If you want to select the entire table, click **Edit** > **Select Table**.

The **Activate** command has been added to the right-click menu.

In previous versions, if you opened an Events Browser from a Device Manager, you would see all events for all devices. Now, you will initially see only events relating to that device.

ServiceCenter ticket numbers now appear in the Events Browser. If you have configured the ServiceCenter access options (**Administration** > **System preferences** > **ServiceCenter configuration**), you can right-click on the ticket number and click **Open Ticket** to access ServiceCenter.

Service Analyzer

The Service Analyzer has been redesigned. Read the section in the *User Guide* for a full description.

You can now use the **File** > **Save Table Data** feature to save selected info into a text file. If you want to select the entire table, click **Edit** > **Select Table**.

ServiceCenter ticket numbers now appear in the Service Analyzer. If you have configured the ServiceCenter access options (**Administration** > **System preferences** > **ServiceCenter configuration**), you can right-click on the ticket number and click **Open Ticket** to access ServiceCenter.

In previous versions, when you selected an alarm category in the Network Map and Health Panel, that alarm category would automatically be chosen in the Service Analyzer as well. That has been changed, so the Service Analyzer is now independent of the Network Map and Health Panel.

The Device Manager, Port Manager, Line Manager, and Attribute Manager

Break information

The format of Break alarms has been improved in the Device Manager, Attribute Manager, and Service Analyzer.

Open ServiceCenter tickets

ServiceCenter ticket numbers now appear in the Device Manager, Port Manager, and Attribute Manager. If you have configured the ServiceCenter access options (**Administration** > **System preferences** > **ServiceCenter configuration**), you can click on the ticket number to access ServiceCenter.

State Panel

The "Tickets" column has been moved to the far-right position.

Statistics Panel in the Managers

In previous versions, if you changed the port you were viewing, the statistic pull-down lists were reset to their default settings (alarm type, time period, max, and granularity). This has been changed so the user can now change the port number, but see the same statistic and time period for the new port.

Device Manager

DNS

The DNS button in the Device Manager has been improved. The output now includes an explanation for highlighted data. Also, this feature now supports IPv6.

Update Model

There are three new options in the Update Model menu:

- Configure Scanner (was previously called Run Scanner)
- Run Scanner (which no longer runs the configuration step)
- Enrich XML

Also, the **Retrieve FSF** command has been renamed **Retrieve Scan File**.

Device Structure

This new section in the Device Manager Configuration panel provides the following types of information about the entities (such as chassis, modules, and power supplies) in a device, if they are reported by the SNMP agent.

- Type of the entity -- it can be anyone of: other, unknown, chassis, backplane, container, powerSupply, fan, sensor, module, port, stack, and misc.
- Manufacturer defined product Name of the entity.
- Hardware revision.

- Firmware revision.
- Software revision.
- Serial Number of the entity.
- Manufacturer defined Model Description/Name of the entity.

Viewer

This is only available if you are using Desktop Inventory with Network Discovery.

When setting up accounts (**Administration** > **Account administration** > **Account properties**), you can configure whether the user opens the Viewer, or if they download the scan file (in **.xsf** format).

Port Manager

There is now autonegotiation data available on the Configuration panel.

VLAN

VLAN information is now shown in the Configuration panel of the Port Manager and Device Manager.

VLANs are software-defined broadcast domains, created by your System Administrator at the switch. By showing VLAN information in Network Discovery, the Administrator can see how the devices in that virtual domain are functioning.

Multiple Line Manager

The Multiple Line Manager has been redesigned, and now looks similar to the Service Analyzer.

Compatibility with other Peregrine products

This is an overview of Network Discovery's compatibility with other Peregrine products. For more information, see the *Compatibility Matrix* in the *Setup Guide*.

With Desktop Inventory

Network Discovery 5.2 can work with Desktop Inventory 8.0 (or with scanners from 7.3).

If you have a new Network Discovery 5.2 installation, the default setting will be to work with scanners from Desktop Inventory 8.0. If you upgrade to Network Discovery 5.2, the default setting will be to work with scanners from Desktop Inventory 7.3. You can change the setting at **Administration** > **System preferences** > **Scanner version**.

Desktop Inventory 8.0 has the capability to save scan files to the appliance over HTTP. Network Discovery has a new account type to support this (see **Administration** > **Account administration**).

With Desktop Administration

Network Discovery 5.2 can work with Peregrine Desktop Administration, but it must be version 6.0 or higher.

With Connect-It

Network Discovery 5.2 can work with Connect-It 3.2.2, which supports UTF-8. Users will find the latest Network Discovery scenario in their Connect-It 3.2.2 software.

New Commands and Moved Commands

Administration Menus

New Commands

Location	Command
Administration > Account administration	■ Account capabilities
Administration > Account administration > Appliance passwords	■ Maximum number of failed login attempts ■ Password history ■ Delete password history
Administration > Network Configuration	■ Import IPv4 ranges ■ CSV Export
Administration > System Preferences	■ Scanner version
Administration > System Preferences > Network Devices	■ SNMP Character Set ■ Number of Explorer Pings ■ Token Ring is active in the network ■ Read VLAN tables where appropriate
Administration > System Preferences > Scanned Devices	■ AutoSequence Number
Administration > System Preferences > Scan File Management	■ Orphaned Scan Files ■ Group Processed Scan Files
Administration > System Preferences > Expiry	■ Device Obliteration Interval
Administration > System Preferences > Report Time Periods	■ Time for Scan Not Recently Seen
Administration > System Preferences > ServiceCenter Configuration	■ Web tier host name or IP address ■ Web tier port
Administration > System Preferences	■ Attribute Export Schedule
Administration > Data management	■ Update report database ■ Send Inventory

Moved Commands

Pre-5.2 location	New location
Administration > ServiceCenter Configuration > ServiceCenter settings	Administration > System preferences > ServiceCenter configuration
Administration > ServiceCenter Configuration > ServiceCenter settings > Appliance ID	Administration > System preferences > Aggregate configuration > Appliance ID
Administration > ServiceCenter Configuration > Test ServiceCenter	Administration > Data management > Test ServiceCenter
Administration > System preferences > Appliance services > Network management features enabled	Administration > System preferences > Appliance services > Force Basic Discovery Mode

Network Map

New Commands

Location	Command
File	■ Revert ■ Save Map Image
View	■ Scale at 100% ■ Hide Background Image
Object	■ Open Device ■ Open Port ■ Open Package ■ Open Line ■ Open Multiline ■ Show All Ports ■ Device Properties ■ Port Properties ■ Package Properties
Object > Diagnosis	■ Listener Ping ■ DNS Query

Location	Command
Object > Update Model	■ Configure Scanner ■ Enrich XML
Object > Visibility	■ Activate
Configure	■ Background Image

Moved Commands

Pre-5.2 location	New location
Object > Update Model > Retrieve FSF	Object > Update Model > Retrieve Scan File
View > Layout	Configure > Layout
View > Pack	Configure > Pack
View > Unpack All	Configure > Unpack All
Object > Lock	Configure > Lock
Object > Unlock	Configure > Unlock
Object > Unpackage	Configure > Unpackage
Object > Package	Configure > Package
Object > Promote	Configure > Promote
Object > Top of Network	Configure > Top of Network
View > Unpack	Configure > Promote All

Health Panel, Events Browser, Alarms Viewer, Service Analyzer

New commands:

■ **File > Save Table Data**

■ **Edit > Select Table**

Events Browser

New commands (for Admin accounts only):

■ **View > Show Access Events**

Internal Improvements

This section has been divided into the following categories:

- *Operating System* on page 37
- *Browser Support* on page 37
- *Devices added to Network Map* on page 38
- *Appliance E-mails Improved* on page 38
- *Aggregation/Proxy Services* on page 38
- *Network Map Sessions* on page 38
- *New MIB Definitions* on page 38
- *Health Panel* on page 39
- *Peregrine Icon appearing in Mozilla and Netscape URL bar* on page 39
- *Database Changes* on page 39
- *Directory permissions* on page 39
- *Cut and Paste* on page 39
- *Disk Partitioning* on page 39

Operating System

The following improvements have been made to the OS:

- upgrade to MySQL 4.1.2
- Apache 1 has been removed; upgrade to Apache 2.0.49
- mod_perl is 1.99_14
- kernel is Linux 2.4.25
- net snmp 5.1.1

Browser Support

Now supporting Mozilla 1.4 - 1.7.

Devices added to Network Map

Network Discovery adds devices to the database and Network Map much faster than in previous versions. When a device responds to a discovery ping (and only a discovery ping), the device is immediately added to the database, and will show up on the map as an IP-only device. The device icon will change as Network Discovery learns more about the device, and updates the device model.

If you would prefer to see the previous behavior, you can use the "Passive Discovery" Network Property Group in **Administration** > **Network configuration** > **Network property groups**, or you can filter IP-only devices.

Appliance E-mails Improved

E-mails generated by the Peregrine appliance will now contain the date and time (and correct time zone) of the appliance. E-mails will no longer show the date in UTC.

Aggregation/Proxy Services

Aggregation and proxy services now work over IPv6.

Network Map Sessions

On medium and large Peregrine appliances (see the *Setup Guide*), the number of available Network Map sessions has been increased to 10.

New MIB Definitions

The following MIB definitions were added:

- INET-ADDRESS-MIB
- NET-SNMP-MIB
- NET-SNMP-TC
- NET-SNMP-AGENT-MIB
- NET-SNMP-MONITOR-MIB
- NET-SNMP-SYSTEM-MIB
- NET-SNMP-EXAMPLES-MIB

- RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions
- RFC 2737 Entity MIB (Version 2)

Health Panel

The Health Panel refresh has been improved and refreshed much faster than in previous versions.

Peregrine Icon appearing in Mozilla and Netscape URL bar

Now, in Mozilla and Netscape 7, you will always see a small Peregrine Systems icon in the URL bar.

Database Changes

The separators between labels in the Network Discovery database has been changed from a straight line (i.e., "|") to a greater-than symbol (i.e., ">").

Directory permissions

In previous versions, if the user deleted a directory in the share, the XML Enricher would recreate the directory with incorrect permissions.

The internal permissions have been changed, so none of the directories in the share can be deleted or moved.

Cut and Paste

There are several places in the UI where you can use keyboard shortcuts to copy data (**Ctrl-C**) and paste it into another application (**Ctrl-V**). You can now also use **Ctrl-Ins** and **Shift-Ins** to cut and paste data from the UI.

Disk Partitioning

The Network Discovery installer has changed how it formats disks. Previously the active and backup partitions were split approximately 60/40. Now the split is approximately 50/50. If you are upgrading from 5.1 to 5.2, your disk partitions will remain unchanged. If you want the new partition scheme, backup your data, reformat the server then re-install. The new partitions are required if you have many or large scan files.

Dropped Functionality

WMI Collector

The WMI Collector is no longer supported since it is no longer included with ServiceCenter.

Device Properties

In previous versions, any user could change the device title and priority for their own account. Now there is only one title and priority visible for all accounts, and it is controlled by Admin and IT Manager accounts.

Host MIB for Windows NT

The Peregrine Host MIB for Windows NT has been removed from the Download directory. This functionality is included in Windows 2000 and later.

Port Find

The Find feature has been changed. You can only find devices, not specific ports.

The **Object** menu for devices contains a new command to replace this feature: **Show All Ports**.

Known issues

Workgroup

In some cases, the appliance will not show up in the Windows "network neighborhood" using the configured workgroup. It may not show up at all.

Use the IP address of the appliance to access the share.

Time zone change after restore

If a backup contains a time zone different from the time zone on the appliance, restart the appliance after restoring the backup. Alternatively, change the time zone of the appliance to the time zone of the backup before you do the restore.

USB Connected UPS

If the UPS is connected to the Peregrine appliance through USB to serial converter and you disconnect the USB to serial converter from the appliance, you must restart the appliance for the UPS to be re-recognized.

Some tape drives do not work

There are some USB tape drives that do not work with the Peregrine appliance.

We have reports of the Sony and LaCie AIT USB tape drives working well, while the Seagate Travan USB tape drives have had problems. The OnStream ADR USB tape drives are not supported at this time.

New Data for some New Interface Elements

Many of the new user interface elements require new data to be collected. If you are upgrading from 5.0 or 5.1, you may find some data elements missing or incorrect until such time as either:

- two poll cycles have passed
  - state of the attribute in the Device Manager, Port Manager, and Attribute Manager.
- the device model is updated

- Cisco port labels
- priority of deactivated devices
- title of deactivated devices
- icon of deactivate devices
- the attribute state changes
  - the "time since" shown in the mouse-over of the attribute state icon (and the State Time column) shows the time of the upgrade, not the time of the state change.
- the reports database updated
  - empty columns in the database including Package and FullyQualifiedPackage

Note: Please let your new version run at least 24 hours before reporting problems to Customer Support.

Time of Adds/Not Recently Seen/Moves

If you are upgrading from 5.0, the time for your Add/Not Recently Seen/Move events are not preserved. Set the new value in **Administration** > **System Preferences** > **Report Time Periods.**

Upgrading with an Aggregator

The aggregator is not compatible with versions previous to 5.2. Upgrade the aggregator first then all the other appliances in quick succession.

Due to the database changes, please let your new version run at least 24 hours to catch up on missing data before reporting problems to Customer Support.

Hardware Upgrade every 2-3 years

Every new major and minor release of Network Discovery adds new features, extending the software functionality to meet our customers' needs. These additional enhancements may introduce new demands on the original hardware, subsequently impacting performance. Customers employing older platforms may find that this release performs a little more slowly than the previous release.

Customers should be prepared to upgrade their Network Discovery appliance every 2-3 years to maintain optimal performance, as they would other enterprise application servers.

If upgrading from Network Discovery 5.0 or 5.1, note that the hardware recommendations have changed. Previously, a small appliance could monitor 5,000 devices, and a large appliance could monitor 10,000. Currently, for Network Discovery 5.2, a small appliance can handle 4,000 devices, a medium appliance can handle 8,000 devices, and a large appliance can handle 16,000 devices. See the *Setup Guide* for specific information.

Customers with 5,000 devices on a hardware platform where now only 4,000 are recommended may notice performance problems. If so, they should add more RAM and/or another CPU. Similar problems may occur if you have 10,000 devices on a hardware platform where 8,000 is now recommended.

Integrating with ServiceCenter

To integrate Peregrine Network Discovery with ServiceCenter 5.1 using event services, you must modify your existing ServiceCenter configuration. Refer to Knowledge Base article S9K-41P-RRD3 for instructions describing how to perform the required upgrade.

Note: ServiceCenter 5.1 does not support UTF-8 characters. If you need to use non-English characters, you should upgrade to ServiceCenter 6.

UNIX Listeners

Network Discovery does not include UNIX Listeners.

UTF-8 Character Set

Using Windows 2000

When using Microsoft Windows 2000, if you are using non-English characters (for example, Chinese), ensure that you have changed the default language setting in Windows to that language. Otherwise, device tags and titles will appear incorrectly.

Exporting CSV files

Microsoft Office 2003 does not properly process UTF-8 encoded CSV files. If you are using Network Discovery data with Microsoft Office applications, you should follow this procedure:

Step 1 When downloading your file from Network Discovery, save the file to disk.

Step 2 Open Microsoft Excel 2003 (or other Microsoft product), and use the **File > Open** command to import the files.

Device tags, titles, and configuration files

Because some non-English UTF-8 characters are larger than one byte each, using non-English characters may require you to use shorter names for your device tags, device titles, and map configuration files.

Network Discovery supports up to 16 bytes for device tags, 80 bytes for device titles, and 30 bytes for map configuration file names.

E-mail messages

In Microsoft Outlook, UTF-8 characters in an e-mail subject line are not displayed properly. If you need to see these characters, they are displayed properly in Mozilla.

Cursor in Editable Fields

When using non-English characters (for example, Chinese or Japanese), you will notice that the cursor does not align properly between the characters. This is a Java issue.

IP Range Viewer

Some UTF-8 characters are not displayed in the IP Range Viewer (**Administration > Network configuration > List IPv4 ranges > IP Range Viewer** [**diagram**]). Small squares will appear in place of the UTF-8 characters.

Asset Viewer

When using the Java Asset Viewer with Internet Explorer, non-English characters will be displayed as "?" (question marks) in the window's title bar.

Access Logging

Network Discovery does not log access for ODBC or MySQL connections in the Access section of the Events Browser.

Synchronizing Data on Aggregate Health Panel

The data on your Aggregate Health Panel may not be synchronized with the data on the Health Panel of your remote appliances. Data transfers from the remote appliances to the aggregator once an hour, so there may be up to a 1-hour delay for some alarms to appear on the Aggregate Health Panel.

HP DL360/DL380 does not have disk I/O information

The HP DL360/DL380 comes with two disks. The second disk cannot provide I/O data.

Automatic reconnect

If the appliance becomes unreachable, you may not see a Connect dialog for the Health Panel. When the appliance is reachable again, your Health Panel freezes, and the indicator at the bottom right corner stays active.

To resolve this situation, you must close all the Network Discovery windows you have opened, as well as the main Toolbar, and start again.

Find

If you search on an IP address, you will always see the IP in the results list, even if the IP address does not exist in the Network Discovery database. There is no visual indication to show that the address does not exist in the database.

Corrections

The following table contains corrected issues from the previous release of Network Discovery. For further updates see the Customer Support web site at http://support.peregrine.com.

SCR #	What's affected	Description
2360	Device Manager and Port Manager	The Properties button will be greyed out if the device is not in the Network Discovery database.
3479	Prime map configuration	The Prime map configuration is now automatically saved every day. This will ensure consistency between the devices appearing on the map, and Reports data.
10141	Backup Files	In previous versions, a backup would produce a fatal error if the filename used non-supported characters. The appliance would require a restart in order to attempt another backup. This has been fixed, so that if an error occurs, the appliance does not need a restart, and you can try to save the backup again with a supported name.
10575	Device Manager/View Scan button	In previous versions, the **View Scan** button might be enabled even if the scan file was not in the correct location (the "processed" directory).
10871	Backup Files	In previous versions, the characters %g and %G were not creating the expected date format in the backup files. This has been corrected.
11007	Break information	In previous versions, there some inconsistent terminology in the Device Manager with respect to Break alarms.
11107	**Administration** > **My map configurations**	In previous versions, if you saved a map configuration with the same name as another map configuration, Network Discovery would overwrite the existing file. This has been fixed, and now you will see an error message, so you can change the file name accordingly.
11109	**Reports** > **Scanned Machine Summaries** > **Summary by Operating System Category**	In previous versions, an SQL error would affect the display of the "All" report.

SCR #	What's affected	Description
11203	Network Map (when disconnected)	In previous versions, you might have had difficulty opening a Network Map session if you have been disconnected, and the connection again became available. You might have seen a warning saying that your account is already logged in, and the map would then close. Now, the map stays open when the connection comes up again.
11220	MIB Browser	In previous versions, an invalid write community string may have appeared in the pull-down list of the MIB Browser. Now, if Network Discovery does not know a valid write community string available for that device, the pull-down list will be blank.
11225	Network Map	In previous versions, a deactivated device would have a red "X" through the icon on the Network Map. Sometimes, if a user reactivated the device, the "X" would remain until the user refreshed the Network Map. This has been fixed, so when a device is reactivated by the user, the red "X" disappears immediately.
11293	Internet Explorer	A possible upcoming change to how Internet Explorer functions will cause a confirmation dialog (telling the user to "Press OK to continue loading the contents of this page") whenever a user loads Network Discovery's Java applet (the Toolbar). This has been fixed in Network Discovery, so the confirmation dialog will not appear. For more information, refer to the Microsoft website: http://msdn.microsoft.com/ieupdate/
11337	FTP Backup	In previous versions, when the user attempted to run and external backup they might get a warning that says "Error: backup server is currently busy."
11342	Number of mapped devices	In **Status** > **Appliance Health** > **Software environment**, you see data on License Capacity Utilization. The internal calculations to determine Mapped Devices Capacity and Mapped Ports Capacity have been fixed.
11496	**Administration** > **Router discovery**	In previous versions, there may have been an error when trying to add your Router Discovery Results to your IPv4 ranges.
11518	**Administration** > **Event filter configuration**	You can now have an empty "description" field in the event filters page.
11526	Backup and Restore	In previous versions, a manual external backup would fail if an internal backup was already running.
11542	Add events	In previous versions, some Add events were delayed for a long time.

SCR #	What's affected	Description
11589	Mozilla	When your account was enabled to highlight rows in the UI, it would not work in Mozilla.
11608	Shared directory	In previous versions, some items in the download shared directory were not accessible.
11613	**Status** > **Aggregate appliance health**	Purged devices are no longer counted when calculating the number of imported devices.
11689	**Reports** > **Aggregate Inventory**	In Aggregate Inventory reports, the name of the remote appliance (from which the Aggregator receives information) was being truncated. The maximum length of the text area has been increased to 50 characters to accommodate longer appliance names.
11772	**Administration** > **Appliance management** > **NTP server**	In previous versions, the time may have been set correctly, but there may have been an erroneous error message when you set your NTP server.
11892	Device Manager Ports panel	In previous versions, the Delays column appeared blank. This has been fixed.
11895	Reports database	The Appliance ID (from **Administration** > **System Preferences** > **Aggregate Configuration**) for the Aggregator appliance (appliance 0) now shows up in the Appliance.Appliance_ServerID field in the Reports Database.
11920	SNMP Traps	In previous versions, the current time would be used as the datetime tag when sending SNMP traps. Now, the trap uses the event time.
11948	IT Manager account	IT Manager accounts can now do SNMP set commands.
11949	Health Panel	The number of devices shown on the Health Panel now shows the "discovered devices." In previous versions, this number represented the number of devices on the Network Map.
12188	**Status** > **Appliance Health** > **Appliance hardware environment**	In previous versions, the Appliance hardware environment screen showed two "Primary Data Backup partitions." The label has been changed to show one primary, and one secondary partition.
12075	Service Analyzer	If a device is not in the database, it cannot be seen in the Service Analyzer.
12381	**Device Manager** > **Diagnosis Panel** > **Listener Ping**	If the Listener Ping function times out, you will see a information message.

SCR #	What's affected	Description
12392	**Reports Database**	The appliance IP address would not be updated in the database when a user changed the IP address in the console interface.
12398	**Administration** > **System Preferences** > **Expiry**	Automatic device expiry is disabled if no SNMP-managed models have been updated in 48 hours. Previously, this was 12 hours which was considered too short in some customer networks.

Documentation

The entire documentation set has been updated:

- *Setup Guide*
- *User Guide*
- *Reference Manual*
- *Data Export Guide*
- *Using Network Discovery with Desktop Inventory and Desktop Administration*

The product inline help has also been updated and improved.

For a complete list of current Network Discovery documentation, see the Documentation pages on the Peregrine Customer Support web site at http://support.peregrine.com. (Access to this web page requires a current login name and password.)

You can download documentation PDF files and view them using Adobe Reader, which is available on the Customer Support web site and through Adobe at http://www.adobe.com.

Internal Modem Recommendation

The Buffalo/Melco modem is deprecated.

Support for this modem will be continued through all 5.2.x maintenance releases. The next major or minor release, whichever comes first, will not support this modem. This is due to changes in the open source driver required by this modem.

Upgrade information

The upgrade information is in the following sections:

- *Upgrading from Peregrine's Network Discovery 5.0/5.0.1/5.0.2/5.1/5.1.1/ 5.1.2/5.1.3* on page 51
- *After an upgrade* on page 52

Warning: The procedure for upgrading varies depending on what version of software you are currently running because the platforms differ. If you are in any doubt, check what version you have.

To check the version of Network Discovery you are currently running

▶ See the version number at the bottom of the Toolbar.

If you have more than one appliance, check which version of Network Discovery is running on *each* appliance. Follow the correct upgrade path for each appliance separately.

Upgrading from Peregrine's Network Discovery 5.0/5.0.1/5.0.2/ 5.1/5.1.1/5.1.2/5.1.3

If you are upgrading your appliance from Network Discovery 5.0/5.0.1/5.0.2/ 5.1/5.1.1/5.1.2/5.1.3 to Network Discovery 5.2, follow this procedure.

Before the upgrade

Before you perform the upgrade, check that you are still entitled to customer support. The Network Discovery CD will not work if the appliance is out of maintenance.

To check that you are still entitled to support

1 Click **Status** > **Current Settings** > **Installed Licenses**.

2 Check the entry, "Maintenance valid until".

If your Maintenance license has expired, renew the contract and contact Peregrine Systems Customer Support for an updated license key.

If you are using Aggregation

- Check that each remote appliance is running 5.2 or later. If not, the Aggregator appliance will not read the remote appliance's data.

- check the maintenance date for each Peregrine appliance.
- Always upgrade the Aggregator appliance *first*.

Performing the upgrade

Note: You can use a monitor and PS2 keyboard attached to the Peregrine appliance or you can use the management workstation to restart the Peregrine appliance through the browser interface at **Administration > Appliance Management > Appliance Restart.**

To upgrade Network Discovery software

1 Place the Network Discovery CD in the CD-ROM drive of the server and restart the server.

The system then reboots from the CD. The CD does not overwrite any newer software components that you have downloaded from the Customer Support web site. After the components have been installed, the CD ejects, and the server reboots.

2 Remove the CD, and store it in its case in a safe place.

Network Discovery is now upgraded to version 5.2.

3 If you are using a monitor attached to the Peregrine appliance, press **Enter.**

The monitor shows **Password:**. If you are using the web browser at the management workstation, Network Discovery comes back on.

If you see an error message telling you that there is a problem with the hardware, contact Peregrine Systems Customer Support.

After an upgrade

It's a good idea to check you have the latest software components from support.peregrine.com. There are instructions for checking and installing software components in the *Setup Guide.*

After you upgrade to Network Discovery 5.2, your SNMP default character set will be UTF-8. If you are using Latin-1 characters in SNMP, change the default setting in **Administration > System Preferences > Network Devices > SNMP Character Set.**

Note: When you upgrade to Network Discovery 5.2, any pending e-mails will be lost.

Upgrading Network Discovery and Desktop Inventory

When you upgrade to Network Discovery 5.2, you will notice some important changes:

- the XML Enricher will be disabled so you can install an SAI file compatible with Desktop Inventory 8.0
- your **xml.gz** files will all be converted to **.xsf** files

You should not upgrade to version 5.2 until you have built a Desktop Inventory 8.0 SAI file. Once you upgrade to Network Discovery 5.2, you should install the new SAI on the appliance.

To ensure you properly upgrade both products at once, follow these steps.

Upgrading Network Discovery and Desktop Inventory

1 If you are using Connect-It, upgrade to version 3.3.2 (or later).

2 Install Desktop Inventory 8 (separate from Desktop Inventory 7.3), but don't use it for anything in production.

3 Generate new SAI for Desktop Inventory 8 and test a sample set of files.

   Note: Your old SAI files are not compatible with Network Discovery 5.2/ Desktop Inventory 8.0. They will be automatically erased when you upgrade your software, which is why you need to create a new SAI.

4 Upgrade to Network Discovery 5.2.

5 Upgrade your ODBC driver (found in the Network Discovery **Download** directory).

6 Install your new SAI on the appliance.

7 Start using Desktop Inventory 8.

8 Change Network Discovery 5.2 to use PDI 8 scanners (**Administration** > **System preferences** > **Scanner version**).

9 (optional) Use Scanner Generator to generate new scanner configurations to take advantage of new features.

10 (optional) Update Connect-It scenarios to take advantage of new database fields.

Need further assistance?

For further information and assistance with this release or Network Discovery in general, contact Peregrine's Customer Support.

Peregrine's CenterPoint Web site

Contact information for local support offices is available through the main contacts shown below or through Peregrine's CenterPoint Web site: http://support.peregrine.com

After logging in with your login and password:

▶ Select **General Information**, on the left.

Under **Customer Support References**, select **Support Contacts Worldwide**.

Corporate Headquarters

Contact Customer Support at Peregrine headquarters using one of the following:

Address:	Peregrine Systems, Inc.
Attn:	Customer Support
	3611 Valley Centre Drive
	San Diego, CA 92130 USA
Telephone:	(1) (800) 960-9998 (US and Canada only, toll free)
	+ (1) (858) 794-7428
Fax:	+ (1) (858) 480-3928
Email:	support@peregrine.com

Contacting Education Services

Training services are available for the full spectrum of Peregrine Products including Network Discover.

Current details of our training services are available through the following main contacts or at:

http://www.peregrine.com/education

Address:	Peregrine Systems, Inc.
Attn:	Customer Support
	3611 Valley Centre Drive
	San Diego, CA 92130 USA
Telephone:	+ (1) (858) 794-5009
Fax:	+ (1) (858) 480-3928