



Guide to Using IPControl

Version 5.0



The information in this document is subject to change without notice. Names of individuals and companies, as well as data used in examples, are fictitious unless otherwise noted. No part of this document may be copied, reproduced, or electronically transmitted in any form without the express written consent of BT Diamond IP.

Adobe and Adobe Acrobat are trademarks of Adobe Systems Incorporated.

Microsoft Windows, Windows 2000, Windows 2003, Windows2008 , and Internet Explorer are trademarks or registered trademarks of

Microsoft Corporation in the U.S. and/or other countries.

MySQL is a registered trademark of Oracle Corporation.

Oracle is a registered trademark of Oracle Corporation.

Solaris is registered trademark of Oracle Corporation.

UNIX is a registered trademark of the Open Group.

Powered by Cryptzone MindTerm - Copyright 1997 – 2012 Cryptzone Group AB (publ). All rights reserved.

February 2012

Guide to Using IPControl

DID# IPC5003 Revision 2

Version 5.0

© 2012 BT INS, Incorporated

BT INS

Diamond IP Software Solutions

801 Springdale Dr., Suite 100

Exton, PA 19341

Tel. 1.610.423.4770

Fax 1.610.423.4774

Contents

Chapter 1 Introduction	1
Overview.....	1
Major Functions	2
Record Information about Subnets.....	2
Individual IP Address Inventory	3
DNS Configuration Management.....	4
DHCP Configuration Management	6
Dynamic DNS.....	6
Address Utilization and Tracking.....	7
Administrator Controls.....	7
Components	7
License Key Support.....	8
Chapter 2 Getting Started	9
How to Begin.....	9
Logging into the IPControl Web User Interface.....	10
Logging in for the First Time	10
The Menu Bar	11
The Home Tab	12
The License Block	12
Quick Links	13
Administrator Features	13
Logging Off.....	14
Displaying IPV6 Capacities	14
Internationalized Domain Names (IDN) Support.....	15
UI Treatment.....	16
Search and IDN	16
Column Selection	17
Column Sorting.....	18
Exporting Output.....	18
Chapter 3 Managing IP Addresses	21
Container View	21
Container View Tree Hierarchy.....	22
Container Details	23
Container Address Block Details.....	24
Logical Container Functions	28
Add Root Block	28
Add Site	31
Add Child Block	34
Address Pool Allocation.....	38
Utilization Display	39
Block Chart	40
History Chart.....	41

Device Container Functions	43
Add Site	43
Device Container Child Blocks	44
Defining a Default Gateway	46
Attach Child Block	47
Block Order	49
Network Switch Functions	50
IP Management	51
Adding an Individual IP Address	52
Workflow (Record Approval Layer)	57
Multi-Homed Host	61
Editing an IP Address	64
Editing Resource Records	64
Adding a Range of IP Addresses	64
Adding an IP Address Pool	67
Show Dynamic Leases	69
Planned vs Actual	70
Subnet/Block View	71
Understanding the Screen Layout	71
Editing Blocks	74
Root Block	75
Child Block	77
Delete Block	79
Split Block	79
Join Block	79
Move Block	79
Block type edit	80
Pending Approvals	81
My Approvals	81
My Submissions	85
Discovery/Collectors	85
Discovery/Collector Task Definition Options	85
On-demand (Immediate) Collection Task	88
Scheduled Collection Task	88
Recurring Collection Task	88
Address Space Reclaim	89
Manual Reclaim	90
Automatic Reclaim	90
Ignoring Specific Device Types during Subnet Reclaim	90
IP Address Space Reclaim	91
Performing Manual IP Address Reclaim	92
Performing a Manual Subnet Reclaim	93
Performing Automatic Reclaim Tasks	95
Container Maintenance	96
Container Maintenance Layout	96
Edit Container	97
Delete Container	98
Add Child Container	98
Reparent/Move this Container	101
Attach Network Service to Container	102
Detach Network Service from Container	103
Attach Switch	103
Detach Switch	104
Network Elements/Devices	104

Adding a Network Element.....	105
Editing a Network Element.....	107
Server Pairs.....	109
Adding a Network Service Pair.....	109
Editing a Network Service Pair.....	111
Chapter 4 Managing DNS.....	113
Servers/Services	113
Managing DNS Servers/Services.....	114
Adding a DNS Network Service.....	115
Zones on a DNS Server	122
Configuring DNS Views on a DNS Server	128
Configuring Zone Templates on a DNS Server	131
Configuration/Deployment	131
Configuration/Deployment Task Definition Options	131
On-demand (Immediate) Config/Deployment Task.....	133
Scheduled Config/Deployment Task	133
Recurring Config/Deployment Task	135
Domains.....	136
Managing DNS Domains.....	136
Adding a DNS Domain.....	137
Editing a DNS Domain.....	140
Managing Resource Records.....	142
Galaxies	145
Adding a DNS Galaxy	146
Log Channels	148
Adding a Logging Channel	149
Editing a Logging Channel	151
Server Templates	151
Managing Server Templates.....	152
Adding a DNS Server Template	153
DNS Domain Types	160
Managing DNS Domain Types.....	160
Address Match Lists	162
Managing Address Match Lists	162
Adding an Address Match List.....	163
Editing an Address Match List.....	164
Transaction Keys.....	165
Managing Transaction Keys	166
Adding a Transaction Key	167
DNS Option Vendor Dictionary.....	168
Managing DNS Option Vendor Dictionaries	168
Editing Syntax for DNS Options	170
DNS Option Master Dictionary.....	171
Managing the DNS Option Master Dictionary.....	171
DNS Software Products.....	173
Managing DNS Software Products	173
Adding a Software Product.....	174
Chapter 5 Managing DHCP	177
Servers/Services	177
Managing DHCP Servers/Services	177
Adding a DHCP Server.....	178
General Tab	180

Collection Tab	181
Configuration Tab.....	182
Failover Peer Tab.....	183
Extensions Tab.....	185
Utilization View	186
Network Services List	186
Utilization Display	187
Block Details.....	188
Configuration/Deployment.....	190
Configuration/Deployment Task Definition Options.....	190
On-demand (Immediate) Config/Deployment Task	192
Scheduled Config/Deployment Task.....	192
Recurring Config/Deployment Task	193
Policy Sets	194
Adding a DHCP Policy Set	196
Working with DHCP Policy Set Policies	196
Option Sets	199
Adding a DHCP Option Set.....	200
DHCP Option Set Options	201
Viewing all options assigned to this option set.....	202
Editing values of options assigned to this option set	203
Removing options from this option set.....	203
Client Classes.....	204
Adding a DHCP Client Class.....	205
Editing a DHCP Client Class.....	205
Option Vendor Dictionary	206
Adding New Options to DHCP Product.....	209
Removing Options from an DHCP Option List	209
Option Master Dictionary.....	209
Editing a DHCP Master Option	212
DHCP Software Products.....	212
Adding a Product	213
Editing a Software Product	214
Chapter 6 Producing Reports	217
Reports Overview.....	217
Filters.....	217
Container Utilization Report	218
Creating a Container Utilization Report	218
Container Utilization Report Output	221
Block Utilization Report.....	222
Creating a Block Utilization Report.....	222
Block Utilization Report Output.....	225
Low Pool	226
Creating a Low Pool Report	226
Low Pool Report Output	228
Container Audit Report.....	229
Creating a Container Audit Report.....	229
Container Audit Report Output.....	230
Block Audit Report	230
Creating a Block Audit Report	231
Block Audit Report Output	232
Device Audit Report	232
Creating a Device Audit Report	233

Device Audit Report Output.....	234
Resource Record Audit Report.....	234
Creating a Resource Record Audit Report.....	235
Resource Record Audit Report Output.....	236
Administrator Audit Report.....	237
Creating an Administrator Audit Report.....	237
Administrator Audit Report Output.....	238
Login Audit Report.....	239
Creating a Login Audit Report.....	239
Login Audit Report Output.....	240
Tasks.....	241
Tasks Screen Layout.....	241
Task Details.....	244
Previewing Configuration Files.....	246
Alert Log.....	246
Working with the Alert Log.....	246
Appliance Dashboard.....	248
Appliance Details.....	249
Appliance Management.....	251
Logged-In Administrators Report.....	253
Accessing the Logged-In Administrators Report.....	253
Logged-In Administrators Report Output.....	253
RIR Summary Report.....	254
Accessing the RIR Summary Report.....	254
RIR Summary Report Output.....	254
SWIP/Net Name Report.....	256
Creating a SWIP/Net Name Information Report.....	256
SWIP/Net Name Information Report Output.....	257
Chapter 7 Setting Up System Policies, Agents, and Importing Data	259
System Policies/Options.....	259
Agents.....	265
Import Wizard	266
Step 1: Select Import Type.....	267
Step 2: Select Import File.....	268
Step 3: Validate Import File Data.....	269
Step 4: Import Data.....	270
Search	273
Chapter 8 Working with Blocks and Subnets	277
Allocation Reason Codes.....	277
Block Types.....	278
Constraining Block Sizes.....	280
Address Pool Allocation Templates.....	281
Searching for an address allocation template.....	281
Deleting an existing address allocation template	282
Adding a new address allocation template	282
Site Allocation Templates	284
Site Allocation Template Functions	285
Site Allocation Template Prerequisites	285
Adding a Site Allocation Template.....	286
Editing a Site Allocation Template.....	291
Deleting a Site Allocation Template.....	292
RIR Organization IDs	293

Chapter 9 Working with IP/Devices	297
Vendor/Models	297
Vendor Maintenance	297
Model Maintenance	298
Device Types	300
Naming Policies	301
Device Interface Template Maintenance.....	304
Adding a Device Template.....	305
Editing a Device Template.....	306
Chapter 10 Using Other Tools	307
Threshold Sets.....	307
Editing a Threshold Set	308
Threshold Alerts	310
Container Alerts	310
Block Alerts.....	311
Network Service Alerts.....	312
User-Defined Fields	314
Creating Radio Button and List Values.....	316
Information Templates.....	318
IDN Converter.....	321
UI Treatment.....	322
Add/Edit Resource Records.....	322
Add/Edit IP Address.....	323
Add/Edit Zone	323
Search and IDN	323
Chapter 11 Managing Appliances	325
Appliance Definition.....	325
Software Updates.....	326
Software Packages	327
Chapter 12 Managing Administrators	329
Administrator Definition.....	329
Adding an Administrator.....	330
Assignable Roles.....	331
Administrator-specific Policies.....	331
Determining Effective Rights for an Administrator.....	331
Authorized Functions	332
Access Control List.....	332
Block Type Access.....	332
Device Type Access.....	332
Policies	332
Domain Access Control.....	333
Net Service Access Control.....	333
Resource Record Type Access.....	333
Address Type Access.....	333
Administrator Roles	334
Adding an Administrator Role	335
Administrator Role Policies	335
Authorized Functions Tab	337
Access Control Lists.....	337
Block Type Access Tab.....	339

Device Type Access Tab	342
Policies Tab	343
Domain Access Control Tab	344
Net Service Access Control Tab	346
Resource Record Type Access Control Tab	347
Address Type Access Tab	348
Chapter 13 Performing Advanced Administration Activities	349
Configuring INS DNS for Selected or Changed Zone Push	349
Configuring IPControl to use External Authentication	351
Input	352
Output	352
Configuration Steps	352
Interfacing with Microsoft Active Directory and Microsoft DNS	354
BIND DNS	355
BIND Redundancy	355
Microsoft DNS	356
BIND DNS and Microsoft DNS Compared	357
Joint Implementation Scenarios	358
Case 1: BIND DNS Supporting Non-DNS AD Environment	358
Case 2: IPControl Centralized Inventory of AD DNS Environment	361
Case 3: AD Multi-Master DNS with BIND DNS Slave	366
Case 4: BIND DNS Master with a Microsoft DNS Slave	368
Case 5: PeerMaster – Effective BIND-Microsoft Multi-Master DNS	371
Creating GSS-TSIG enabled account in Microsoft MMC	373
Overview	373
Microsoft Active Directory	373
IPControl	374
Other Considerations	374
IPControl Management of Windows DHCP Server	375
Overview	375
Prerequisites	375
Windows Server Procedures	375
IPControl Procedure	379
Configuring DHCP Failover	381
Failover Scenarios	381
Simple Failover	382
Many to One Failover	382
Failover Checklist	383
Configuring Failover within IPControl	384
Configuring IPControl for Failovers	384
Administrator Access Control Use Cases	387
Use Case - Regional Administrators	387
Use Case - Specific Block Access Required	388
Use Case - DNS Administrator	388
Use Case - Third Party Access	389
Configuring DNS on a TwinMirror Appliance	390
Supported RFCs	390

Chapter 1 Introduction

Overview

Welcome to the IPControl IP Address Management System. IPControl is a comprehensive software solution that helps organizations plan and maintain their IP address space and leverages that information for use by IP services such as DNS and DHCP.

No matter what size or type of organization, anyone that runs an IP network needs to manage their IP address space effectively. However, the Internet Protocol specifications do not provide any tools that help with this process. Some people may say that DHCP provides “automated IP address assignment”, but the scopes that are assigned to a DHCP server must still be allocated out of larger blocks used by the company. Some products that track IP addresses have been around for the last decade, but they are considered first generation tools that do not adequately address the needs of enterprises and service providers in the 21st century.

IPControl is a next generation tool that offers advanced functionality:

- Centralized planning and management of the complete address space down to the individual IP address level.
- Centralized DNS and DHCP configuration management.
- IPv4 and IPv6 support.
- Automated address utilization collection and reporting.
- Address utilization forecasting and trending analysis.
- APIs and Command Line Interfaces for integration with any type of system. Examples are work-flow systems, provisioning systems, change management systems, or network management systems.

Unlike other tools that maintain IP name and address data as discrete information maintained uniquely and separately, IPControl interacts with network devices and services to:

- Verify that the actual network matches the information in IPControl.
- Capture and record utilization information to be able to establish historical trends.
- Reclaim inactive addresses.

This interaction not only maintains consistency between the planned and deployed network, but allows proactive modification to the network to adjust for IP address shortages and overages.

IPControl is one product that is part of a complete and robust IP Address Management Suite. It can be used standalone or in conjunction with other products in the suite. The other members of this product family are:

- **NetControl** A sophisticated IP Address Block management tool that plans and deploys address blocks automatically.
- **Sapphire** IPControl Management and high-availability DNS/DHCP Server appliances.

Collectively, these products form the InControl IP Address Management Suite. When multiple products are installed, they appear and function seamlessly.

Major Functions

IPControl has the following general functions:

- Record information about subnets.
- Individual IP Address inventory and asset management.
- Centralized DNS (Domain Name System) configuration and management.
- Centralized DHCP configuration and management.
- Updates DNS Dynamically for DHCP clients and for immediate changes to the IP Address Inventory.
- Captures address utilization and tracks it over time by the periodic and recurring retrieval of DHCP information, enabling trending and regression analysis to extrapolate when an IP address block will be exhausted.
- Creation of unique administrators that only allow access to those parts of the system authorized for that individual.

Record Information about Subnets

The basic building block of modern IP networks is the subnet. Yet, how are companies tracking information about those subnets? What are all the IP addresses eligible to be a “default gateway” for hosts on that subnet? What is the proper subnet mask for a subnet? It is not surprising that many companies rely on routing tables to obtain this information, or at least to use them to verify the accuracy of manually maintained information.

IP Addressing rules, such as verifying and enforcing bit-boundary rules when defining subnets are standard in IPControl. Classless Inter-Domain Routing (CIDR) and Variable Length Subnet Mask (VLSM) are fully supported.

In keeping with the dynamics of growing networks, many organizations have had to resort to having duplicate IP network numbers. Mergers have often forced IT departments into this practice. IPControl can easily handle this situation, helping companies keep these duplicate iterations of address space separate and distinct.

Before individual IP addresses can be recorded and managed, subnets must be declared. When a subnet is declared in IPControl, it is tagged as either an IPv4 subnet or an IPv6 subnet. Once declared, that subnet is supported in its native form, either IPv4 or IPv6. That subnet must exist in a network of that address type and all the individual IP addresses in that subnet will be of that type.

With IPControl, subnets can be automatically created out of larger address blocks. IPControl allows a customer to organize and allocate their address space at many different levels, fitting any geographic, organizational or topology design.

IPControl provides a central repository for all subnet information; it verifies the accuracy of that information by “reading” the network and comparing it to the repository. The result is a single, correct picture of what is deployed on the network.

Individual IP Address Inventory

Historically, IP Addresses have been recorded with a number of different methods. These include spreadsheets and logs. Some organizations have used DNS files or DHCP configurations to track which IP addresses were assigned and which ones were available. Common to all these techniques was a single view of the information. These processes only looked at the information in one way regardless of how those addresses were actually deployed on the network. DNS looked at it strictly from a DNS resource-record view.

IP addresses do not live by themselves. They are always equated with something, specifically some device or host on the network.

IPControl’s design took this into consideration. IPControl keeps track of a number of elements that represent real aspects of an IP network. These elements are:

- IP Addresses
- Devices
- DNS Information
- DHCP Information
- Services
- Users
- Logical or Physical representations of how a network is organized.

Relationships are then established between these elements in such a way that represent real network situations. Examples are:

- IP addresses are associated with devices
- Devices can have any number of DNS Resource Records
- Users own devices
- Devices reside at physical locations
- Subnets reside at physical locations
- Subnets form a logical network topology
- Services execute on Devices

A comprehensive IP Address Management System not only tracks the IP addresses themselves, but also how those addresses affect, and are affected by, other things on the network. For example, if a network management system such as HP Openview discovers a router, it will report on all the subnets that are attached to that device. It is the IP Address Inventory System that is the source for data needed to translate the HP Openview discovered data into meaningful information. The IP Address Inventory System can answer such questions as:

- Are the IP addresses and subnets on that router correct based on the plan, design and architecture of the network?
- What are the physical locations of those subnets and routers?
- Are the proper names registered in DNS for that device and all the IP addresses on that device?

IPControl not only provides a source for such information, but can periodically verify it to ensure its accuracy.

An extremely useful feature of IPControl is the general way that it allows a company to organize its IP Address information. IPControl uses “Containers” to create any type of hierarchical topology. Address information can then be placed into these Containers. The flexibility of a hierarchy allows the rendering of information in almost any fashion, allowing the company to represent the IP address information in the way that makes the most sense for that company.

Access to the IPControl Address Inventory is not just through a human Graphical User Interface (GUI). It is also accessible through Command Line Interfaces (CLI) and Application Programming Interfaces (API). This allows other systems and programs to get to IP Address Inventory information for automatic population of those other systems and programs, leveraging the Address Inventory for any number of uses.

Views of the elements are summarized wherever possible to reduce the amount of information that must be scrolled. This is especially important for companies that have a very large address space or numerous DNS elements. Whenever there is a relationship between IPControl elements (addresses, devices, DNS records, etc.), those relationships can be easily displayed from any of the elements. For example, can we see all the IP addresses associated with a device? Or, what are all the DNS records that will be generated for a given IP address? IPControl provides this information from an easy to use interface.

DNS Configuration Management

Without an automated, centralized IP Address Management System, there can be considerable duplication of data for different uses. The person tracking IP address using one method, such as a spreadsheet, would provide that information to a DNS administrator. The administrator would enter the same information, but in a different context and syntax, into a different system, specifically DNS configuration (i.e. zone) files.

IPControl eliminates this additional administrative task. IPControl takes the information that is used to record IP address and device information and builds the needed DNS records automatically, populating the DNS configurations in real time using dynamic DNS (RFC 2136) updates. It can also build, or rebuild, a complete set of DNS configuration files that are compliant with ISC’s BIND Versions 9 DNS servers, as well as a number of 3rd party DNS servers including Microsoft’s. These DNS configuration files (boot and zone db files) are remotely loaded onto DNS servers distributed on the network.

IPControl’s DNS configuration feature allows the easy entry and management of some of BIND’s newer features, reducing those feature’s complexity and making it easier to implement and deploy them, and in much less time. Some of these features are:

- BIND Views

- TSIG support (for dynamic updates and zone transfers)
- Nested Access Control Lists (ACLs)
- Configuration for remote management via the RNDC command
- Zone types of forward, stub and delegate-only
- Multiple masters per zone

BIND 9 is exceptionally feature-rich. However, with that increased functionality comes configuration complexity. There are a daunting number of options, parameters and keywords that can be coded in the DNS configuration files. IPControl minimizes this complexity by hiding all options that may not pertain in a specific environment. A customer has complete control on which BIND options are made visible and externalized, and which ones should take defaults and not shown. A master DNS dictionary contains every possible BIND option available. Subsets are defined and associated with DNS server “models” or “templates”. These models can then be applied to a real server definition, almost eliminating the need to specify options for that server. A high level DNS administrator can define these models once, and then let them be applied to any number of server definitions by less experienced administrators.

What are some of the other ways that IPControl can make administration of DNS servers easier?

- Automatic generation of **key** statements between two DNS servers to insure that they have consistent private keys between them.
- Definition of **server** statements that insure correct communication between different DNS servers.
- Creation of **control** statements that facilitate external communication to the DNS server from only authorized sources.
- Proper inclusion of ACLs in the configuration files whenever they are referenced.

Even though IPControl reduces the complexity of these definitions, they are all still accessible and configurable, giving complete flexibility in those situations that demand the advanced DNS features implemented. The philosophy of IPControl is simple: make configuration easy, but don't compromise functionality.

Another unique feature of IPControl's DNS Configuration Management is the ability to have multiple domains per DNS zone. For example, a DNS domain called **company.com** exists as a delegated domain with its DNS resource records in a single db zone file. Child domains to company.com might be **newyork.company.com** and **california.company.com**. The DNS resource records for these child domains can exist as delegated domains in unique zone files (with their own SOA records) or in the parent's db zone file. IPControl fully supports this model.

Prior to activating any new DNS configuration, it is checked for syntax and consistency to make sure that DNS configuration files are built correctly. This will ensure that DNS servers always initialize properly.

In addition to supporting BIND Version 9, any DNS server that is compliant with BIND 9 is supported. Support for Microsoft's Windows 2003/2008 DNS server is also provided.

DHCP Configuration Management

Another service that benefits from the common central repository of IP address information is DHCP. Addresses assigned to DHCP servers (scopes) come out of the overall management of the address space that is part of the IP Address Inventory feature of IPControl.

As with DNS, address information needs to be manually replicated in a DHCP server configuration without the aid of an IP Address Management System. With IPControl, the actual configuring of scopes is completely hidden from the administrator.

Ranges of addresses are defined with an attribute of “dynamic”. They are then assigned to a DHCP server. The DHCP servers are defined before-hand to IPControl, along with operational parameters for those servers. IPControl includes a software based DHCP server that can run on Sun Solaris 10, Windows 2003/2008 or Linux (RedHat, Enterprise 4 or 5). A variety of other DHCP servers are also supported, including Microsoft’s.

Rather than link DHCP options (the IP parameters sent by the server to the DHCP client) to address ranges or scopes, options are defined as sets. These sets are then associated with a rule. If the information provided by the DHCP client in the process of obtaining an IP address matches the rule, those options are sent, regardless of the subnet from which an address is provided to the client. This way, a limited set of option lists can be maintained, even for the largest of networks. Options don’t have to be defined and associated for each and every subnet or scope. Broad policies can dictate what options a client will get, disassociated from the address pools that are appropriate for the client based on their network location.

IPControl’s DHCP server supports “failover”, a high availability option where two DHCP servers work in concert to provide a single appearance of DHCP services to the DHCP client. This DHCP server implements the IETF DHCP Failover Protocol Internet Draft and allows very flexible primary/secondary DHCP server deployment designs. With the IPControl DHCP server you can:

- Declare one server as a primary and one as a backup for a given subnet.
- Have one DHCP server act as a backup for any number of primaries.

These capabilities allow limitless combinations that can effectively provide for high availability and redundancy of the DHCP configuration while maximizing the use of address space.

Dynamic DNS

IPControl has full support of updating the DNS name space with RFC 2136 compliant dynamic UPDATE packets. There are two sources for these updates:

- The IPControl DHCP server
- Changes made directly to the IP Address Inventory repository for static address changes

The result is a DNS name space that is synchronized with the IP Address Inventory. Dynamic updates are performed in two different ways:

- Immediately
- Batched to combine a number of dynamic updates in a single operation

BIND Version 9 brings true dynamic DNS operation as the primary mechanism for maintaining the DNS space. Unlike earlier versions of this DNS server, which used modifications to zone db files as the definitive update mechanism, BIND 9 relies almost exclusively on dynamic DNS to keep its

domain information current. IPControl fully supports this model. Zone db files are only updated by the IP Address inventory initially, and in disaster situations. At all other times, dynamic updates are used to update zone information.

Name and address binding information from a DHCP server is verified before a dynamic DNS update is performed using the method outlined in the IETF Internet Draft “Resolution of DNS Name Conflicts among DHCP Clients”. This method does not rely on the IP Address Management Repository for name and address information, but rather DNS itself, allowing that data to be replicated for a much more robust availability model.

Address Utilization and Tracking

Planning and recording of IP addresses in a central repository is a unidirectional approach to IP address management. It is not a complete solution for an IP Address Management System. That is why IPControl is multi-directional system. That is, it not only plans and records information about the IP address space, but it also interacts with the actual network to read, verify and compare configurations and utilizations on the network against the IP Address Inventory repository. IPControl will go out to the network and:

- Verify the use of a statically defined address
- Ensure that free addresses in the repository are not in use on the network
- Capture information about DHCP clients.

These three features provide the raw data to report and trend address utilization. This can be displayed as current snapshots, or historically, providing trending information at any level of the IP address hierarchy.

Administrator Controls

IPControl is a multi-administrator system. As such, access to system is limited based on rights and privileges given to that administrator. These rights can be very broad, or limited to a very narrow set of conditions. To any element and/or Container in IPControl, an administrator can be allowed read access, write access, or create/delete access. Options within the Graphical User Interface can be exposed or withheld. The use of the CLIs can be denied or allowed, as well as the APIs.

Components

IPControl is a highly scalable, distributed solution that consists of four major components:

- **InControl Executive** – The central management system responsible for initiating work requests or recording the results of completed requests. There is typically one InControl Executive per IPControl system.
- **InControl Agents** – Lightweight, distributed processes that execute work requests from the InControl Executive. The InControl Agents are the entities that interface directly with DHCP servers, DNS servers, or Network Devices such as routers. There can be any number of InControl Agents distributed on a network. They may be located wherever is optimal for the network topology.

- **IPControl Database** – The central repository that stores information and auditing data about IP network space. This database is under the control of the InControl Executive.
- **IPControl Administrative Interface** – A Web-based Graphical User Interface (GUI), hosted on the InControl Executive that allows administrators to control the InControl system.

License Key Support

You must have a valid serial number to install IPControl on a Windows platform. Furthermore, IPControl requires you to enter a license key the first time you log in to the product. The license key determines how many IP Addresses, devices, and/or agents that can be managed.

To obtain your serial number and license key, please contact Software Support at swsupport@diamondipam.com.

Chapter 2 Getting Started

How to Begin

Note: For information on installing IPControl, refer to *Guide to Installing IPControl*.

To start using the IPControl Management System, all IPControl services, and the IPControl database must be started.

Windows: To start InControl services, use the Windows Services Controller, and start the following services:

- MySQL Relational Database
- InControl Message Router Service
- InControl Task Manager Service
- InControl Result Manager Service
- InControl Log Manager Service
- InControl File Manager Service
- InControl Callout Manager Service
- InControl Agent
- Tomcat

Unix: To start InControl services, execute the **\$INCHOME/etc/incontrol start** command.

Table 2-1 Description of InControl Services

Windows service	What does it do?	Running on
MySQL (Community Version) or Oracle (customer provided)	Provides the relational database system that supports the InControl system.	InControl Executive server only.
InControl Task Manager Service	Provides scheduling functions and controls the tasks (units of work) that are sent to the InControl Agents.	InControl Executive server only.
InControl Result Manager Service	Collects task result information from all InControl Agents and places that information into the InControl database.	InControl Executive server only
InControl Message Router Service	Provides reliable message transport between the InControl Task Manager, the Result Manager, and the Agent.	InControl Executive server, and all InControl Agents
InControl Log Manager Service	Provides a centralized log message	InControl Executive server only.

Windows service	What does it do?	Running on
InControl Callout Manager Service	Provides a mechanism to invoke customer defined scripts after certain events are triggered within the system.	InControl Executive server only.
InControl Agent	Communicates with servers and devices to gather statistics.	InControl Agent server(s) only.
InControl File Manager Service	Provides file transport capabilities.	InControl Executive server only.
InControl DNS Listener Service	Listens for changes to the DNS environment and updates IPControl with the appropriate DNS Resource Records.	InControl Executive server only.
Tomcat	Provides the http web server and serves the InControl web interface.	InControl Executive server.

Logging into the IPControl Web User Interface

You need to log into the IPControl Web user interface to perform all functions. Before you log into IPControl for the first time, you need to be assigned a user name and password from your IPControl administrator.

IPControl is administered via a Web browser. If you are administering IPControl from the same server you installed IPControl on, you will find a shortcut in your Programs folder (**Start > Programs > InControl → InControl Supervisor**). Otherwise, follow the directions in the next section.

Logging in for the First Time

To log into IPControl, follow these steps:

1. Open your Web browser.
2. In the Address bar, type the following URL:
`http://xxx.xxx.xxx.xxx:8080/incontrol`
 where xxx.xxx.xxx.xxx is the IP address of the InControl Executive.
 One example might be: **`http://172.16.32.50:8080/incontrol`**
 You may also use the DNS name of the InControl server, such as:
`http://ncexec.mycompany.com:8080/incontrol`
3. You see the following login screen.



Figure 2-1 Login

4. Enter the Login name and Password assigned to you by your IPControl administrator, and click **Log In**.

Note: The first time you log into the IPControl system, use the user name **incadmin**, and the password **incadmin**. Refer to “Changing Password” on page 14 for instructions on changing the password of this user.

The Menu Bar

The bar across the top of the browser display is called the menu bar. There are four menu lists in the IPControl Supervisor interface:



Figure 2-2 Menu Bar

- Home
- Management
- Reports
- Tools

The menu options are described in detail in the sections below.

The Home Tab

The **Home** tab displays the current status of your system and some quick links for easy navigation, as shown in Figure 2-3.

Note: The **Home** tab displays the same content as the **About** report on the **Reports** menu.

The License Block

The screenshot shows the IPControl™ web interface. The top navigation bar includes 'MANAGEMENT', 'REPORTS', and 'TOOLS'. The main content area displays the following information:

IPControl™
IP Address Planning and Management System

Version 5.0 Build 31

Address Block Information:

Current Public IPv4 Space:	0
Current Private IPv4 Space:	4,583
Current total IPv4 Space:	4,583
Maximum Allowed IPv4 Space:	Unlimited
Current Number of IPv6 /64 Blocks:	26
Maximum Allowed IPv6 /64 Blocks:	4,294,967,296

Individual IP Address Information:

Maximum Allowed Used IP Addresses:	250,000
Current Number of Used IP Addresses:	897
Maximum Allowed Defined IP Addresses:	Unlimited
Current Number of Defined IP Addresses:	18,285
Maximum Agents:	0
Current Agents:	5
Maximum Appliances:	0
Current Appliances:	4
Maximum Virtual Appliances:	0
Current Virtual Appliances:	0

Other Key Information:

Expiration Date of License Key: 12/1/12

Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Copyright (c) 2007-2011, BT INS, Inc.
All Rights Reserved - Use subject to terms of license agreement

Quick Links

- [Management Containers](#)
- [Address Blocks](#)

Administration Features

- [Pending Approvals](#)
- [Change Password](#)
- [Add Administrator](#)
- [Logout](#)

Additional Information

- [IPControl Documentation](#)

Product Support Information

Email: swwsupport@diamondipam.com

Online Support: [Click to visit](#)

Help Desk Telephone Number: +1 610.280.2345

Help Desk Fax Number: +1 610.423.4774

Figure 2-3 License Block

Several key pieces of information are shown on the **Home** screen:

Version and Build number

In the example above, it is listed as **Version 5.0 Build 24**. You need to know the version that is installed when getting support for IPControl. For support, refer to the links and phone numbers in the Product Support Information section.

Address Block Information:

- **Current Public IPV4 Space** - This is the size of public IPV4 address space (blocks and subnets) currently defined in the system. A “public” address is one that is not within the ranges defined in [RFC1918](#).

- **Current Private IPv4 Space** - This is the size of private IPv4 address space (blocks and subnets) currently *used* (has a status of “in-use”) in the system. A “private” address is one that lies within the address ranges defined in [RFC1918](#).
- **Current total IPv4 Space** – This is the sum of the public and private IPv4 address space counters above.
- **Maximum Allowed IPv4 Space** - This is the total IPv4 space (subnets and blocks) allowed by your license key.
- **Current Number of IPv6 /64 Blocks** - If you have licensed IPv6 support, this counter shows the number of /64 subnets defined.
- **Maximum Allowed IPv6 /64 Blocks** - The total number of /64 blocks allowed by your license.

Individual IP Address Information:

- **Maximum Allowed Used IP Addresses** - The total number of used IP Addresses allowed by your license key.
- **Current Number of Used IP Addresses** - The total number of used IP Addresses within the system. This count includes devices with the following status; Static, Manual DHCP, Dynamic DHCP with an active lease, and Automatic DHCP with an active lease.
- **Maximum Allowed Defined IP Addresses** - The total number of defined IP Addresses that allowed by your license key.
- **Current Number of Defined IP Addresses** - The total number of defined IP Addresses within the system. This count includes devices with the following status; Static, Manual DHCP, Dynamic DHCP, Automatic DHCP, and Reserved.
- **Maximum Number of Agents, Appliances, and Virtual Appliances** – The total number of agents, appliances, and virtual appliances defined in the system.

Other Key Information:

- **Expiration of License Key:** The date on which your license key for IPControl expires.

Quick Links

Quick Links provide you with direct links to some of the more commonly used functions. Use these to save time navigating through the other tabs. You can add up to four custom links in **Policies and Options** on the **Tools** menu.

Administrator Features

Administrator Features provides you with convenient links to four commonly used functions.

Pending Approvals

The Pending Approvals screen allows you to view two sets of data related to device workflow.

To review the status of device changes that either need your approval or that you have submitted for approval, click the **Pending Approvals** link. The Pending Approvals screen opens, as described in “Pending Approvals” on page 81.

Changing Password

To change your password, click the **Change Password** link. The Change Password screen opens.

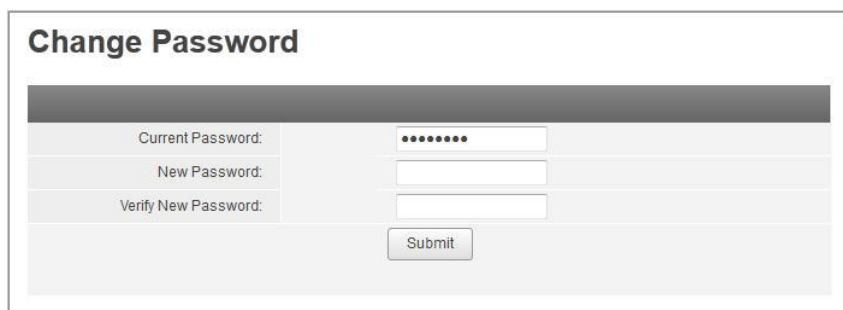
The image shows a web form titled "Change Password". It has a dark header bar with the title. Below the header, there are three input fields: "Current Password:" with a masked password (dots), "New Password:", and "Verify New Password:". A "Submit" button is located at the bottom right of the form.

Figure 2-4 Change Password

Enter a new password in the **New Password** field and then confirm the password by retyping it in the **Verify New Password** field. Click **Submit** to complete the procedure.

Adding an Administrator

Refer to “Adding an Administrator” on page 330.

Logging Off

To exit the system, choose one of the following:


- Click the **Logout** link at the top of the screen.
- Click the **Logoff** link in the Administration Features section of the **Home** menu.

You are logged out of the system and returned to the initial login screen (Figure 2-1 on page 11).

Displaying IPV6 Capacities

IPV6 subnets are extremely large. Displaying these numbers is challenging because the numbers are so large that they lose meaning. IPControl enables you to display these numbers in one of three different formats, so their values are easier to interpret. The formats are:

- **CIDR** – The number is displayed in terms of a CIDR value, e.g., 1 /64
- **Full** – The full decimal number is displayed, e.g., 18446744073709551616
- **Exponential** – The number displayed as a power of 10, e.g., 1.8x10¹⁹

A gear drop-down () appears above the rightmost column in the display. Click on the gear drop-down to change the display format. The fields that will be affected are marked with a shaded triangle

in the upper right-hand corner (1 / 96). Place the cursor over the triangle to see the value in all formats, as shown in the sample container utilization display in Figure 2-5.

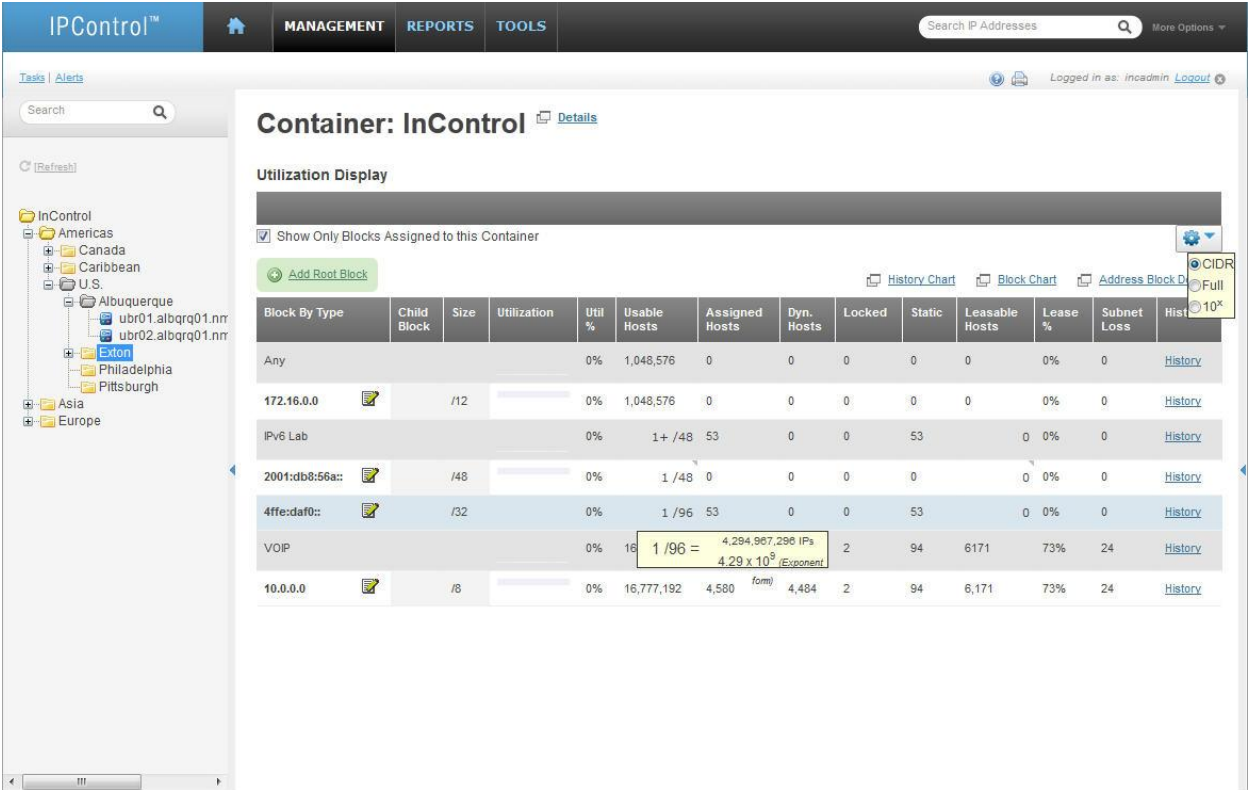


Figure 2-5 Utilization Display

Internationalized Domain Names (IDN) Support

Internationalized Domain Names use characters drawn from a large repertoire (Unicode). IDNA (Internationalized Domain Names for Applications) as described in RFC 3490 allows the non-ASCII characters to be represented using only the ASCII characters already allowed in so-called host names today. This backward-compatible representation is required in existing protocols like DNS, so that IDNs can be introduced with no changes to the existing infrastructure.

IDNA is only meant for processing domain names, not other text.

IPControl supports IDNA as defined in RFC 3490. It allows for data to be entered using Unicode characters and ASCII characters both when entering domain names. IPControl also gives the users the ability to switch between IDN and ASCII when viewing the data. The underlying data is always stored as ASCII or ASCII Compatible encoding (ACE).

For example, for Internationalized Domain name ‘bücher.com’, the ACE equivalent is ‘xn--bcher-kva’.

UI Treatment

Screens involving domain names, FQDNs and hostnames in case of domains/zones and owner and RDATA fields in case of resource records get special treatment for IDN support.

If an internationalized domain name is entered, an international drop-down icon appears on the screen (🌐). Click on the icon to switch between IDN (Unicode character set) and ACE (ASCII compatible encoding) views. Hover the cursor over domain names to see the value in the alternate format, as shown in Figure 2-6.

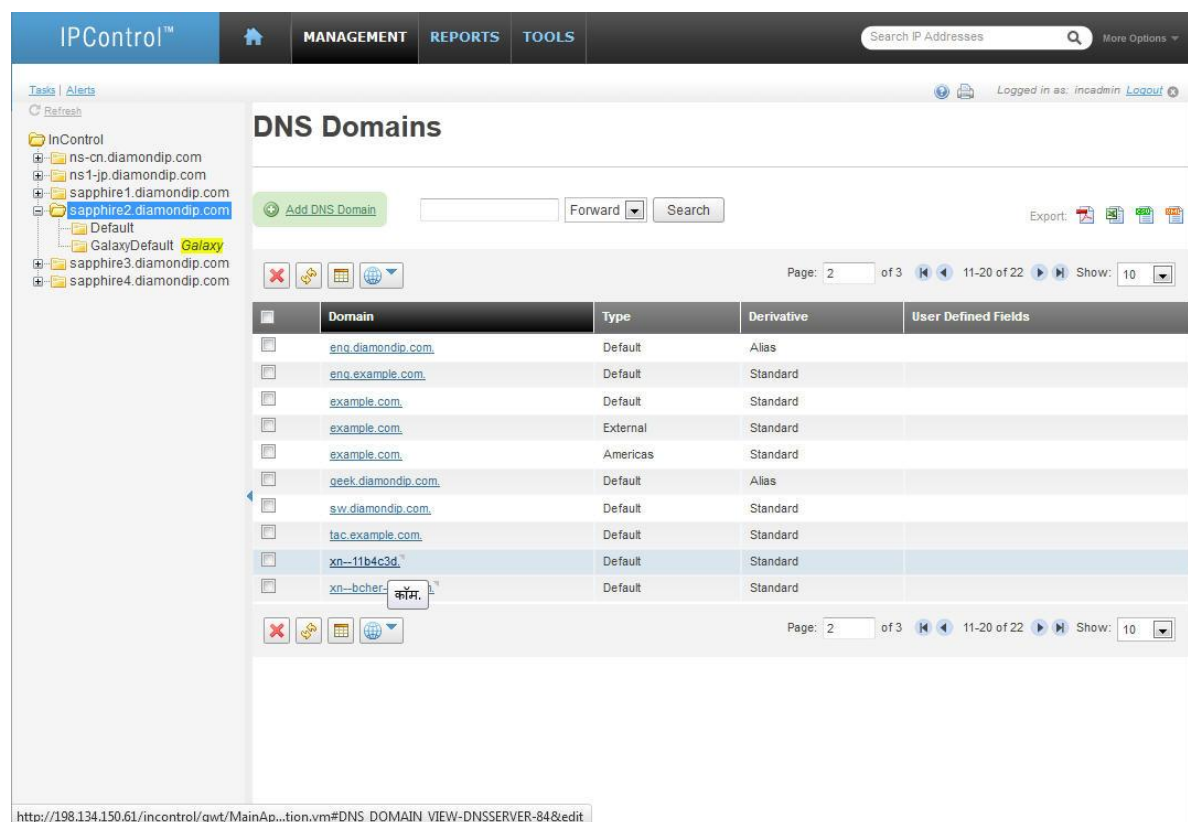


Figure 2-6 Internationalized DNS Domain Showing Alternate ACE Format

Search and IDN

Domain and resource record searches in IPControl are performed using the ASCII representations. If you have Internationalized Domain Names, type a full IDN domain name or full/partial ASCII domain name in the search box to get back the desired result. Partial IDN search does not work.

For example, to search domain “bücher.com”, you can enter “bücher.com” or “xn--bcher-kva” (ASCII Compatible representation) or any part of the ASCII compatible name (for example, “bch”) and get back the desired result.

However, putting “büc” does not return the domain “bücher.com” since the search is performed using the ASCII equivalent.

Column Selection

In addition to being able to filter report data selection criteria, you can select which columns you want to view in lists and reports where the  icon is displayed.

To change the column selection, follow these steps.

1. Click on one of the  icons. The Column Selection dialog opens, showing all columns selected, as shown in Figure 2-7

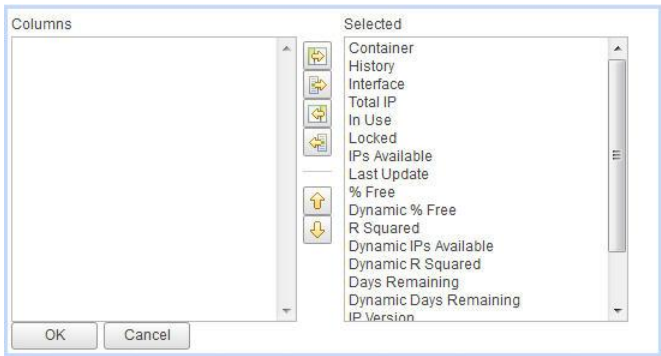








Figure 2-7 Report Column Selection

2. Choose from the following actions.

To ...	Then ...
Remove a currently displayed column	<ol style="list-style-type: none">1. Select the column in the Selected list.2. Click . The column is moved to the Columns list.
Remove all currently selected columns	Click  . All columns in the Selected list are moved to the Columns list.
Add a column that is not currently selected to the report output	<ol style="list-style-type: none">1. Select the column in the Columns list.2. Click . The column is moved to the Selected list.
Add all columns that are not currently selected to the report output	Click  . All columns now appear in the Selected list.
Move a column leftward in the report output	<ol style="list-style-type: none">1. Select the column in the Selected list.2. Click  until the column is located in the position you want it to appear in the output.
Move a column rightward in the report output	<ol style="list-style-type: none">1. Select the column in the Selected list.2. Click  until the column is located in the position you want it to appear in the output.

3. Click **OK** to implement your changes or **Cancel** to restore the default column display.


Column Sorting

Many columns in lists and reports can be sorted. Sortable columns are distinguished by their black headings, in contrast to gray column headings that cannot be sorted.

To sort a column, click the heading. The ▼ icon appears beside the heading as the data is sorted. To reverse the sort order, click the heading a second time. The ▲ icon appears beside the heading as the data is resorted.

Exporting Output

Once you have customized a list or report by modifying the filters and columns, you may want to save the output for analysis or review. IPControl provides the following export formats:

Format	Icon	Sample Output																																																																																																																																																																																																																																																																																																																		
PDF		<table><tr><th>Container</th><th>Block Type</th><th>Interface Name</th><th>Total IP</th><th>In Use</th><th>Locked</th><th>IPs Available</th><th>Last Update</th><th>% Free</th><th>Dynamic % Free</th><th>Dynamic Ips Available</th><th>R Squared</th><th>Dyna mic R Squared</th><th>Days Left</th><th>Dyna mic Days Left</th><th>V</th><th>Cont ainer Type</th><th>UDF</th></tr><tr><td>InControl</td><td>Data</td><td></td><td>11842</td><td>6175</td><td>21</td><td>5449</td><td>10/8/08 12:00 AM</td><td>46.01%</td><td>20.95%</td><td>1642</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v4</td><td>Logic al</td><td></td></tr><tr><td>Europe</td><td>Data</td><td></td><td>254</td><td>0</td><td>0</td><td>230</td><td>10/8/08 12:00 AM</td><td>90.55%</td><td>100.0%</td><td>125</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v4</td><td>Logic al</td><td></td></tr><tr><td>Americas</td><td>Data</td><td></td><td>11078</td><td>6175</td><td>21</td><td>4734</td><td>10/8/08 12:00 AM</td><td>42.73%</td><td>18.34%</td><td>1392</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v4</td><td>Logic al</td><td></td></tr><tr><td>Asia</td><td>Data</td><td></td><td>510</td><td>0</td><td>0</td><td>485</td><td>10/8/08 12:00 AM</td><td>95.1%</td><td>100.0%</td><td>125</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v4</td><td>Logic al</td><td></td></tr><tr><td>Asia</td><td>VOIP</td><td></td><td>254</td><td>0</td><td>0</td><td>244</td><td>10/8/08 12:00 AM</td><td>96.06%</td><td>100.0%</td><td>36</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v4</td><td>Logic al</td><td></td></tr><tr><td>U.S.</td><td>Data</td><td></td><td>8780</td><td>6175</td><td>21</td><td>2494</td><td>10/8/08 12:00 AM</td><td>28.41%</td><td>15.15%</td><td>1106</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v4</td><td>Logic al</td><td></td></tr><tr><td>U.S.</td><td>VOIP</td><td></td><td>13098</td><td>4484</td><td>2</td><td>8528</td><td>10/8/08 12:00 AM</td><td>65.11%</td><td>26.88%</td><td>1649</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v4</td><td>Logic al</td><td></td></tr><tr><td>U.S.</td><td>IPv6 Lab</td><td></td><td>3</td><td>0</td><td>0</td><td>-20</td><td>10/8/08 12:00 AM</td><td>-666.67%</td><td></td><td>0</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v6</td><td>Logic al</td><td></td></tr><tr><td>Canada</td><td>Data</td><td></td><td>254</td><td>0</td><td>0</td><td>230</td><td>10/8/08 12:00 AM</td><td>90.55%</td><td>100.0%</td><td>125</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v4</td><td>Logic al</td><td></td></tr><tr><td>Canada</td><td>IPv6 Lab</td><td></td><td>1</td><td>0</td><td>0</td><td>-9</td><td>10/8/08 12:00 AM</td><td>-900.0%</td><td></td><td>0</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v6</td><td>Logic al</td><td></td></tr><tr><td>Caribbean</td><td>Data</td><td></td><td>2044</td><td>0</td><td>0</td><td>2010</td><td>10/8/08 12:00 AM</td><td>98.34%</td><td>100.0%</td><td>161</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v4</td><td>Logic al</td><td></td></tr><tr><td>Caribbean</td><td>IPv6 Lab</td><td></td><td>16</td><td>0</td><td>0</td><td>6</td><td>10/8/08 12:00 AM</td><td>37.5%</td><td></td><td>0</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v6</td><td>Logic al</td><td></td></tr><tr><td>China</td><td>VOIP</td><td></td><td>254</td><td>0</td><td>0</td><td>244</td><td>10/8/08 12:00 AM</td><td>96.06%</td><td>100.0%</td><td>36</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v4</td><td>Logic al</td><td></td></tr><tr><td>Japan</td><td>IPv6 Lab</td><td></td><td>1</td><td>0</td><td>0</td><td>-9</td><td>10/8/08 12:00 AM</td><td>-900.0%</td><td></td><td>0</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v6</td><td>Logic al</td><td></td></tr><tr><td>Australia</td><td>Data</td><td></td><td>510</td><td>0</td><td>0</td><td>485</td><td>10/8/08 12:00 AM</td><td>95.1%</td><td>100.0%</td><td>125</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v4</td><td>Logic al</td><td></td></tr><tr><td>Ireland</td><td>Data</td><td></td><td>254</td><td>0</td><td>0</td><td>230</td><td>10/8/08 12:00 AM</td><td>90.55%</td><td>100.0%</td><td>125</td><td>0.0</td><td>0.0</td><td>0</td><td>0</td><td>v4</td><td>Logic al</td><td></td></tr></table>	Container	Block Type	Interface Name	Total IP	In Use	Locked	IPs Available	Last Update	% Free	Dynamic % Free	Dynamic Ips Available	R Squared	Dyna mic R Squared	Days Left	Dyna mic Days Left	V	Cont ainer Type	UDF	InControl	Data		11842	6175	21	5449	10/8/08 12:00 AM	46.01%	20.95%	1642	0.0	0.0	0	0	v4	Logic al		Europe	Data		254	0	0	230	10/8/08 12:00 AM	90.55%	100.0%	125	0.0	0.0	0	0	v4	Logic al		Americas	Data		11078	6175	21	4734	10/8/08 12:00 AM	42.73%	18.34%	1392	0.0	0.0	0	0	v4	Logic al		Asia	Data		510	0	0	485	10/8/08 12:00 AM	95.1%	100.0%	125	0.0	0.0	0	0	v4	Logic al		Asia	VOIP		254	0	0	244	10/8/08 12:00 AM	96.06%	100.0%	36	0.0	0.0	0	0	v4	Logic al		U.S.	Data		8780	6175	21	2494	10/8/08 12:00 AM	28.41%	15.15%	1106	0.0	0.0	0	0	v4	Logic al		U.S.	VOIP		13098	4484	2	8528	10/8/08 12:00 AM	65.11%	26.88%	1649	0.0	0.0	0	0	v4	Logic al		U.S.	IPv6 Lab		3	0	0	-20	10/8/08 12:00 AM	-666.67%		0	0.0	0.0	0	0	v6	Logic al		Canada	Data		254	0	0	230	10/8/08 12:00 AM	90.55%	100.0%	125	0.0	0.0	0	0	v4	Logic al		Canada	IPv6 Lab		1	0	0	-9	10/8/08 12:00 AM	-900.0%		0	0.0	0.0	0	0	v6	Logic al		Caribbean	Data		2044	0	0	2010	10/8/08 12:00 AM	98.34%	100.0%	161	0.0	0.0	0	0	v4	Logic al		Caribbean	IPv6 Lab		16	0	0	6	10/8/08 12:00 AM	37.5%		0	0.0	0.0	0	0	v6	Logic al		China	VOIP		254	0	0	244	10/8/08 12:00 AM	96.06%	100.0%	36	0.0	0.0	0	0	v4	Logic al		Japan	IPv6 Lab		1	0	0	-9	10/8/08 12:00 AM	-900.0%		0	0.0	0.0	0	0	v6	Logic al		Australia	Data		510	0	0	485	10/8/08 12:00 AM	95.1%	100.0%	125	0.0	0.0	0	0	v4	Logic al		Ireland	Data		254	0	0	230	10/8/08 12:00 AM	90.55%	100.0%	125	0.0	0.0	0	0	v4	Logic al	
Container	Block Type	Interface Name	Total IP	In Use	Locked	IPs Available	Last Update	% Free	Dynamic % Free	Dynamic Ips Available	R Squared	Dyna mic R Squared	Days Left	Dyna mic Days Left	V	Cont ainer Type	UDF																																																																																																																																																																																																																																																																																																			
InControl	Data		11842	6175	21	5449	10/8/08 12:00 AM	46.01%	20.95%	1642	0.0	0.0	0	0	v4	Logic al																																																																																																																																																																																																																																																																																																				
Europe	Data		254	0	0	230	10/8/08 12:00 AM	90.55%	100.0%	125	0.0	0.0	0	0	v4	Logic al																																																																																																																																																																																																																																																																																																				
Americas	Data		11078	6175	21	4734	10/8/08 12:00 AM	42.73%	18.34%	1392	0.0	0.0	0	0	v4	Logic al																																																																																																																																																																																																																																																																																																				
Asia	Data		510	0	0	485	10/8/08 12:00 AM	95.1%	100.0%	125	0.0	0.0	0	0	v4	Logic al																																																																																																																																																																																																																																																																																																				
Asia	VOIP		254	0	0	244	10/8/08 12:00 AM	96.06%	100.0%	36	0.0	0.0	0	0	v4	Logic al																																																																																																																																																																																																																																																																																																				
U.S.	Data		8780	6175	21	2494	10/8/08 12:00 AM	28.41%	15.15%	1106	0.0	0.0	0	0	v4	Logic al																																																																																																																																																																																																																																																																																																				
U.S.	VOIP		13098	4484	2	8528	10/8/08 12:00 AM	65.11%	26.88%	1649	0.0	0.0	0	0	v4	Logic al																																																																																																																																																																																																																																																																																																				
U.S.	IPv6 Lab		3	0	0	-20	10/8/08 12:00 AM	-666.67%		0	0.0	0.0	0	0	v6	Logic al																																																																																																																																																																																																																																																																																																				
Canada	Data		254	0	0	230	10/8/08 12:00 AM	90.55%	100.0%	125	0.0	0.0	0	0	v4	Logic al																																																																																																																																																																																																																																																																																																				
Canada	IPv6 Lab		1	0	0	-9	10/8/08 12:00 AM	-900.0%		0	0.0	0.0	0	0	v6	Logic al																																																																																																																																																																																																																																																																																																				
Caribbean	Data		2044	0	0	2010	10/8/08 12:00 AM	98.34%	100.0%	161	0.0	0.0	0	0	v4	Logic al																																																																																																																																																																																																																																																																																																				
Caribbean	IPv6 Lab		16	0	0	6	10/8/08 12:00 AM	37.5%		0	0.0	0.0	0	0	v6	Logic al																																																																																																																																																																																																																																																																																																				
China	VOIP		254	0	0	244	10/8/08 12:00 AM	96.06%	100.0%	36	0.0	0.0	0	0	v4	Logic al																																																																																																																																																																																																																																																																																																				
Japan	IPv6 Lab		1	0	0	-9	10/8/08 12:00 AM	-900.0%		0	0.0	0.0	0	0	v6	Logic al																																																																																																																																																																																																																																																																																																				
Australia	Data		510	0	0	485	10/8/08 12:00 AM	95.1%	100.0%	125	0.0	0.0	0	0	v4	Logic al																																																																																																																																																																																																																																																																																																				
Ireland	Data		254	0	0	230	10/8/08 12:00 AM	90.55%	100.0%	125	0.0	0.0	0	0	v4	Logic al																																																																																																																																																																																																																																																																																																				

Chapter 2 Getting Started

Excel

	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	UDF
	Container	Block Type	Interface Name	Total IP	In Use	Locked	IPs Available	Last Update	% Free	Dynamic % Free	Dynamic IPs Available	R Squared	Dynamic R Squared	Days Left	Dynamic Days Left	V	Container Type		
1	InControl	Data		11842	6175	21	5449	10/8/08 12:00 AM	46.01%	20.95%	1642	0.0	0.0	0	0	v4	Logical		
2	Europe	Data		254	0	0	230	10/8/08 12:00 AM	90.55%	100.0%	125	0.0	0.0	0	0	v4	Logical		
3	Americas	Data		11078	6175	21	4734	10/8/08 12:00 AM	42.73%	18.34%	1392	0.0	0.0	0	0	v4	Logical		
4	Asia	Data		510	0	0	485	10/8/08 12:00 AM	95.1%	100.0%	125	0.0	0.0	0	0	v4	Logical		
5	Asia	VOIP		254	0	0	244	10/8/08 12:00 AM	96.06%	100.0%	36	0.0	0.0	0	0	v4	Logical		
6	U.S.	Data		8780	6175	21	2494	10/8/08 12:00 AM	28.41%	15.15%	1106	0.0	0.0	0	0	v4	Logical		
7	U.S.	VOIP		13098	4484	2	8528	10/8/08 12:00 AM	65.11%	26.88%	1649	0.0	0.0	0	0	v4	Logical		

CSV

```

Container,Block Type,Interface Name,Local IP,In Use,Locked,IPs Available,Last Update,% Free,Dynamic % Free,Dynamic Ips Available,R Squared,Dynamic R Squared,Days Left,Dynamic Days Left,V,Container Type,UOF
InControl,Data,11842,6175,21,5449,10/8/08 12:00 AM,46.01%,20.95%,1642,0.0,0.0,0.0,v4,Logical,
Europe,Data,254,0.0,230,10/8/08 12:00 AM,90.55%,100.0%,125,0.0,0.0,0.0,v4,Logical,
Americas,Data,11078,6175,21,4734,10/8/08 12:00 AM,42.73%,18.34%,1392,0.0,0.0,0.0,v4,Logical,
Asia,Data,510,0.0,485,10/8/08 12:00 AM,95.1%,100.0%,125,0.0,0.0,0.0,v4,Logical,
Asia,VOIP,254,0.0,244,10/8/08 12:00 AM,96.06%,100.0%,36,0.0,0.0,0.0,v4,Logical,
U.S.,Data,8780,6175,21,2494,10/8/08 12:00 AM,28.41%,15.15%,1106,0.0,0.0,0.0,v4,Logical,
U.S.,VOIP,13098,4484,2,8528,10/8/08 12:00 AM,65.11%,26.88%,1649,0.0,0.0,0.0,v4,Logical,
U.S.,IPv6 Lab,3,0.0,-20,18/8/08 12:00 AM,-666.67%,0.0,0.0,0.0,v6,Logical,
Canada,Data,254,0.0,230,10/8/08 12:00 AM,90.55%,100.0%,125,0.0,0.0,0.0,v4,Logical,
Canada,IPv6 Lab,1,0.0,-9,10/8/08 12:00 AM,-900.0%,0.0,0.0,0.0,v6,Logical,
Caribbean,Data,2044,0.0,2010,10/8/08 12:00 AM,98.34%,100.0%,161,0.0,0.0,0.0,v4,Logical,
Caribbean,IPv6 Lab,16,0.0,0,6,18/8/08 12:00 AM,37.5%,0.0,0.0,0.0,v6,Logical,
China,VOIP,254,0.0,244,10/8/08 12:00 AM,96.06%,100.0%,36,0.0,0.0,0.0,v4,Logical,
Japan,IPv6 Lab,1,0.0,-9,10/8/08 12:00 AM,-900.0%,0.0,0.0,0.0,v6,Logical,
Australia,Data,510,0.0,485,10/8/08 12:00 AM,95.1%,100.0%,125,0.0,0.0,0.0,v4,Logical,
Ireland,Data,254,0.0,230,10/8/08 12:00 AM,90.55%,100.0%,125,0.0,0.0,0.0,v4,Logical,
Exton,Data,762,0.0,726,10/8/08 12:00 AM,95.28%,100.0%,161,0.0,0.0,0.0,v4,Logical,
Exton,VOIP,4914,0.0,4834,10/8/08 12:00 AM,98.37%,0.0,0.0,0.0,v4,Logical,
Pittsburgh,Data,892,0.0,859,18/8/08 12:00 AM,96.3%,100.0%,161,0.0,0.0,0.0,v4,Logical,
Pittsburgh,IPv6 Lab,2,0.0,-21,10/8/08 12:00 AM,-1050.0%,0.0,0.0,0.0,v6,Logical,
Albuquerque,Data,7126,175,201,909,10/8/08 12:00 AM,12.76%,11.23%,784,0.0,0.0,0.0,v4,Logical,
Albuquerque,VOIP,8184,4484,2,3694,10/8/08 12:00 AM,45.14%,26.88%,1649,0.0,0.0,0.0,v4,Logical,
ubr01.albqr001.nm.diamondip.com,Data,i50,1526,1194,4,323,10/8/08 12:00 AM,21.17%,14.18%,198,0.0,0.0,0.0,v4,Device,
ubr01.albqr01.nm.diamondip.com,Data,i50,1780,1462,4,308,10/8/08 12:00 AM,17.3%,17.36%,308,0.0,0.0,0.0,v4,Device,
ubr01.albqr01.nm.diamondip.com,VOIP,i50,2046,1201,0,844,10/8/08 12:00 AM,41.25%,41.27%,844,0.0,0.0,0.0,v4,Device,
ubr01.albqr01.nm.diamondip.com,VOIP,i50,2046,1428,0,617,10/8/08 12:00 AM,30.16%,30.17%,617,0.0,0.0,0.0,v4,Device,
ubr02.albqr01.nm.diamondip.com,Data,s01,2038,1818,9,206,10/8/08 12:00 AM,10.11%,10.13%,206,0.0,0.0,0.0,v4,Device,
ubr02.albqr01.nm.diamondip.com,Data,s11,1782,1701,4,72,10/8/08 12:00 AM,4.04%,4.05%,72,0.0,0.0,0.0,v4,Device,
ubr02.albqr01.nm.diamondip.com,VOIP,s01,2046,1855,2,188,10/8/08 12:00 AM,9.19%,9.19%,188,0.0,0.0,0.0,v4,Device,
extonhub,VOIP,BVI230,254,0.0,250,18/8/08 12:00 AM,98.43%,0.0,0.0,0.0,v4,Device,
extonhub,VOIP,BVI180,62,0.0,50,18/8/08 12:00 AM,81.55%,0.0,0.0,0.0,v4,Device,
extonhub,VOIP,BVI150,1022,0.0,999,10/8/08 12:00 AM,97.75%,0.0,0.0,0.0,v4,Device,
extonhub,VOIP,BVI160,254,0.0,251,10/8/08 12:00 AM,98.82%,0.0,0.0,0.0,v4,Device,
extonhub,VOIP,BVI220,2046,0.0,2020,18/8/08 12:00 AM,98.73%,0.0,0.0,0.0,v4,Device,
extonhub,VOIP,BVI48,254,0.0,243,18/8/08 12:00 AM,95.67%,0.0,0.0,0.0,v4,Device,
Puerto Rico,Data,380,0.0,346,10/8/08 12:00 AM,91.05%,100.0%,161,0.0,0.0,0.0,v4,Logical,
Puerto Rico,IPv6 Lab,1,0.0,-9,10/8/08 12:00 AM,-900.0%,0.0,0.0,0.0,v6,Logical,

```

XML		<pre> <?xml version="1.0" encoding="UTF-8"?> <report> <containerutilization> <container>U.S.</container> <blockType>IPv6 Lab</blockType> <interfaceName/> <totalIp>3</totalIp> <inUse>0</inUse> <locked>0</locked> <ipsAvailable>-20</ipsAvailable> <lastUpdate>2008-10-08</lastUpdate> <percentFree>-666.67%</percentFree> <dynamicPercentFree/> <r2>0.0</r2> <dynamicIpsAvailable>0</dynamicIpsAvailable> <dynamicr2>0.0</dynamicr2> <daysRemaining>0</daysRemaining> <dynamicDaysRemaining>0</dynamicDaysRemaining> <ipversion>v6</ipversion> <containerType>Logical</containerType> <udfs/> </containerutilization> <containerutilization> <container>Canada</container> <blockType>IPv6 Lab</blockType> <interfaceName/> <totalIp>1</totalIp> <inUse>0</inUse> <locked>0</locked> <ipsAvailable>-9</ipsAvailable> <lastUpdate>2008-10-08</lastUpdate> <percentFree>-900.0%</percentFree> <dynamicPercentFree/> <r2>0.0</r2> <dynamicIpsAvailable>0</dynamicIpsAvailable> <dynamicr2>0.0</dynamicr2> <daysRemaining>0</daysRemaining> <dynamicDaysRemaining>0</dynamicDaysRemaining> <ipversion>v6</ipversion> <containerType>Logical</containerType> </containerutilization> </report> </pre>
-----	-----------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Note: For best results, XML export data should be opened in a text editor or Internet Explorer.

Chapter 3 Managing IP Addresses

In IPControl 5.0, all the features you need to perform IP address management are located in the IPAM section of the Management menu. This chapter describes how to use each selection.

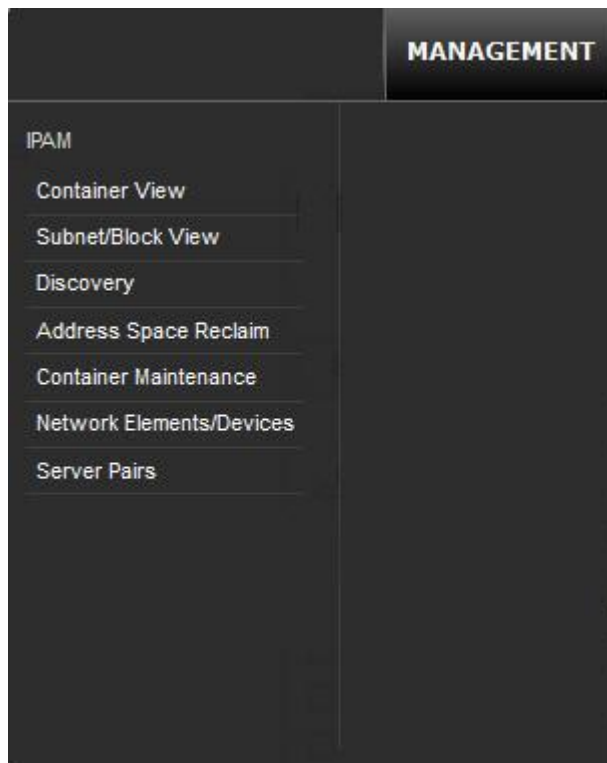


Figure 3-1 IPAM Menu

Container View

The Container View option allows you to view and manage IP Address space by using a user-defined management hierarchy. Day to day management of IP Address space is accomplished using the Container View option. Using this option, blocks are added, deleted, and split. IP Addresses are added, deleted, and allocated to network services. IPControl adheres to strict CIDR rules and maintains referential integrity of your address space.

Container View Tree Hierarchy

After logging in, or when you select the **Container View** option from the IPAM section of the **Management** menu, you see a tree hierarchy of your management containers in the left frame of your browser, as shown in Figure 3-2.

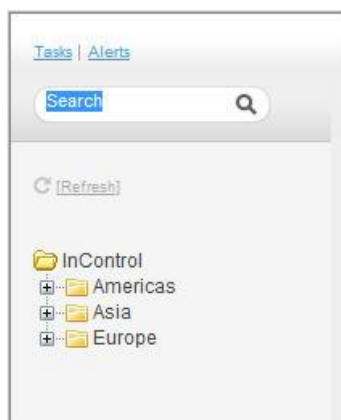



Figure 3-2 Default Container View Tree

In the Container View tree, you can choose from the following actions.

To ...	Do this ...
Expand a node in the container tree	Click the expand icon (+).
Collapse a node in the container tree	Click the collapse icon (=).
View Address Block Details for a populated logical container	Click the name of an open (📁) or closed (📁) logical container icon.
View Address Block Details for an empty logical container	Click the name of an open (📁) or closed (📁) logical container icon.
View Address Block Details for a device container with assigned blocks	Click the name of a 📁 device container icon.
View Address Block Details for a device container with no assigned blocks	Click the name of a 📁 device container icon.
View Switch Port Details	Click the name of a 📁 icon. For more information, refer to Network Switch Functions on page 50.
Refresh the Container View tree hierarchy	Click 🔄 or the Refresh link.

To ...	Do this ...
Search for a specific container	<ol style="list-style-type: none"> 1. Click in the Search field above the Container View tree hierarchy. 2. Type a search string into the text block. A Results list opens to display a bulleted list of containers that match the search criteria as you type, as shown in Figure 3-3. <div data-bbox="829 585 1166 1041" data-label="Image"> </div> <p style="text-align: center;">Figure 3-3 Container Search</p> <ol style="list-style-type: none"> 3. Select the container for which you are searching. The container tree hierarchy expands to show the selected container and the Address Block Details appear in the Container View Details frame.

Container Details

To see more details on a container, click the  [Details](#) link. A Details screen opens, as shown in Figure 3-4. Information on the type of container and when and by whom it was created is provided. If the container type is **Device**, additional information on make, vendor, device type, and IP address is provided.

Container: ubr01.albqrq01.nm.diamondip.com

Details:	
Type:	Device
Created on:	5/3/07 13:36
Created by:	incadmin
Make:	uBR7100
Vendor Name:	Cisco Systems
Device Type:	(CMTS) Cable Modem Termination System
IP Address:	10.250.200.11

Figure 3-4 Container Details

Click the ✕ icon to close the Container Details screen.

Container Address Block Details

In the Container Address Block Details on the right side of the screen, you see address block details for the management container that is currently selected in the tree hierarchy in the left frame, as shown in Figure 3-5.

Container View Tree
Container Address Block Details

The screenshot displays the IPControl web interface. On the left, the 'Container View Tree' shows a hierarchical structure starting with 'InControl' as the root container. It branches into geographical regions: Americas (including Canada, Caribbean, and U.S.), Asia, and Europe. The 'U.S.' region is expanded, showing sub-containers like Albuquerque, Exton, and Philadelphia. On the right, the 'Container Address Block Details' pane shows the 'InControl' container selected. It includes a table of address blocks assigned to this container. The table has columns for Select, Block By Type, Child Block, Size, Root, Status, Container, Parent Block, Create Date, Creator, Create Reason, and User Defined Fields. The table lists four blocks: 172.16.0.0 (IPv4 Lab), 2001:db8:56a:: (IPv6 Lab), 4ffe:da:f0:: (IPv6 Lab), and 10.0.0.0 (VOIP). Each block is an aggregate, rooted in the 'InControl' container, and was created by 'incadmin'.

Select	Block By Type	Child Block	Size	Root	Status	Container	Parent Block	Create Date	Creator	Create Reason	User Defined Fields
<input type="checkbox"/>	172.16.0.0		/12	Yes	Aggregate	InControl		10/19/11			
IPv6 Lab											
<input type="checkbox"/>	2001:db8:56a::		/48	Yes	Aggregate	InControl		7/13/11			
<input type="checkbox"/>	4ffe:da:f0::		/32	Yes	Aggregate	InControl		5/3/07	incadmin		
VOIP											
<input type="checkbox"/>	10.0.0.0		/8	Yes	Aggregate	InControl		5/3/07	incadmin		

Figure 3-5 Container Address Block Details

Root Container

The default container displayed after logging in is the Root Container, or **InControl**. You can change the default name of the Root Container using the Edit Container function, available in Container Maintenance (see “Edit Container” on page 97).

Blocks Assigned to Container

IPControl defaults to showing only blocks assigned to the currently selected container. If you want to view assigned and unassigned blocks for a container, uncheck the **Show Only Blocks Assigned to this Container** check box. The Address Block Details list changes to remove the **Select** column and shows free address space, as shown in Figure 3-6.

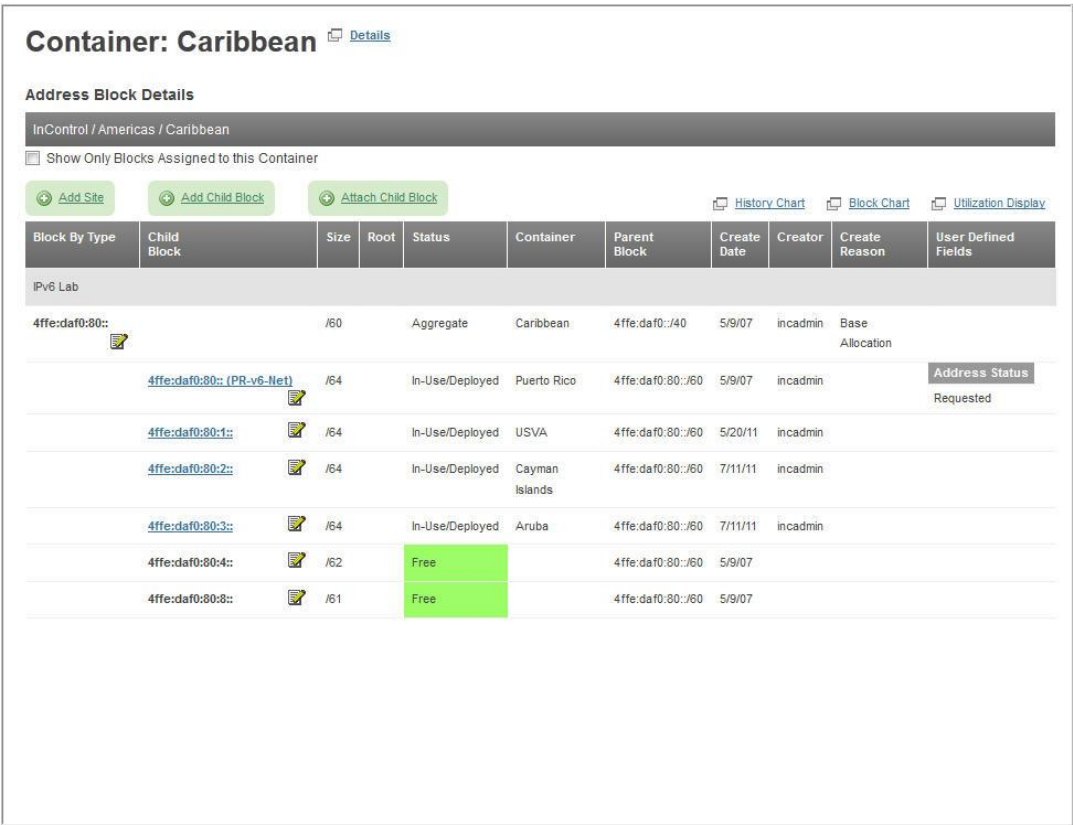


Figure 3-6 All Blocks Available to Container

Block Types

The blocks that are displayed in the container view are organized within the container by block type, for example **Data** and **Ipv6 Lab** in Figure 3-7. Block types are user defined and are created using the **Block Types** function in the SUBNET/BLOCK section of the **Tools** menu. For more information, refer to “Block Types” on page 278.

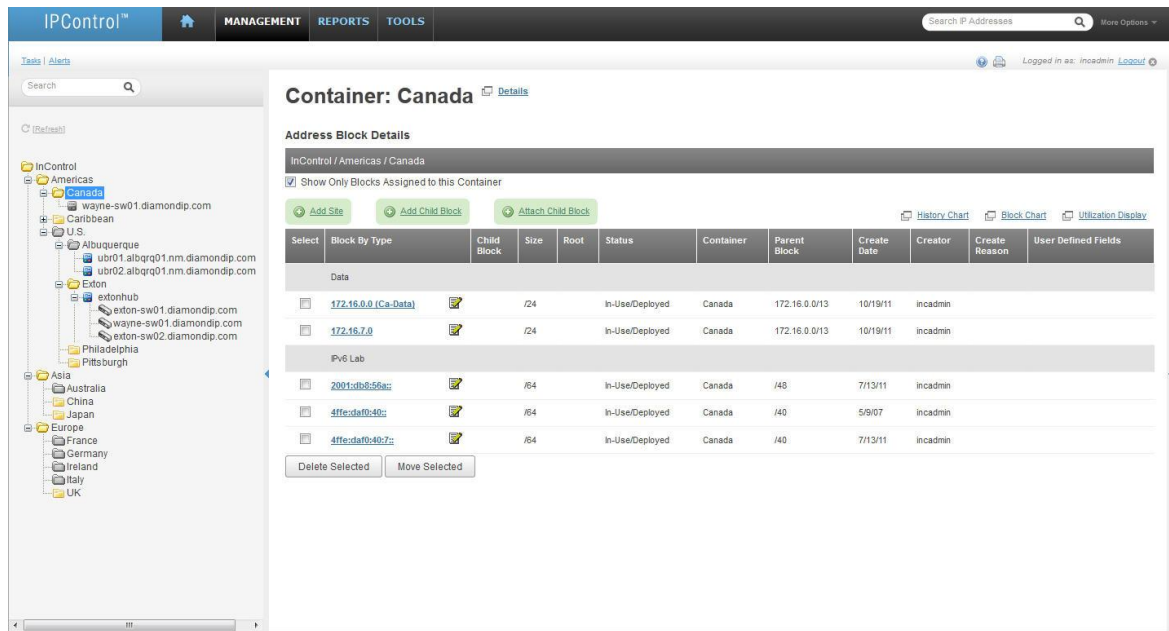



Figure 3-7 Address Block Details

Address Block Details screen components are described in Table 3-1.

Table 3-1 Address Block Details Screen Elements

Field	Description
Block By Type	Displays the blocks assigned to the selected container, organized by Block Type. If the block has a status of In User/Deployed, you can select the link and open the Subnet List screen. For more information, refer to “IP Management” on page 51.
 Child Block	Edit the properties of this block.
Child Block	The starting address of the child blocks.
Size	The size in CIDR notation of the block.
Root	If this block is a Root block, then “Yes” will be displayed in this column.
Status	The current status of this block.
Container	The name of the container that holds this block.
Parent Block	The parent block is the block from which this block was derived. <ul style="list-style-type: none"> IPv4 blocks display the starting address and size of the Parent Block of the current block. IPv6 blocks display the CIDR size only of the Parent Block.
Create Date	The date this block was created.
Creator	The administrator that created this block.
Create Reason	The reason code entered when this block was created.
User Defined Fields	The User Defined Fields that are associated with this block.

Container View Function Links

Links to several functions are available, depending on the type of container selected in the container tree hierarchy:

- **Add Site** – Click this link to add a number of blocks using a site allocation template. For more information, refer to:
 - ▶ Logical container: “Add Site” on page 31
 - ▶ Device container: “Add Site” on page 43.
- **Add Child Block** – Click this link to add a child block to this container. For more information, refer to “Add Child Block” on page 34.
- **Attach Child Block** – *Device Container only*. Click this link to model connections between devices. For more information, refer to “Attach Child Block” on page 47.
- **Add Root Block** – Click this link to add a root block to this container, as described below. This link can optionally be suppressed for this container based on the policies defined for this container in the Container Maintenance option. See the “Allow Root Block Creation” policy on page 100.
- **Block Order**– *Device Container only*. Click this link to place the blocks in a specific order.
- **Utilization Display** – Click this link to display the utilization information for the blocks in this container, as described in “Utilization Display” on page 39.
- **Block Chart** – Click this link to display the block allocation graph for the blocks located within this container, as described in “Block Chart” on page 40.
- **History Chart** – Click this link to display the chart of this container showing the overall history of address space allocated to this container, as described in “History” on page 41.

Logical Container Functions

This section describes the functions available to manage a Logical Container.

Note: Device containers contain the same options as Logical Containers plus some extra device-specific features. These differences are outlined in “Device Container Functions” on page 43.

Add Root Block

The Add Root Block display is used to initially define address space to IPControl. This includes initial allocations of space from an internet registry such as ARIN, or private [RFC 1918](#) address space. Once this space has been defined to IPControl, you use the “Add Site” and “Add Child Block” options to allocate space from this block to your network.

Container: InControl

Add Root Block

Address Space:	<input type="text"/>
Block Type:	<div>--- Please Select ---</div>
IP Address Version:	<div><input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6</div>
Block Size:	<div>--- Please Select ---</div>
Block Name:	<input type="text"/>
Block Description:	<div><input type="text"/></div>
Current Status:	<div>Aggregate</div>
Create Reverse DNS Domain(s):	<div><input type="checkbox"/> DNS Domain Type <div>Default</div></div>
Allow Overlapping Address Space:	<div><input type="checkbox"/> (Checked=Yes)</div>
Internet Registry:	<div>Generic Root Block</div>
Organization ID:	<div>None</div>
SWIP/Net Name:	<input type="text"/>
Reason for Allocation:	<div>--- Please Select ---</div>
Reason Description:	<div><input type="text"/></div>
<div>Submit</div>	

Figure 3-8 Add Root Block

Table 3-2 Add Root Block Parameters

Field	Description
Address Space	<p>Enter the starting address for the block of addresses that you are defining.</p> <ul style="list-style-type: none"> For IPv4 addresses, use standard dotted decimal notation (x.x.x.x) such as 10.0.0.0. For IPv6 addresses, use the 2 standard text conventions as defined in RFC 2373 below. <ol style="list-style-type: none"> The preferred form is x:x:x:x:x:x:x:x, where each x is the hexadecimal value of the eight 16-bit pieces of the address, such as: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210 1080:0:0:0:8:800:200C:417A Note: It is not necessary to write the leading zeros in an individual field, but there must be at least one numeral in every field (except for the case described in 2). Due to certain methods of allocating certain styles of IPv6 addresses, it is common for addresses to contain long strings of zero bits. To make writing addresses containing zero bits easier, a special syntax is available to compress the zeros. The use of :: indicates multiple groups of 16-bits of zeros. The :: can only appear once in an address. The :: can also be used to compress the leading and/or trailing zeros in an address. For example, the following address: 1080:0:0:0:8:800:200C:417A may be represented as: 1080::8:800:200C:417A
Block Type	Select from the user defined block types that have been defined in the system. This assigns this block a specific type. The list that is displayed in the “block type” list is controlled by rules defined in the container maintenance option.
IP Address Version	Select the version of IP Address space that you are adding to the system, IPv4 or IPv6. Note that the license key controls which versions of IP Address space are supported within the product.
Block Size	Select the block size that you are adding. The block sizes are listed in CIDR notation.
Block Name	<p>Enter the name of a block, or use the system supplied name of {Address space/BlockSize}.</p> <p>Note: The block name appears on the container screen.</p>
Block Description	Enter a description of the block.
Current Status	<p>The current status of this block:</p> <p>Aggregate – This block is an aggregate block.</p> <p>Note: All root blocks have an aggregate status.</p>

Field	Description
Create Reverse DNS Domain(s)	If this option is checked, the system automatically creates an in-addr.arpa reverse domain for this address space. You can optionally select the “type” if you have overlapping address space. Domain types are defined in Domain Types in the DNS section of the Management menu, as defined in “DNS Domain Types” on page 160. Note: You must still assign this domain to a DNS server or a DNS galaxy using the Management > DNS menu. This option only creates the reverse domain for you.
Allow Overlapping Address Space	If this option is checked, this address space may be defined multiple times within the system. This allows for overlapping address space if needed. Any overlapping space must not be in the same container or any of its parents. It is recommended that you do not check this option, unless you specifically want to define duplicate address space within the product.
Internet Registry	If this is public IP Address space, select the Internet Registry from which you received this block. If this is private IP Address space, select RFC1918 . For any other types of blocks, select Generic Root Block .
Organization ID	Default is None . Select an ID that has already been defined via System Setup.
SWIP/Net Name	Enter the SWIP name (specific to the ARIN Internet Registry) or the Net Name (specific to RIPE). This is an optional field unless the rules specified on this container require the SWIP/Net Name.
Reason for Allocation	Select the reason why this block is being allocated. Reasons are defined by your IPControl administrator. For more information, refer to “Allocation Reason Code” on page 277.
Reason Description	Enter an optional description that outlines why this block is being allocated.

Add Site

Use the Add Site screen to select a previously defined site allocation template to apply to the currently selected container. For more information on creating site allocation templates, refer to “Site Allocation Templates” on page 284.

Container: Americas

Add Site

Site Allocation Template: --- Please Select ---

#	Block Type	IP Version	Block Size	Allocation Strategy	Block Name	Block Status	Address Allocation Template	SWIP / Net Name	Allocation Reason	Allocation Reason Description
<div> <input type="button" value="Submit"/> <input type="button" value="Cancel"/> </div>										

Figure 3-9 Add Site

To add a site with a site allocation template, follow these steps.

1. Select a logical container in the Container Tree.
The Address Block Details screen (Figure 3-7) for the selected container opens.
2. Click the **Add Site** link.
The Add Site screen opens, as shown in Figure 3-9.
3. Select the site allocation template you want to use from the **Site Allocation Template** drop-down list. Only site allocation templates defined for logical containers are listed.
A sequenced list of blocks in the selected template appears.

Figure 3-10 Logical Container Add Site List

4. Enter block-specific data in the fields, as described in Table 3-3.

Table 3-3 Add Site Parameters

Field	Description
SWIP/Net Name	<i>Optional</i> (unless the rules specified on this container require the SWIP/Net Name). Enter the SWIP name (specific to the ARIN Internet Registry) or the Net Name (specific to RIPE).
Reason for Allocation	<i>Optional</i> . Select the reason why this block is being allocated. Reasons are defined by your IPControl administrator. For more information, refer to “Allocation Reason Code” on page 277.
Reason Description	<i>Optional</i> . Enter a description that outlines why this block is being allocated.

5. If an address allocation template is included in the site template, select the link and enter any data required for the address template, for example, network service and shared network name.

Starting Offset	Starting Offset From	Ending Offset	Ending Offset From	Address Type	Create Individual IP Objects	Create Resource Record	Device Type	Network Service	Shared Network Name
1	Beginning of Subnet	1	Beginning of Subnet	Static	Yes	Yes	Router	--- Same as Subnet --	
2	Beginning of Subnet	3	Beginning of Subnet	Static	Yes	Yes	Router	--- Same as Subnet --	
4	Beginning of Subnet	6	Beginning of Subnet	Automatic DHCP	Yes	Yes	Printer	--- Same as Subnet --	
7	Beginning of Subnet	12	Beginning of Subnet	Static	Yes	Yes	File Server	--- Same as Subnet --	
16	Beginning of Subnet	48	Beginning of Subnet	Dynamic DHCP	No	No	Unknown	--- Same as Subnet --	

Figure 3-11 Edit Address Allocation Template for a Logical Container

- ▶ **Network Service** – Select a previously-defined network service from the drop-down list. For information on network service, refer to “Network Services List” on page 186.
The contents of the Network Service list are dependent on the **Limit DHCP Servers by Container Tree** system policy, as follows:
 - **false:** Displays all DHCP servers in the system.
 - **one:** Automatically set to the single network service assigned to the parent container.
 - **many:** Displays list of network services assigned to the parent container.
- ▶ **Shared Network Name** – Enter a unique name that is specific to the physical network. All pools that share the same physical network should be declared with the same shared network name.

Note: If the **Enable Primary Subnet Handling** system policy is set to **true**, the shared subnet name is automatically set to the name of the primary subnet on the device interface.

6. If user-defined fields are associated with a block, click the **UDFs** button and enter the required data. Click **Submit** to save the UDF data.
7. Click **Submit**.
The Edit Address Allocation Template screen closes.
8. Click **Submit**.
The subnet is added to the Address Block Details list.

Add Child Block

The Add Child Block display is used to define sub-allocations of address space to IPControl. Sub-allocations are taken from parent address space. This space is allocated from the parent, and then marked with the status that has been selected.

General Tab

For Logical Containers, the **General** tab shows:

Container: Americas

Add Child Block

General

Policies

Block Type

--- Please Select ---

IP Address Version

IPv4

IPv6

Block Size

--- Please Select ---

Parent Block

Best fit

Manual

--- Please Select ---

Sort by

Block Type and Size

Address

Exclude from Discovery

☐

Discovery Agent

Inherit from Parent Block

Inherit from Parent Container

Select Agent

Executive Agent

Address Space

Block Name

Block Description

Current Status

In Use/Deployed

Create Reverse DNS Domain(s)

☐

DNS Domain Type

Default

SWIP/Net Name

Reason for Allocation

--- Please Select ---

Reason Description

Allocation Template

--- Please Select ---

Address Allocation

Starting Offset	Starting Offset From	Ending Offset	Ending Offset From	Address Type	Create Individual IP Objects	Create Resource Records	Default Gateway	Device Type	Network Service	Shared Network Name
<div>Submit</div>										

Figure 3-12 Add Child Block to Logical Container

Table 3-4 General Tab Parameters

Field	Description
Block Type	Select from the user-defined block types that have been defined in the system. This assigns this block a specific type. The list that is displayed in the “block type” list is controlled by rules defined in the container maintenance option.

Field	Description
IP Address Version	Select the version of IP Address space that you are adding to the system, IPv4 or IPv6. Note that the license key controls which versions of IP Address space are supported within the product.
Block Size	Select the block size that you are adding. The block sizes are listed in CIDR notation.
Parent Block	<ul style="list-style-type: none"> • To use the automated “best fit” allocation routine, select the “Best fit” option. • To use the automated “random”(IPv6 only) allocation routine, select the “Random” option. • To use the automated “sparse”(IPv6 only) allocation routine, select the “Sparse” option. • To manually select the parent block to use for the space allocation, select “Manual”. The drop-down list will be populated with space that can be used for the allocation based on the version, size, and type entered above. <p>In either case the selection of allocation candidate blocks follows the rules defined for the container.</p>
Exclude from Discovery	Select this checkbox if you want this address space to be ignored during the discovery process.
Discovery Agent	<p>Allows you to specify the InControl Agent that will be used to “discover” hosts on this subnet/block.</p> <p>Inherit from Parent Block – Indicates that the agent specified on the parent block will be used for discovery.</p> <p>Inherit from Container – Indicates that the agent specified on the container will be used for discovery.</p> <p>Select Agent – allows you to select and specify a specific agent that will perform discovery for this subnet/block.</p>

Field	Description
Address Space	<p>Enter the starting address for the block of addresses that you are defining.</p> <ul style="list-style-type: none"> For IPv4 addresses, use standard dotted decimal notation (x.x.x.x) such as 10.0.0.0. For IPv6 addresses, use the 2 standard text conventions as defined in RFC 2373 below. <ol style="list-style-type: none"> The preferred form is x:x:x:x:x:x:x:x, where each x is the hexadecimal value of the eight 16-bit pieces of the address, such as: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210 1080:0:0:0:8:800:200C:417A Note: It is not necessary to write the leading zeros in an individual field, but there must be at least one numeral in every field (except for the case described in 2). Due to certain methods of allocating certain styles of IPv6 addresses, it is common for addresses to contain long strings of zero bits. To make writing addresses containing zero bits easier, a special syntax is available to compress the zeros. The use of :: indicates multiple groups of 16-bits of zeros. The :: can only appear once in an address. The :: can also be used to compress the leading and/or trailing zeros in an address. For example, the following address: 1080:0:0:0:8:800:200C:417A may be represented as: 1080::8:800:200C:417A
Block Name	<p>Enter a name of the block (manual parent block selection only), or use the system supplied name of {Address space/BlockSize}.</p> <p>Note: The block name appears on the container screen.</p>
Block Description	Enter a description of the block.
Current Status	<p>The current status of this block:</p> <ul style="list-style-type: none"> Aggregate – This block is an aggregate block. In-Use/Deployed – The block is in use as a subnet. In-Use/Fully Assigned – The block is in use and all IP Addresses are fully utilized. Reserved – This block is reserved for future use.
Create Reverse DNS Domain(s)	<p>If this option is checked, the system automatically creates an in-addr.arpa reverse domain for this address space. You can optionally select the “type” if you have overlapping address space. Domain types are defined in Domain Types in the DNS section of the Management menu, as defined in “DNS Domain Types” on page 160.</p> <p>Note: You must still assign this domain to a DNS server or a DNS galaxy using the Management > DNS menu. This option only creates the reverse domain for you.</p>
SWIP/Net Name	<p>Enter the SWIP name (specific to the ARIN Internet Registry) or the Net Name (specific to RIPE). This is an optional field unless the rules specified on this container require the SWIP/Net Name.</p>

Field	Description
Reason for Allocation	Select the reason why this block is being allocated. Reasons are defined by your IPControl administrator. For more information, refer to “Allocation Reason Code” on page 277.
Reason Description	Enter an optional description that outlines why this block is being allocated.
Allocation Template	Select from the user-defined Allocation Templates that have been defined in the system. This assigns this block the address allocation rules defined for the selected Allocation Template.

Policies Tab

The **Policies** tab provides further Child Block configuration options:

Container: Americas

Add Child Block

General Policies

Default Gateway:

Primary DHCP Server:

Failover DHCP Server:

Primary WINS Server:

DHCP Policy Set:

DHCP Options Set:

Forward Domains: [Add Domains](#)
(→ = Default)

Reverse Domains: [Add Domains](#)
(→ = Default)

DNS Servers: [Add DNS Server](#)
(→ = Default)

Figure 3-13 Add Child Block Policies Tab

Table 3-5 Policies Tab Parameters

Field	Description
Default Gateway	The IP Addresses of the default gateway for this subnet. Used to provide this information to DHCP for Dynamic Address types. You may specify multiple IP Addresses by typing them in a comma-separated format, for example: 192.168.1.1, 192.168.1.2 For more information on defining a default gateway, refer to “Defining a Default Gateway” on page 46.
Primary DHCP Server	Select the Primary DHCP server that serves this address space.
Failover DHCP Server	Select the Failover DHCP server that serves this address space.

Field	Description
Primary WINS Server	The IP Addresses of the Primary WINS Servers for this subnet. Used to provide this information to DHCP for Dynamic Address types. You may specify multiple IP Addresses by typing them in a comma separated format, for example: 192.168.1.1,192.168.1.2
DHCP Policy Set	Select the default DHCP Policy set to assign to dynamic devices on this subnet.
DHCP Option Set	Select the default DHCP Option set to assign to dynamic devices on this subnet. To create a set specifically for this subnet, select Subnet Specific Option Set . Use the View/Edit link to edit the set.
Effective DHCP Options	<i>Edit Only.</i> When editing an existing In-Use/Deployed Child Block (that is, a Subnet), a button will be available which will show a popup page displaying the currently saved DHCP options which are effective for this subnet. The effective options for the subnet are determined by combining DHCP options from the option set assigned to the current Primary DHCP Server for the subnet with options from the current DHCP Option Set assigned to this subnet.
Forward Domains	Select the default DNS Forward domains for this subnet. These appear in the drop-down list when defining devices. If multiple domains are specified, then the default that is used when adding objects is the first one in the list (an arrow appears next to the default).
Reverse Domains	Select the default DNS Reverse domains for this subnet. This domain is used to hold DNS PTR records. Note that this is optional; if no default is specified, the system automatically calculates the correct reverse zone for DNS PTR records. If multiple domains are specified, the default that is used when adding objects is the first one in the list (an arrow appears next to the default).
DNS Servers	Select the default DNS Servers for this subnet. Used to provide this information to DHCP for Dynamic Address types. If multiple DNS servers are specified, the default that is used when adding objects is the first one in the list (an arrow appears next to the default).

Important Note: For flexibility, IPControl optionally allows for the creation of the same domain name (both forward and reverse) multiple times within the system. It is required that each of these domains be placed in a separate “DNS Domain Type” namespace. An example of this is when you have overlapping private address space, being managed by two different DNS servers. It is required that if you are using the same domain name more than once, then you must specify the “default domains” on the subnet’s “policies” screen above. This permits the system to place the automatically generated DNS Resource Records in the correct domain(s) for this subnet.

Address Pool Allocation

If you select a Block Status of **In Use/Deployed**, the form displays additional input fields for the creation of **Address Pools**.

Starting Offset	Starting Offset From	Ending Offset	Ending Offset From	Address Type	Create Individual IP Objects	Create Resource Records	Default Gateway	Device Type	Network Service	Shared Network Name
2	Beginning of Subnet	4	Beginning of Subnet	Static Address	Yes	Yes	Yes	Router		
5	Beginning of Subnet	9	Beginning of Subnet	Automatic DHCP	Yes	Yes	No	Printer	--- Same as Subnet ---	
10	Beginning of Subnet	20	Beginning of Subnet	Static Address	Yes	Yes	No	File Server		
21	Beginning of Subnet	30	Beginning of Subnet	Static Address	Yes	Yes	No	Desktop		
31	Beginning of Subnet	100	Beginning of Subnet	Dynamic DHCP	No	No	No		--- Same as Subnet ---	
101	Beginning of Subnet	150	Beginning of Subnet	Dynamic DHCP	No	No	No		--- Same as Subnet ---	
151	Beginning of Subnet	200	Beginning of Subnet	Reserved	Yes	No	No	Desktop		

Figure 3-14 Address Pool Allocation

This allows you to create **Address Pools** from the newly created Block. To do so, select an Allocation Template from the **Allocation Template** field. See “Address Pool Allocation Template” on page 281 for instructions on creating these templates.

Once you select a template, the screen will refresh with a new set of rows, one for each row in the template.




Utilization Display

The **Utilization Display** link is used to display the details about the utilization of the selected container.

Container: Exton Details													
Utilization Display													
<input checked="" type="checkbox"/> Show Only Blocks Assigned to this Container													
<input type="button" value="Add Site"/> <input type="button" value="Add Child Block"/> <input type="button" value="Attach Child Block"/> History Chart Block Chart Address Block Details 													
Block By Type	Child Block	Size	Utilization	Util %	Usable Hosts	Assigned Hosts	Dyn. Hosts	Locked	Static	Leasable Hosts	Lease %	Subnet Loss	History
Data				0%	508	0	0	0	0	0	0%	4	History
172.16.11.0 (Exton Net 1)		/24		0%	254	0	0	0	0	0	0%	2	History
172.18.20.0 (Exton EngNet)		/24		0%	254	0	0	0	0	0	0%	2	History
IPv6 Lab				0%	1 / 128	0	0	0	0	0	0%	0	History
4ffe:daf0:0:1:: (4FFE:DAF0:0000:0001::/64)		/64		0%	1 / 128	0	0	0	0	0	0%	0	History
VOIP				0%	126	0	0	0	0	0	0%	2	History
10.30.4.128 (Exton VoipNet)		/25		0%	126	0	0	0	0	0	0%	2	History

Figure 3-15 Utilization Display

Table 3-6 Utilization Display Screen Elements

Field	Description
 and 	Changes the display format of IPV6 hosts. See “Displaying IPV6 Capacities” on page 14 for more information.
	Edit the properties of this block.
Child Block	The starting address of the child blocks.
Size	The size in CIDR notation of the block.
Utilization	A graph of the current utilization of the block.
Util %	The percentage of this block that is currently utilized.
Usable Hosts	The number of usable hosts that are contained within the current block
Assigned Hosts	The number of hosts that are in use in this block.
Dynamic Hosts	The number of dynamic hosts within the subnet or block. This is inclusive of the “locked” hosts.
Locked	The number of Locked addresses in this block.
Static	The number of Static addresses in this block.
Leasable Hosts	The number of dynamic addresses available to DHCP for allocation.
Lease %	The percentage of dynamic addresses leased to clients.
Subnet Loss	The number of addresses lost due to subdivision of this block.
History	Click this link to display a history graph of the utilization for the current block.

Block Chart

The block chart option allows you to graph the allocations of address space to a specific container. It can be used to quickly visualize the details of the blocks, and to show contiguous areas of space.

The chart defaults to a pie chart but you can change the display to a bar chart by selecting **Bar Chart**.

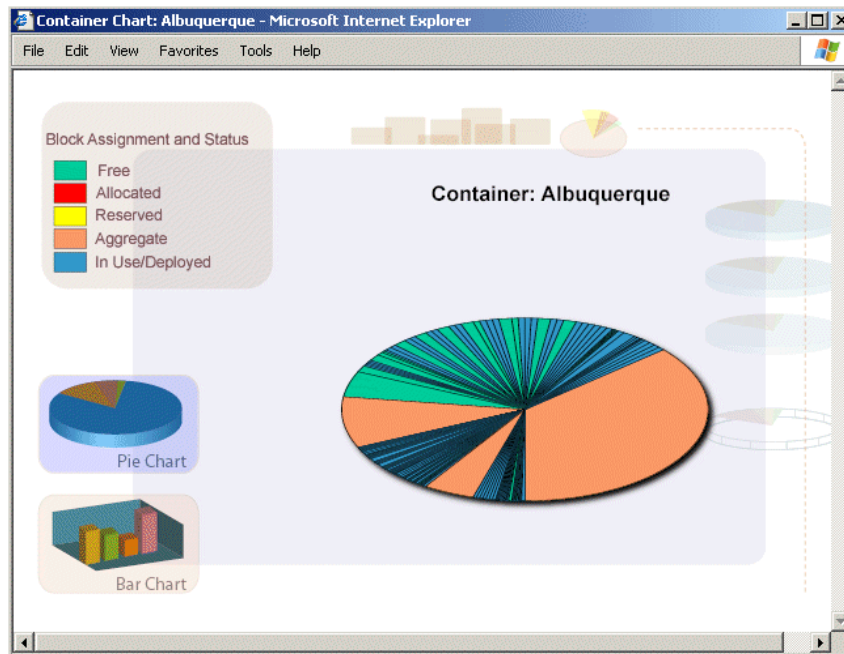


Figure 3-16 Block Chart

History Chart

The **History Chart** graphs the history of address space utilization over time for this container. It allows you to visualize overall address space, used space, and provides a forecast of space usage based on the history data.



Figure 3-17 History Chart

Table 3-7 History Chart Screen Elements

Field	Description
Forecast	Enter the number of periods (past the current date) that you want to create a forecast for.
Periods	<p>Enter the number of history periods that you want to be included in the graph.</p> <p>Select the “Periods” in the drop-down list.</p> <ul style="list-style-type: none">• Days – View the history data by days.• Weeks – View the history data by weeks.• Months – View the history data by months.• Years – View the history data by years.
Use Dynamic Data	Checked indicates the data for the graph is filtered to only show data for the Dynamic hosts for the given history period. The days left calculation is also relative to the dynamic host numbers.
Width	The Width in pixels of the graph.
Height	The Height in pixels of the graph.
Zero Min. Y	When checked, always includes zero on the Y axis.

Device Container Functions

Add Site

Use the Add Site screen to select a previously defined site allocation template to apply to the currently selected device container. For more information on creating site allocation templates, refer to “Site Allocation Templates” on page 284.

Figure 3-18 Add Site

To add a site with a site allocation template, follow these steps.

1. Select the site allocation template you want to use from the **Site Allocation Template** drop-down list. Only site allocation templates defined for device containers are listed. A sequenced list of blocks in the selected template appears.

Figure 3-19 Site Allocation Template Blocks for a Device Container

2. Enter block-specific data in the fields, as described in the following table.

Table 3-8 Site Allocation Template Block Parameters

Field	Description
Interface	Select the Interface that the address space will be allocated to from the drop-down list.
SWIP/Net Name	Enter the SWIP name (specific to the ARIN Internet Registry) or the Net Name (specific to RIPE). This is an optional field unless the rules specified on this container require the SWIP/Net Name.
Reason for Allocation	Select the reason why this block is being allocated. Reasons are defined by your IPControl administrator. For more information, refer to “Allocation Reason Code” on page 277.
Reason Description	Enter an optional description that outlines why this block is being allocated.

3. If an address allocation template is included in the site template, select the link and enter any data required for the address template, for example, network service and shared network name.

Starting Offset	Starting Offset From	Ending Offset	Ending Offset From	Address Type	Create Individual IP Objects	Create Resource Record	Device Type	Network Service	Shared Network Name
1	Beginning of Subnet	1	Beginning of Subnet	Static	Yes	Yes	Router	--- Same as Subnet ---	

Submit Cancel

Figure 3-20 Edit Address Allocation Template for a Device Container

- ▶ **Network Service** – Select a previously-defined network service from the drop-down list. For information on network service, refer to “Network Services List” on page 186. The contents of the Network Service list are dependent on the **Limit DHCP Servers by Container Tree** system policy, as follows:
 - **false:** Displays all DHCP servers in the system.
 - **one:** Automatically set to the single network service assigned to the parent container.
 - **many:** Displays list of network services assigned to the parent container.
- ▶ **Shared Network Name** – Enter a unique name that is specific to the physical network. All pools that share the same physical network should be declared with the same shared network name.

Note: If the **Enable Primary Subnet Handling** system policy is set to **true**, the shared subnet name is automatically set to the name of the primary subnet on the device interface.

4. If user-defined fields are associated with a block, click the **UDFs** button and enter the required data. Click **Submit** to save the UDF data.
5. Click **Submit**.
The Edit Address Allocation Template screen closes.
6. Click **Submit**.
The subnet is added to the Address Block Details list.

Device Container Child Blocks

When you allocate child blocks on a Device Container, you must assign at least one interface on the network element to an IP address in the child block. If you use an address allocation template to allocate child blocks on a Device Container, IPControl ensures that you do not use a template that would create devices with the same IP addresses as those assigned to the network element interfaces.

When allocating space to a Device container, you must first select the Interface to which the space will be attached, and then specify the Interface Address for that space.

The screen for allocating space to a device container has all the fields that are available for logical containers, with the addition of some device-specific information.

Container: extonhub

Add Child Block

General Policies

Interface	--- Please Select ---	
Block Type	--- Please Select ---	
IP Address Version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	
Block Size	--- Please Select ---	
Parent Block	<input checked="" type="radio"/> Best fit <input type="radio"/> Manual	<div> --- Please Select --- 192.168.4.0/22 (Any) 192.168.132.0/22 (Any) 172.16.40.0/21 (Any) 172.18.8.0/21 (Any) </div>
Exclude from Discovery	<input type="checkbox"/>	
Discovery Agent	<input type="radio"/> Inherit from Parent Block <input checked="" type="radio"/> Inherit from Parent Container <input type="radio"/> Select Agent Executive Agent	
Interface IP Address	Number of IP Address(es): 1 <div> Addr 1: <input checked="" type="radio"/> Auto allocate Offset From Start 1 <input type="radio"/> Manual IP Address <input type="text"/> <input type="checkbox"/> Default Gateway </div>	
Address Space	<input type="text"/>	
Block Name	<input type="text"/>	
Block Description	<input type="text"/>	
Current Status	In Use/Deployed	
Create Reverse DNS Domain(s)	<input type="checkbox"/>	
DNS Domain Type	Default	
SWIP/Net Name	<input type="text"/>	
Reason for Allocation	--- Please Select ---	
Reason Description	<input type="text"/>	
Allocation Template	--- Please Select ---	

Address Allocation

Starting Offset	Starting Offset From	Ending Offset	Ending Offset From	Address Type	Create Individual IP Objects	Create Resource Records	Default Gateway	Device Type	Network Service	Shared Network Name
<div>Submit</div>										

Figure 3-21 Device Container Add Child Block

Table 3-9 Additional Device Child Block Fields

Field	Description
Interface	Select the Interface that the space will be allocated to.
Interface IP Address	Number of IP Addresses Choose the number of IP addresses this block will have on this interface. Typically, this will be one. However, there are some high-availability configurations where more than one is needed. If you are not sure, leave this at one.
	Auto allocate Select this radio button to have IPControl calculate the Interface IP Address using the Offset From Start field.
	Offset From Start Use this in conjunction with Auto allocate to have IPControl calculate the Interface Address. If selected, the Interface Address is the Block Starting address plus this Offset.
	Manual Select this radio button if you wish to enter the Interface IP address manually.
	IP Address This field is enabled only when Manual is selected. Fill in the desired Interface IP Address. The supplied address must be within the allocated block.
	Default Gateway Select this option to designate that the Interface IP Address is the default Gateway address. For more information, refer to “Defining a Default Gateway” following.
Primary Subnet	When using shared subnets (see Enable Primary Subnet Handling in System Policies on page 264), select this check box if the subnet you are creating should be the primary subnet. Otherwise, leave blank.

Defining a Default Gateway

IPControl now supports three methods that you can use to specify that an interface IP address be designated as the Default Gateway when you allocate a child block:

1. Explicitly list the default gateway IP(s) on the **Subnet Policies** tab (if administrator privileges allow), as described in “Policies Tab” on page 37.

Note: If this method is used, IPControl does not let you use the following two methods.

2. Use an Address Allocation Template with the **Default Gateway** option, as described in “Address Pool Allocation Templates” on page 281.
3. Select the **Default Gateway** checkbox on one or more interface IPs, when allocating a block on a Device Container, as described above in “Device Container Child Blocks”.

Methods 2 and 3 can be used together, but with the following restrictions:

- If the IPs allocated by the address template conflict or overlap with the IPs assigned to the network element interfaces, an error is generated.
- If the IPs do not conflict or overlap, then the **Default Gateway** field for the Subnet Policies is populated with the interface IPs in which the **Default Gateway** checkbox is selected, followed by any default gateway IPs created by the address allocation template.

In most cases, the router addresses that are assigned to DHCP clients (that is, the default gateways) are simply the interface IP addresses. In these cases, the **Default Gateway** field on the Subnet Policies screen should be populated with the IP addresses assigned to the network element interfaces.

Attach Child Block

The **Attach Child Block** function allows for the same block to exist in multiple locations. In versions prior to 2.2.173, this functionality was only available to Device containers. Now this can be done with Device containers or Logical containers, and an attached block is not restrained by the container type. A block created in a Device container can be attached to a Logical container, and vice versa.

The **Attach Child Block** function for Device containers links an *existing* block to a specified interface on the current device container.

Container: extonhub

Attach Child Block

IP Address Version: ☒ IPv4 ☐ IPv6

Block Size:

Block Type:

Select Block to Attach: ☒ Select Block From List ☐ Specify Block

Attach to Interface:

Number of IP Address(es):

Interface IP Address:

Addr 1: ☒ Auto allocate ☐ Manual ☐ First Available from Start ☐ First Available from End

Figure 3-22 Device Container Attach Child Block

Table 3-10 Attach Child Block Fields

Field	Description
Block Size	Select the CIDR size of the block you wish to attach.
Block Type	Select the Block Type to attach. Note that this list is limited to those block types that are marked as Attachable. It is further limited by the administrator's Block Type permissions. See Block Type Maintenance for instructions on setting up Attachable block types.
Select Block to Attach	Select the <i>existing</i> block to attach. If you choose the Select Block from List Option , the drop-down box shows a list of candidate blocks that match the Block Size and Block Type and have an available IP Address. If you choose the Specify Block option, you can type in the starting address of a block. The specified block must match the specified block size and type.
Attach to Interface	<i>For blocks being attached to Device containers only.</i> Select the Device Interface to which this block will be attached.
Number of IP Addresses	Choose the number of IP addresses this block will have on this interface. Typically, this will be one. However, there are some high-availability configurations where more than one is needed. If you are not sure, leave this at one.
Auto-Allocated	<i>For blocks being attached to Device containers only.</i> Select this radio button to have IPControl calculate the Interface IP Address using the Offset From Start field.
Offset From Start	Use this in conjunction with the Auto Allocated selection to have IPControl calculate the Interface Address. If selected, the Interface Address will be the Block Starting address plus this Offset. Note: This offset cannot conflict with the Interface Addresses already in use by the other devices.
Manual	<i>For blocks being attached to Device containers only.</i> Select this radio button if you wish to enter the Interface IP address manually.
IP Address	This field is enabled only when the Manual option is selected. Fill in the desired Interface IP Address. The supplied address still must be within the allocated block. Furthermore, it cannot conflict with the Interface Addresses already in use by the other devices.
First Available From Start	<i>For blocks being attached to Device containers only.</i> Select this radio button if you wish IPControl to determine the first unused IP address from the beginning of the block to use as the interface address.
First Available From End	<i>For blocks being attached to Device containers only.</i> Select this radio button if you wish IPControl to determine the first unused address from the end of the block to use as the interface address.

There are several rules that govern when blocks may be attached to each other.

When you try to pick the block from the list, the list is filtered on the following things:

- The blocktype must be marked as Attachable to multiple containers.
- The blocktype must be allowable in the container to be attached.

- The block size must be allowable in the container to be attached.
- There must be a pre-existing block.
- If the pre-existing block resides in a Logical container then it must be allocated as In Use/Deployed.
 - ▶ There is no restriction on the block status if the pre-existing block resides in a Device container, though it is recommended only attaching In-Use/Deployed blocks together.
- If you do not select a block from the list, the validations are:
 - ▶ The blocktype must be marked as Attachable to multiple containers.
 - ▶ The blocktype must be allowable in the container to be attached.
 - ▶ There must be a pre-existing block.
 - ▶ The pre-existing block must be already assigned to a Device container.

Block Order

This link only appears on Device Containers. Use this to place the blocks in a specific order.

Container: ubr01.albqrq01.nm.diamondip.com

Manage Interface Block Order

[Address Block Details](#)

	Size	Status	IP Address		
i3/o					
10.168.0.0	/21	In-Use/Deployed	10.168.0.1	<button>Up</button>	<button>Down</button>
172.16.12.0	/22	In-Use/Deployed	172.16.12.1	<button>Up</button>	<button>Down</button>
172.18.5.0	/25	In-Use/Deployed	172.18.5.1	<button>Up</button>	<button>Down</button>
172.18.17.0	/25	In-Use/Deployed	172.18.17.1	<button>Up</button>	<button>Down</button>
i5/o					
10.168.8.0	/21	In-Use/Deployed	10.168.8.1	<button>Up</button>	<button>Down</button>
172.16.17.128	/25	In-Use/Deployed	172.16.17.129	<button>Up</button>	<button>Down</button>
172.16.24.0	/22	In-Use/Deployed	172.16.24.1	<button>Up</button>	<button>Down</button>
172.16.35.0	/24	In-Use/Deployed	172.16.35.1	<button>Up</button>	<button>Down</button>
172.18.5.128	/25	In-Use/Deployed	172.18.5.129	<button>Up</button>	<button>Down</button>

Figure 3-23 Device Container Block Order

- To access the specific details of the Address Block, click on the IP address.

- To move the blocks up and down in the list, use the corresponding **Up** and **Down** links.

Network Switch Functions

Selecting a network switch icon within the Container Hierarchy causes the display in the right pane to change to a view of the ports that have been discovered on the switch using the “Discover Switch Ports” task in the Discovery/ Collectors section. For more information, refer to “Discovery/Collector Task Definition Options” on page 85.

To view more address information, pause the cursor on an address link, as shown in Figure 3-24. To edit an address, click on the link to open the Edit IP Address screen. For more information, refer to “Editing an IP Address” on page 64.

Container:extonhub:exton-
sw01.diamondip.com

Switch Port Details
☐ Show Used Ports Only

Interface Name	Interface Type	Status	Port Speed	Device HW Address	IP Address	Host Name	Domain Name
sl0	Unknown	Up	9600 bps				
1/1	Ethernet	Up	100 Mbps				
1/2	Ethernet	Up	100 Mbps				
2/1	Ethernet	Up	10 Mbps				
2/2	Ethernet	Up	10 Mbps				
2/3	Ethernet	Up	10 Mbps				
2/4	Ethernet	Up	10 Mbps				
2/5	Ethernet	Up	10 Mbps				
2/6	Ethernet	Up	100 Mbps	080020918CD3	10.30.48.70	prtr-z98	dev.diamondip.com
2/7	Ethernet	Up	10 Mbps				

1 2 3 4 5 6 Next [Last]

Page size: 10

Id122

Type4

Device typePrinter

Subnet10.30.48.0/24

Containerextonhub

Device interfaces

Default

Resource Records

Figure 3-24 Network Switch View

IP Management

In the Address Block Details list, all blocks that appear in the **Block By Type** column as a hyperlink have a status of In-Use/Deployed, as shown in Figure 3-25.








Container: Pittsburgh [Details](#)

Address Block Details

InControl / Americas / U.S. / Pittsburgh

☒ Show Only Blocks Assigned to this Container

[Add Site](#)
[Add Child Block](#)
[Attach Child Block](#)
[History Chart](#)
[Block Chart](#)
[Utilization Display](#)

Select	Block By Type	Child Block	Size	Root	Status	Container	Parent Block	Create Date	Creator	Create Reason	User Defined Fields
Data											
<input type="checkbox"/>	172.16.18.0		/24		Reserved	Pittsburgh	172.16.0.0/13	10/19/11	incadmin		Address Status Requested
<input type="checkbox"/>	172.16.32.0 (Pitt-Production-1)		/23		In-Use/Deployed	Pittsburgh	172.16.0.0/13	10/19/11	incadmin		Address Status Requested
<input type="checkbox"/>	172.18.7.0		/24		In-Use/Deployed	Pittsburgh	172.16.0.0/13	10/21/11	incadmin		Address Status Requested
<input type="checkbox"/>	192.168.129.0		/24		In-Use/Deployed	Pittsburgh	192.168.0.0/16	7/13/11	incadmin	Base Allocation	Address Status requested,Requested,false,assigned,Assigned,false,pending,Pending,false,aging,Aging,false;
Pv6 Lab											
<input type="checkbox"/>	2001:db8:56a:1::		/64		In-Use/Deployed	Pittsburgh	/48	7/13/11	incadmin		
<input type="checkbox"/>	4ffe:daf0:: (Pitt-v6-Lab)		/64		In-Use/Deployed	Pittsburgh	/40	5/9/07	incadmin		
<input type="checkbox"/>	4ffe:daf0:40:1:: (Pitt-v6)		/64		In-Use/Deployed	Pittsburgh	/40	5/17/07	incadmin		

[Delete Selected](#)
[Move Selected](#)

Figure 3-25 In Use/Deployed Blocks





When you select a block hyperlink, the Subnet List screen appears, as shown in Figure 3-26.




Subnet List

List Dynamic Leases Planned vs Actual

Subnet Pitt-Production-1 in Container Pittsburgh

[Add IP Address](#)
[Add IP Range](#)
[Add IP Address Pool](#)




Export:    

   Move Objects

Page: 1 of 39 1-10 of 390 Show: 10

☒ Show Used IPs Only

IP Address	Host Name	Domain Name	HW Address	Type	Device Type	Description	User Defined Fields	Pending Action
172.16.32.1								
172.16.32.2	router-172-16-32-2	sw.diamondip.com.		Static	Router			
172.16.32.3	router-172-16-32-3	sw.diamondip.com.		Static	Router			
172.16.32.4	router-172-16-32-4	sw.diamondip.com.		Static	Router			
172.16.32.5	prtr-01067	sw.diamondip.com.		Automatic DHCP	Printer		Asset Link View IP Asset	
172.16.32.6	prtr-01068	sw.diamondip.com.		Automatic DHCP	Printer		Asset Link View IP Asset	
172.16.32.7	prtr-01069	sw.diamondip.com.		Automatic DHCP	Printer		Asset Link View IP Asset	
172.16.32.8	prtr-01070	sw.diamondip.com.		Automatic DHCP	Printer		Asset Link View IP Asset	
172.16.32.9	prtr-01071	sw.diamondip.com.		Automatic DHCP	Printer		Asset Link View IP Asset	
172.16.32.10	fileserv-584	sw.diamondip.com.		Static	File Server		Contact Name	

   Move Objects

Page: 1 of 39 1-10 of 390 Show: 100

Figure 3-26 Ipv4 Subnet List

Using this display, you can add a single IP Address, an IP Address Range, or an IP Address Pool.

Note: In IPv4 blocks, you can select the **Show User IPs Only** check box to view only in-use IP addresses. In IPv6 blocks, however, only in-use blocks are displayed, no matter whether the **Show User IPs Only** check box is checked or not.

Adding an Individual IP Address

Select the **Add IP Address** option to manage a single IP Address record within the system. The Add IP Address screen opens, as shown in Figure 3-27.

Add IP Address

IP Address: 172.16.19.13 Subnet: [172.16.19.0/24](#)

Address Type: Static Container: [Philadelphia](#)

Device Type: -- Please Select -- Multi-Homed Host: ☐

General Resource Records Ports

Hostname:

Domain: geek.diamondip.com (Default)

Description:

OS:

HW Type: -- Please Select --

HW Address:

Exclude from Discovery: ☐

Figure 3-27 Add IP Address

Enter the details of the IP address you want to add, as described in Table 3-11.

Table 3-11 Add IP Address Screen Elements

Field	Description
IP Address	Enter the IP Address that you are adding. The address displayed is the next available address in the subnet.
Address Type	Specify the address type to be created from the drop-down list: <ul style="list-style-type: none"> • Static – Statically addressed device. • Dynamic DHCP – DHCP IP Address with a lease. • Automatic DHCP – DHCP IP Address unlimited lease. • Manual DHCP – DHCP Address assigned to a specific HW Address, unlimited lease. • Reserved – Reserved for future use.
Device Type	Specify the device type being assigned to this IP Address from the drop-down list. Device types are created in the Device Types function in the IP/DEVICES section of the Tools menu, as described in “Device Types” on page 300.
Subnet	<i>Read only.</i> Displays the subnet that you are currently working within. Click the link if you want to return to the Subnet List.
Container	<i>Read only.</i> Displays the container that you are currently working within. Click the link if you want to return to Address Block Details.

Field	Description
Multi-Homed Host	<i>Only enabled for Static Address Type devices.</i> When checked, indicates that this is a multi-homed host (has multiple interfaces). A Multi-Homed Host tab is added to the display, where you can enter information about each interface.
General Tab	
Hostname	The hostname of this device. If you are using Naming Policies, the system generates a unique name based on the policy that you have defined. You may use this generated name, or you may overwrite the system-generated name.
Domain	Select a DNS Domain Name to associate to this device. This list box is initially populated with domains configured in the Subnet Policy, but any domain in the system can be chosen by clicking Search .
Description	Enter a description of this device.
OS	
DNS Records	The Create Default DNS Resource Records check box defaults to being checked when a Device Type is selected and indicates that the system will automatically create DNS A and PTR records for this object. Uncheck if you want to create any DNS records manually for the device.
HW Type	Ethernet or Token Ring. If a HW Type is chosen, then a HW Address is mandatory.
HW Address	<i>Mandatory if HW Type is chosen.</i> Enter the MAC Address of this device in hexadecimal format.
Exclude from Discovery	Select this checkbox if you want this address space to be ignored during the discovery process.
DHCP Policy Set	<i>Only applicable for Dynamic Address Types.</i> Select the DHCP Policy set to assign to this device. You can choose -Same As Subnet- to use the policy set that you have defined at the subnet level.
DHCP Option Set	<i>Only applicable for DHCP address types.</i> Select the DHCP Option set to assign to this device. You may choose - Same As Subnet - to use the option set that you have defined at the subnet level. To create a set specifically for this device, select "IP Address Specific Option Set". Use the View/Edit link to edit the set.
Effective DHCP Options	<i>Edit Only.</i> When editing an existing DHCP address, you can click Show Currently Saved DHCP Options to view the currently saved DHCP options that are in effect for this address. The effective options for the address are determined by combining DHCP options from the option set assigned to the current Primary DHCP Server for the address (or subnet, if Same as Subnet) with options from the current DHCP Option Set assigned to the subnet that contains this address, as well as with the options from the current DHCP Option Set assigned to this address.
Primary DHCP Server	<i>Only applicable for Dynamic Address Types.</i> Select the Primary DHCP server that will serve this address space.
Failover DHCP Server	<i>Only applicable for Dynamic Address Types.</i> Select the Failover DHCP server that will serve this address space.

Field	Description
User-defined Fields	If any Information Templates are associated with the chosen device type via the rules established on Container Add/Edit (page 97), then User Defined Fields appear. For more information, refer to “User-Defined Fields” on page 314.
Resource Records Tab	
Add Resource Record	Select this link to add DNS resource records to this device.
Interfaces Tab	
Add Interface	<p>Select this link to add additional interfaces to this device. Enter the following information:</p> <ul style="list-style-type: none"> • Interface Name – Enter a name for this interface • Interface Type – Select the type of interface • Hardware Address – Enter the Mac/HW Address of this interface • IP Address – Enter the IP Address of this Interface <p>Note: If the IP Address entered exists in overlapping space, a prompt for a container opens.</p>

Selecting **Resource Record** displays the following:

Add IP Address

IP Address: 172.16.19.13 Subnet: 172.16.19.0/24

Address Type: Static Container: Philadelphia

Device Type: -- Please Select -- Multi-Homed Host: ☐

General Resource Records Ports

[Add Resource Record](#)

Select	Owner	Class	Type	TTL	Data	Domain/Zone	Domain Type	Comments	Pending Action	Details
Delete Selected										

Figure 3-28 Add IP Address Resource Records Tab

Important Note: For flexibility, IPControl optionally allows for the creation of the same domain name (both forward or reverse) multiple times within the system. It is required that each of these domains be placed in a separate “DNS Domain Type” namespace. An example of this is when you have overlapping private address space, being managed by two different DNS servers. It is required that if you are using the same domain name more than once, then you must specify the “default domains” on the subnet’s “policies” screen (see “Add Child Block” on page 31). This permits the system to place the automatically generated DNS Resource Records in the correct domains for this subnet.

Selecting the **Add Resource Record** link displays the following:

Add Resource Record

Resource Record Type: A (IPv4 Address Record/Name-to-address)

Domain/Zone Owner: [Dropdown] Search

Owner	TTL	Class	Type	IPv4 Address
[Text Box]	[Text Box]	IN	A	192.168.128.2

Comment: [Text Area]

Example: localhost IN A 127.0.0.1

Current Record: IN A 192.168.128.2

Description: Address record (code 1) - The A resource record is used to provide a hostname to IP Address mapping. It is one of the most important resource record types, since it provides the IP address of the host being looked-up. Typically, each host should have an A record unless it is an alias for another host (using the CNAME resource record). It is possible for a host to have multiple A resource records. This is common on routers and other devices with multiple network interfaces and IP addresses. Defined in RFC 1035.

Create Source: [Text Box]

Update Source: [Text Box]

Submit Cancel

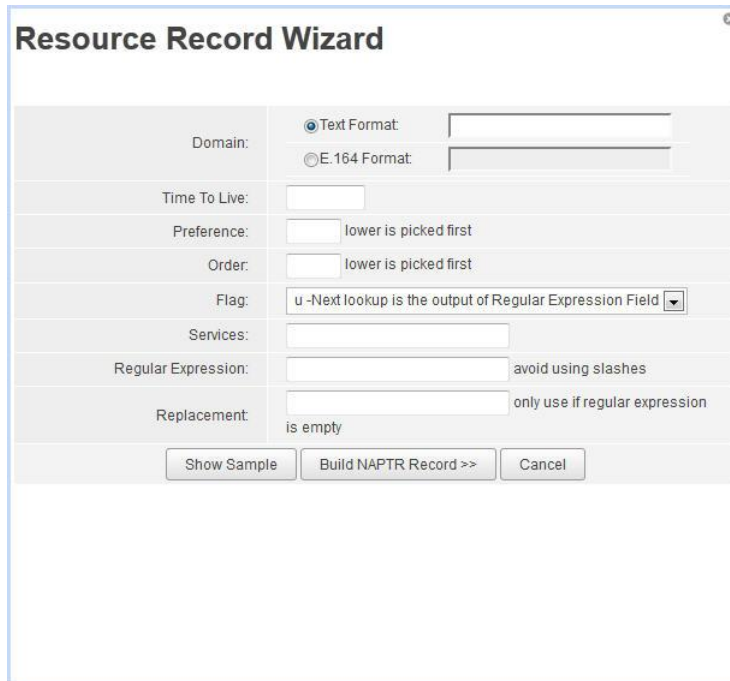
Figure 3-29 Add Resource Record

You may select from the drop-down list of **Resource Record Types** which includes all the standard DNS resource record types that are typically used. If you select **OTHER RESOURCE RECORD** as the Resource Record type, a free format text area is presented that allows you to enter any type of resource record, including experimental options.

If you select **NAPTR**, the **NAPTR Wizard** button appears. Click this button to open the Resource Record wizard screen shown in Figure 3-30, where you can map NAPTR DNS resource records to telephone numbers for use with ENUM.

Resource Record Wizard

The Resource Record Wizard enables you to build a NAPTR record according to the format described in [RFC 3403](#).



The Resource Record Wizard dialog box contains the following fields and controls:

- Domain:** A text input field.
- Format:** Two radio buttons: ☒ Text Format and ☐ E. 164 Format. Each has an associated text input field.
- Time To Live:** A text input field.
- Preference:** A text input field with the text "lower is picked first" to its right.
- Order:** A text input field with the text "lower is picked first" to its right.
- Flag:** A dropdown menu showing "u -Next lookup is the output of Regular Expression Field".
- Services:** A text input field.
- Regular Expression:** A text input field with the text "avoid using slashes" to its right.
- Replacement:** A text input field with the text "only use if regular expression is empty" to its right.
- Buttons:** "Show Sample", "Build NAPTR Record >>", and "Cancel".

Figure 3-30 Resource Record Wizard

Choose from the following actions:

- Select **Show Sample** to review the type of data that is required.
- Select **Build NAPTR Record >>** to populate the resource record with the data you have entered.

Workflow (Record Approval Layer)

A new system policy has been added in IPControl 5.0 that allows you to select one of the following Workflow Types (described in “Workflow Type” on page 265).

- Device
- Resource Record
- None

Workflow functionality adds an approval layer to specific record adds/edits/deletes within IPControl.

If you are upgrading, your current workflow settings carry forward as the default workflow system after the upgrade. If you are performing a fresh installation, a super user can configure a Device Workflow, a Resource Record Workflow, or a workflow of None.

Note: If a super user needs to change the Workflow Type setting, no Pending Records can exist before the configuration change is made.

Device Workflow Type

The Device Workflow Type restricts administrators to either approval or non-approval access to device records that are managed within containers and/or blocks as follows:

- Approving administrators can add, edit, and delete devices without the device ever reaching a pending approval status.
- Non-Approving admins can add and delete devices but not without the device record being marked as Pending Approval.
- Any administrator can edit approved device records, but any device record that is in a pending status cannot be edited.

Administrator Policies

Login ID: incadmin
Description:

Authorized Functions | Access Control List | Block Type Access | Device Type Access | Policies | Domain Access Control
Net Service Access Control | Resource Record Type Access Control | Address Type Access

Container Name:	Read	Write	Delete	Apply to Children	Device Approve Access	
Americas	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete Add Block
Asia	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete Add Block
Europe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete Add Block

Add Container(s)

Block Name:	Container Name	Read	Write	Delete	Device Approve Access	
172.24.4.0/22	Europe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete

Submit Cancel

Figure 3-31 Effect of Device Workflow Type on Administrator Policies Access Control List

In order for a Pending Device Record to be usable within the product, it must be approved by an administrator with Approving capabilities. An Approving administrator can either open the Edit IP Address screen and perform the approval/rejection there, or select **Pending Approvals** from the IPAM section of the **Management** menu and perform individual or bulk approvals/rejections to device records.

Device Workflow rules are as follows:

- Add IP address by a device non-approving administrator, generates a Pending Create device record.
- Add IP Address Range by a device non-approving administrator, generates Pending Create device records.

- Via Domain 'A' resource record creation, selecting to auto generate a device record, performed by a:
 - ▶ Device non-approving administrator generates a Pending Create device record.
 - ▶ Device approving administrator generates an Approved device record.
- Add IP by an device approving administrator, generates an Approved device record.
- Add IP Address Range by a device approving administrator, generates Approved device records.
- Edit IP on a Pending Create device record by any administrator is not possible, because the record is locked for edits.
- Edit IP on an Approved Record by any administrator, the record remains in an Approved status.
- Delete IP/device record by a device non-approving administrator, generates a Pending Delete record.
- Delete IP/device record by a device approving administrator, deletes the IP/device record from the system and the IP become available for use again.
- Reclaim IP record by a device non-approving administrator, generates a Pending Delete record.
- Reclaim IP record by a device approving administrator, generates a deleted record.
- If a device non-approving administrator is performing a discovery on a subnet, and is performing the update from the **Planned vs. Actual** tab, net additions are marked as Pending Create.
- If device approving administrator is performing a discovery on a subnet, and is performing the update from the **Planned vs. Actual** tab, net additions are marked as Approved.
- Approving a Pending Create device record generates an approved device record.
- Rejecting a Pending Create device record removes the device criteria and the IP is available for use again.
- Approving a Pending Delete device record removes the approved device record and the IP is again available for use.
- Rejecting a Pending Delete device record removes the Pending Delete status and the device IP remains approved.

Device approval permissions are ignored when:

- Adding/deleting an interface to the block
- Splitting blocks
- Joining blocks
- Moving blocks
- Deleting blocks

- Creating Address Pools (although certain conditions apply on existing device records when generating Pools – see section Rules on Address Pools)

Resource Record Workflow Type

A Resource Record Workflow Type restricts administrators to either approval or non-approval access to resource records that are managed within domains. Approving administrators can add, edit, and delete resource records without the resource record ever reaching a pending approval status. Non-Approving administrators can add, edit, and delete resource records but not without the resource record being marked as Pending Approval.

The screenshot shows the 'Administrator Policies' configuration page. At the top, there's a header with 'Login ID: incadmin' and a 'Description:' field. Below this is a navigation bar with tabs: 'Authorized Functions', 'Access Control List', 'Block Type Access', 'Device Type Access', 'Policies', 'Domain Access Control', 'Net Service Access Control', 'Resource Record Type Access Control', and 'Address Type Access'. The 'Policies' tab is selected. The main content area shows a table for 'Domain: example.com'. The table has columns for 'Read', 'Write', 'Delete', 'Resource Record Access', 'Resource Record Write Access', 'Resource Record Approve Access', and 'Apply to Children'. The 'Resource Record Approve Access' column is highlighted with a red box. Below the table, there are 'Submit', 'Add Domain(s)', and 'Cancel' buttons.

Figure 3-32 Effect of Resource Record Workflow Type on Administrator Policies Domain Access Control

In order for a Pending Resource Record to be usable, it must be approved by an administrator with Approving capabilities. The approving administrator can either open the domain Resource Record or device Resource Record screen and perform the Approval/Rejection by performing any form of record edit/save, or select **Pending Approvals** from the IPAM section of the **Management** menu and perform individual or bulk Approvals/Rejections to Resource Records.

Resource Record Workflow rules are as follows:

- Add resource record by a resource record non-approving administrator, generates a Pending Create resource record.
- Add resource record by a resource record approving administrator, generates an Approved resource record.
- Edit resource record by a resource record non-approving administrator, generates a Pending Update resource record.
- Edit resource record by a resource record approving administrator, generates an Approved resource record.
- Delete resource record by a resource record non-approving administrator, generates a Pending Delete resource record.

- Delete resource record by a resource record approving administrator, deletes the resource record from the domain/device with which it is associated.
- Approving a Pending Create resource record generates an approved resource record.
- Rejecting a Pending Create resource record removes the record from the domain/device it is attached to and no longer exists in the system.
- Approving a Pending Edit resource record generates an approved resource record.
- Rejecting a Pending Edit resource record generates an approved resource record which includes the edits applied before the pending updates.
- Approving a Pending Delete resource record removes the approved resource record from the domain/device it is attached to and no longer exists in the system.
- Rejecting a Pending Delete resource record removes the Pending Delete status from the resource record and it remains approved.

None Workflow Type

A None Workflow Type disables the administrator approval process and prevents pending type records from being used in IPControl.

Multi-Homed Host

Selecting **Multi-Homed Host** displays the **Interfaces** tab, as displayed in Figure 3-33.

Add IP Address

IP Address:	172.16.19.13	Subnet:	172.16.19.0/24
Address Type:	Static	Container:	Philadelphia
Device Type:	-- Please Select --	Multi-Homed Host:	<input checked="" type="checkbox"/>

General Interfaces Resource Records Ports

[Add Interface](#)

Select	Interface	Interface Type	Hardware Address	IP Address	Exclude from Discovery
<input type="checkbox"/>	Default			172.16.19.13	false

Delete Selected

Figure 3-33 Add IP Address Interfaces Tab

To add additional interfaces to a device, select **Add Interface**.

Add Interface

Interface Name:

Interface Type:

--- Please Select ---

Hardware Address:

IP Address:

Exclude from Discovery:

☐

Ports/Switch:

Port

Switch

Submit

Cancel

Figure 3-34 Add Interface

Enter the information described in Table 3-12.

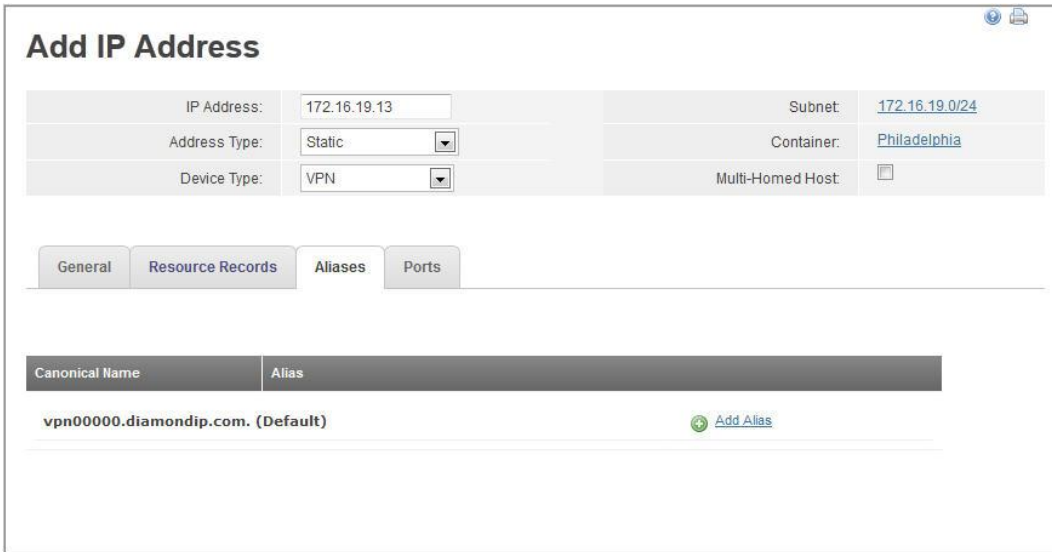
Table 3-12 Add Interface Screen Elements

Field	Description
Interface Name	Enter a name for this interface.
Interface Type	Select the type of interface.
Hardware Address	Enter the MAC/Hardware address of this interface.
IP Address	Enter the IP Address of this interface.
Exclude from Discovery	Select this checkbox if you want this address space to be ignored during the discovery process.

Click **Submit** to save your changes. The interface appears as a link on the **Interfaces** tab. You can select the link to edit the interface or select the check box and click **Delete Selected** to remove it altogether.

Aliases Tab

When you select a Domain on the **General** tab, the **Aliases** tab appears.



Add IP Address

IP Address:	172.16.19.13	Subnet:	172.16.19.0/24
Address Type:	Static	Container:	Philadelphia
Device Type:	VPN	Multi-Homed Host:	<input type="checkbox"/>

General Resource Records Aliases Ports

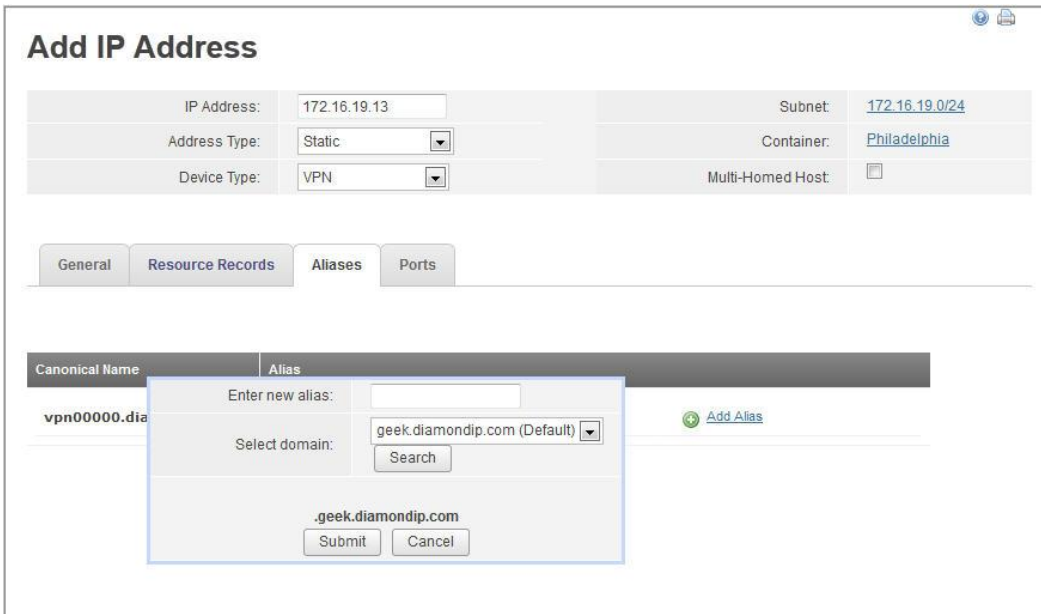
Canonical Name	Alias
vpn00000.diamondip.com. (Default)	

[Add Alias](#)

Figure 3-35 Aliases Tab

Adding an Alias

To add an alias, click the **Add Alias** link.



Add IP Address

IP Address:	172.16.19.13	Subnet:	172.16.19.0/24
Address Type:	Static	Container:	Philadelphia
Device Type:	VPN	Multi-Homed Host:	<input type="checkbox"/>

General Resource Records Aliases Ports

Canonical Name	Alias
vpn00000.dia	

[Add Alias](#)

Enter new alias:

Select domain:

geek.diamondip.com (Default)

Search

.geek.diamondip.com

Submit Cancel

Figure 3-36 Add Alias

Follow these steps:

1. Enter an alias in the **Enter new alias** field.
2. Select a domain from the **Select domain** drop-down list. Click **Search** to open the DNS Domains Search window where you can enter criteria to select the server you want.

3. Click **Submit** to save your changes. The alias appears as a link on the **Aliases** tab. You can select the link to edit the alias or click **Delete** to remove it altogether.

Editing an IP Address

You can edit an individual IP Address by clicking on a link in the Subnet List (see Figure 3-26 on page 52). You can change the properties on the main page and/or various tabs and click **Submit** to save the changes. All the changes from various tabs are collected together and saved together when you click **Submit**.

Changing the IP Address, Domain or Hostname on the **General** tab is not allowed if there are resource records associated with the IP Address that are pending approval. When you try to submit such a change, a message is displayed indicating that the pending changes need to be approved or rejected before proceeding with further changes.

Editing Resource Records

Resource records can be edited by clicking on the link inside the **Owner** field.

If an approver edits a resource record that is pending approval, their change is saved. The disposition of the pending change depends on the state and pending action on the resource record as detailed in “**Error! Reference source not found.**” on page **Error! Bookmark not defined.**

If a non-approver edits a resource record that is pending approval, their change is saved but the record remains in the pending state.

Adding a Range of IP Addresses

Use the **Add IP Range** option to add a range of IP Address that share common attributes within the system. This option creates multiple individual IP Addresses (as opposed to a pool of addresses), which allows you to maintain the details of each device if needed.

Selecting **Add IP Range** displays the screen shown in Figure 3-37:

Subnet: 172.18.6.0/24

Add IP Range

Start Address: ☐ Auto Calculate

End Address: Size:

Description:

Address Type:

Device Type:

Host Name Template:

Example Host Name:

Domain:

Create ARecords for All: ☒

Create PTR Records for All: ☒

Figure 3-37 Add IP Range

Table 3-13 Add IP Range Screen Elements

Field	Description
Start Address	Enter the starting IP Address within the range that you are adding. Note: You can only add a range of IP Addresses within a subnet. You cannot create a range that spans subnets.
Auto Calculate	<i>Optional.</i> You can select this checkbox, and enter the number (Size) of the range that you want to create. The system will then automatically calculate the End Address.
Size	<i>Only applicable when Auto Calculate is checked.</i> Enter the number of IP Addresses to create. For example, if the “Start Address” was 10.0.0.1, and the “Size” is 3, then the following IP Addresses will be created: 10.0.0.1, 10.0.0.2, 10.0.0.3
End Address	Enter the ending IP Address within the range that you are adding.
Address Type	Specify the address type to be created: <ul style="list-style-type: none"> • Static – Statically addressed device. • Dynamic DHCP – DHCP IP Address with a lease. • Automatic DHCP – DHCP IP Address unlimited lease. • Reserved – Reserved for future use.
Device Type	Specify the Device Type being assigned to these IP Addresses. Device Types are created in the Tools menu.

Field	Description
Host Name Template	<p>Optional. Generate a hostname using an <i>on-the-fly</i> naming policy instead of one you have previously defined in Naming Policies (page 301). When typing text, specify which generator to use by enclosing the generator in % characters, for example, %incr.nopad%.</p> <p>Constants are defined for generator names. To produce device names for an IP range of 3, for example:</p> <ul style="list-style-type: none"> • lp-printer%incr.nopad% generates hostnames: lp-printer0 lp-printer1 lp-printer2 • lp-%incr.nopad%-printer generates hostnames lp-0-printer lp-1-printer lp-2-printer <p>Use one of the following generator types:</p> <ul style="list-style-type: none"> • Unpadded incrementor: incr.nopad Example: lp-printer%incr.nopad% generates lp-printer1 • Zero filled incrementor: incr.pad Example: lp-printer%incr.pad% generates lp-printer00001 • IPV4 – dash separated: ipv4addr.dash Example: lp-printer%ipv4addr.dash% generates lp-printer10-0-0-1 • IPV4 – zero filled: ipv4addr.pad Example: lp-printer%ipv4addr.pad% generates lp-printer01000000001 • Container name: container.name Example: lp-printer-%container.name% generates lp-printerIp-Test1
DHCP Policy Set	Only applicable for Dynamic Address Types. Select the DHCP Policy set to assign to these devices. You may choose ---Same As Subnet--- to use the policy set that you have defined at the subnet level.
DHCP Option Set	Only applicable for Dynamic Address Types. Select the DHCP Option set to assign to these devices. You may choose ---Same As Subnet--- to use the option set that you have defined at the subnet level.
Primary DHCP Server	Only applicable for Dynamic Address Types. Select the Primary DHCP server that will serve this address space.
Failover DHCP Server	Only applicable for Dynamic Address Types. Select the Failover DHCP server that will serve this address space.
Example Host Name:	Read Only: Displays the sample hostname that will be generated for each IP Address based on a specified naming policy. If you are using Naming Policies rather than the Host Name Template , the system generates a unique name based on the policy that you have defined for each IP Address. For more information, refer to “Naming Policies” on page 301.
Domain	Select a DNS Domain Name to associate to these devices. Use Search to search for any domain defined within the system.

Field	Description
Create A Records for All	Checked indicates that the system will automatically create “A” DNS records for each object. See note below. Unchecked indicates that you must manually create any “A” DNS records that you may want for these objects.
Create PTR Records for All	Checked indicates that the system will automatically create “PTR” DNS records for each object. See note below. Unchecked indicates that you must manually create any “PTR” DNS records that you may want for these objects.

Important Note: For flexibility, IPControl optionally allows for the creation of the same domain name (both forward and reverse) multiple times within the system. It is required that each of these domains be placed in a separate “DNS Domain Type” namespace. An example of this is when you have overlapping private address space, being managed by two different DNS servers. It is required that if you are using the same domain name more than once, then you must specify the “default domains” on the subnet’s Policies screen (refer to “Add Child Block” on page 34). This permits the system to place the automatically generated DNS Resource Records in the correct domains for this subnet.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Adding an IP Address Pool

Use the **Add IP Address Pool** option to add an IP Address Pool to the system. An Address Pool encompasses a range of IP addresses, but unlike individual IP addresses, you manage the attributes of a Pool as a whole.

For example, if you create an IP Address Pool from 10.0.0.1-10.0.0.10, you cannot change the attributes of the individual IP Addresses. When you change the attribute of an IP Address Pool, the change affects all IP addresses within that pool. IP Address Pools are very helpful when you are creating large DHCP address pools, or creating large blocks of “static” or “reserved” space, that you do not need to individually manage.

Selecting **Add IP Address Pool** displays the following screen:

The screenshot shows a web interface for adding an IP address pool. At the top, it says "Subnet: 10.30.5.0/24". Below that is a section titled "Add IP Address Pool" with a dark grey header bar. The main area contains several input fields: "Start Address:" with a text box, "End Address:" with a text box, "Name" with a text box, "Share Name" with a text box, and "Address Type" with a dropdown menu showing "-- Please Select --". To the right of the "Start Address" field is an "Auto Calculate" checkbox and a "Size:" field with a greyed-out text box. At the bottom right are "Submit" and "Cancel" buttons.

Figure 3-38 Add IP Address Pool

Selecting **Dynamic DHCP** or **Automatic DHCP** for the **Address Type** reveals additional DHCP-specific fields:

Subnet: 10.30.5.0/24

Add IP Address Pool

Start Address: Auto Calculate ☐ Size:

End Address:

Name:

Share Name:

Address Type: **Dynamic DHCP**

DHCP Policy Set: **--- Same as Subnet ---**

DHCP Option Set: **--- Same as Subnet ---**

Primary DHCP Server: **--- Same as Subnet ---**

Failover DHCP Server: **None**

Allow Client Classes: Add Client Class

Deny Client Classes: Add Client Class

Figure 3-39 Add Dynamic Addresses to IP Address Pool

Table 3-14 Add IP Address Pool Screen Elements

Field	Description
Start Address	Enter the starting IP Address of the pool that you are adding. Note: You can only add a pool of IP Addresses within a subnet. You cannot create a pool that spans subnets.
Auto Calculate	<i>Optional.</i> You can select this checkbox, and enter the number (Size) of the range that you want to create. The system will then automatically calculate the End Address.
Size	<i>Only applicable when Auto Calculate is checked.</i> Enter the number of IP Addresses to create. For example, if the “Start Address” was 10.0.0.1, and the “Size” is 3, then the following IP Addresses will be included in the pool (10.0.0.1, 10.0.0.2, 10.0.0.3)
End Address	Enter the ending IP Address of the pool that you are adding.
Name	Enter a unique name for this Address Pool. Note that IPControl provides a default name of the Start and End Address.
Share name	<i>Optional.</i> If this IP Pool is on a shared subnet (shared network), enter the shared network name. The Share name should be a unique name that is specific to the physical network. All pools that share the same physical network should be declared with the same Share name.

Field	Description
Address Type	Specify the address type to be created: <ul style="list-style-type: none"> • Static – Statically addressed device. • Dynamic DHCP – DHCP IP Address with a lease • Automatic DHCP – DHCP IP Address unlimited lease • Reserved – Reserved for future use.
DHCP Policy Set	<i>Only applicable for Dynamic Address Types.</i> Select the DHCP Policy set to assign to these devices. You may choose “—Same As Subnet—” to use the policy set that you have defined at the subnet level.
DHCP Option Set	<i>Only applicable for DHCP address types.</i> Select the DHCP Option set to assign to these devices. You may choose “—Same As Subnet—” to use the option set that you have defined at the subnet level. To create a set specifically for this address pool, select “Address Pool Specific Option Set”. Use the View/Edit link to edit the set.
Effective DHCP Options	<i>Edit Only.</i> When editing an existing address pool, a button will be available which will show a popup page displaying the currently saved DHCP options which are effective for this address pool. The effective options for the address pool are determined by combining DHCP options from the option set assigned to the current Primary DHCP Server for the address pool (or subnet, if Same as Subnet) with options from the current DHCP Option Set assigned to the subnet which contains this address pool, and with the options from the current DHCP Option Set assigned to this address pool.
Primary DHCP Server	<i>Only applicable for Dynamic Address Types.</i> Select the Primary DHCP server that will serve this address space.
Failover DHCP Server	<i>Only applicable for Dynamic Address Types.</i> Select the Failover DHCP server that will serve this address space.
Allow Client Classes	<i>Only applicable for Dynamic Address Types.</i> Select the client classes that are ALLOWED to receive an IP Address from this pool. Note: The selected Client Class must also be assigned to the DHCP server within the DHCP server definition.
Deny Client Classes	<i>Only applicable for Dynamic Address Types.</i> Select the client classes that are DENIED from receiving an IP Address from this pool. Note: The selected Client Class must also be assigned to the DHCP server within the DHCP server definition.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Show Dynamic Leases

Use the **Dynamic Leases** tab to view DHCP lease information that has been collected from the DHCP server. Collecting active lease information is accomplished through the **Discovery** option in the IPAM section of the **Management** menu. For more information, refer to “Discovery/Collectors” on page 82.

Subnet List

List Dynamic Leases Planned vs Actual

Subnet 172.24.0.0/24 in Container UK

Search

Export

Page: 1 of 1 1-3 of 3 Show: 100

IP Address	Host Name	Domain Name	HW Address	Address Type	Device Type	Device Status	Lease Start	Lease End	Client Hostname	Last Update
172.24.0.4	ptr-01189	example.com		Automatic DHCP	Printer	Available				
172.24.0.5	ptr-01190	example.com		Automatic DHCP	Printer	Available				
172.24.0.6	ptr-01191	example.com		Automatic DHCP	Printer	Available				

Page: 1 of 1 1-3 of 3 Show: 100

Figure 3-40 Show Dynamic Leases

Table 3-15 Show Dynamic Leases Screen Elements

Field	Description
IP Address	The IP Address of this lease record.
Host Name	The hostname of this device as defined within IPControl.
Domain Name	The Domain name of this device as defined within IPControl.
HW Address	The MAC Address of this device in hex format.
Address Type	The address type of this lease: <ul style="list-style-type: none"> Dynamic DHCP – DHCP IP Address with a lease. Automatic DHCP – DHCP IP Address unlimited lease. Manual DHCP – DHCP IP address that has been directly assigned to this client via MAC address.
Device Type	The Device Type being assigned to this IP Address. Device Types are created in the “System” menu.
Device Status	The current Device Status.
Lease Start	The lease start time for this IP Address.
Lease End	The lease end time for this IP Address.
Client Hostname	The hostname of the device as it was collected directly from the active lease file.
Last Update	The last date/time that this lease record was updated.

Planned vs Actual

Use the **Planned vs Actual** tab to view planned *vs.* actual of what has been defined within IPControl *vs.* what has been discovered on the subnet using the integrated discovery agent. You must first run a discovery task against this subnet to populate this screen. You can then selectively choose which updates you want to apply.

You can use this option to effectively find and record devices that appear on the network without knowledge or assignment of the IPControl administrator.

Subnet List

List Dynamic Leases Planned vs Actual

Subnet 192.168.193.0/25 in Container exton-core

Actual from network Differences highlighted

Export

Page: 1 of 3 1-10 of 21 Show: 10

	IP Address	Address Type	Device Type	In DB?	Answered Ping?	Fully Qualified Domain Name	Hardware Address	Host O/S
<input type="checkbox"/>	192.168.193.1	Static	Unknown	✓	✓	exton-core gw-193.sw.ins.com		
<input type="checkbox"/>	192.168.193.2	Static	Unspecified	✓	✓	extms3750 extms3750.diamondipam.int.		
<input type="checkbox"/>	192.168.193.4	Static	Unspecified	✓	✓	ext12821internal ext12821internal.diamondipam.int.		
<input type="checkbox"/>	192.168.193.8	Static	Unspecified	✓	✓	extmsfwoffice extmsfwoffice.diamondipam.int.		
<input type="checkbox"/>	192.168.193.10	Static	Unspecified	✓	✓	extmskmm1 extmskmm1.diamondipam.int.		
<input type="checkbox"/>	192.168.193.11	Static	Unspecified	✓	✓	extms3560g extms3560g.diamondipam.int.		

Planned vs. Actual

Click to save any changes you have made, or to refresh the display.

Subnet/Block View

The Subnet/Block View option allows you to view and manage IP Address space by CIDR block. This feature allows you quickly see how a specific CIDR block has been allocated throughout your network.

Understanding the Screen Layout

When you select **Subnet/Block View** from the IPAM section of the **Management** menu, a view of your address blocks is visible in the left frame of your browser. You can select individual blocks and drill down into child blocks that are derived from the CIDR block. On the right side of the screen, you see details about the block that is currently selected in the tree view in the left frame.

Guide to Using IPControl

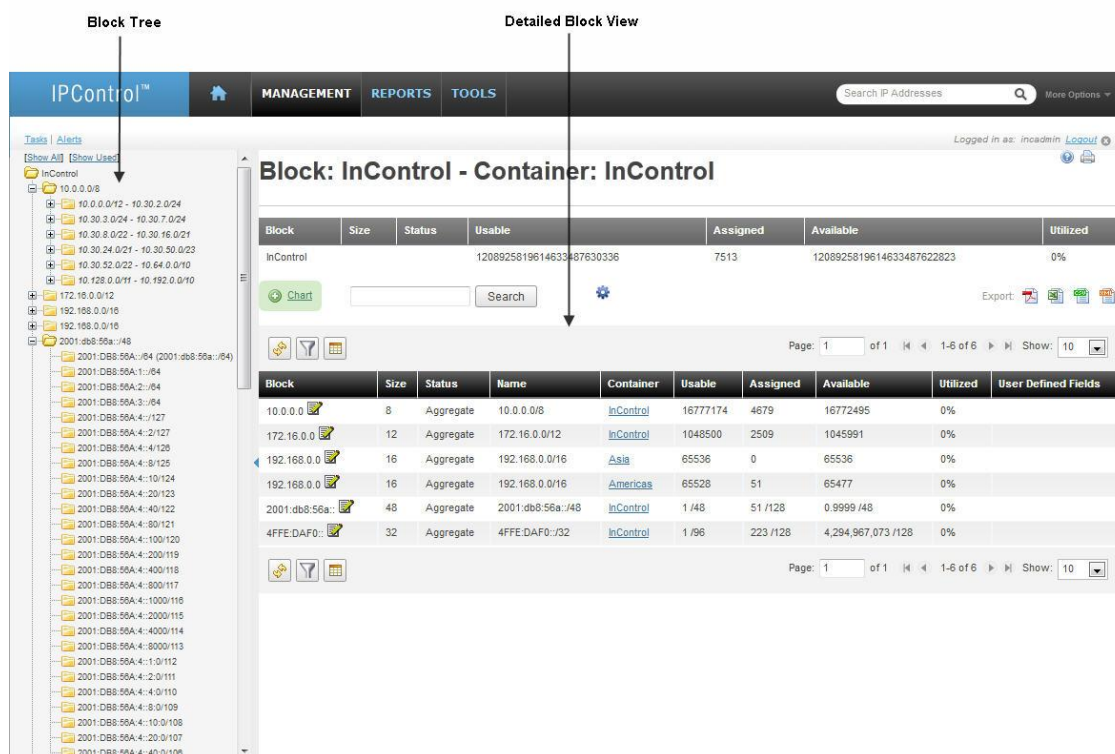


Figure 3-41 Address Block Details

In the **Block Tree** frame, two selections are available:

- **Show All** – refreshes the tree display, and shows all blocks including free space.
- **Show Used** – (*default view*) refreshes the tree display, and only shows blocks that are used (all blocks that are not free).

In the **Detailed Block View** frame, the details about the specific block that is selected in the block tree are displayed.



The top of the display shows the details about the current block, such as size, name and status.

Block: 10.0.0.0/8 - Container: InControl						
Block	Size	Status	Usable	Assigned	Available	Utilized
10.0.0.0	/8	Aggregate	16777192	4580	16772612	0%
<div> <input type="text"/> <input type="button" value="Search"/> </div> <div> Export: </div>						











Figure 3-42 Detailed Block View

Table 3-16 Block View Screen Elements

Field	Description
Block	The starting address of the CIDR block.
	Edit the properties of this block.
Size	The size in CIDR notation of the block.

Field	Description
Status	<p>The current status of this block:</p> <ul style="list-style-type: none"> • Free – The block is available for use or allocation. • Aggregate – This block is an aggregate block. • In-Use/Deployed – The block is in use as a subnet. • In-Use/Fully Assigned – The block is in use and all IP Addresses are fully utilized. • Reserved – This block is reserved for future use.
Usable	The number of usable IP Addresses in this block.
Assigned	The number of hosts that have been assigned (are in use) in this block.
Available	The number of hosts in this block that are available to be assigned.
Utilized	The percent of the block that is used.
User Defined Fields	The User Defined Fields affiliated with this block
 and 	Displayed when IPV6 address pools are listed. Used to change the display format of IPV6 hosts. See “Displaying IPV6 Capacities” on page 14 for more information.

The bottom of the display shows the details about any child blocks that have been derived from this block.

Block	Size	Status	Name	Container	Usable	Assigned	Available	Utilized	User Defined Fields
10.0.0.0 	12	Free	10.0.0.0/12	InControl	1048576	0	1048576	0%	
10.128.0.0 	11	Free	10.128.0.0/11	InControl	2097152	0	2097152	0%	
10.16.0.0 	13	Free	10.16.0.0/13	InControl	524288	0	524288	0%	
10.160.0.0 	13	Free	10.160.0.0/13	InControl	524288	0	524288	0%	
10.168.0.0 	13	Aggregate	10.168.0.0/13	Americas	524288	4490	519790	1%	
10.176.0.0 	12	Free	10.176.0.0/12	InControl	1048576	0	1048576	0%	
10.192.0.0 	10	Free	10.192.0.0/10	InControl	4194304	0	4194304	0%	
10.24.0.0 	14	Free	10.24.0.0/14	InControl	262144	0	262144	0%	
10.28.0.0 	15	Free	10.28.0.0/15	InControl	131072	0	131072	0%	
10.30.1.0 	24	In-Use/Deployed	10.30.1.0/24	extonhub	254	4	250	2%	








Page: 1 of 4 1-10 of 40 Show: 10


Figure 3-43 Children Block Details

Table 3-17 Children Block Details Screen Elements

Field	Description
Block	The starting address of the CIDR block.
	Edit the properties of this block.
Size	The size in CIDR notation of the block.

Field	Description
Status	<p>The current status of this block:</p> <ul style="list-style-type: none"> • Free – The block is available for use or allocation. • Aggregate – This block is an aggregate block. • In-Use/Deployed – The block is in use as a subnet. • In-Use/Fully Assigned – The block is in use and all IP Addresses are fully utilized. • Reserved – This block is reserved for future use.
Name	The name that has been assigned to this block. By default, IPControl sets the name to the address/size.
Container	The name of the container that holds this block.
Usable	The number of usable IP Addresses in this block.
Assigned	The number of hosts that have been are in use in this block.
Available	The number of hosts in this block that are available to be assigned.
Utilized	The percent of the block that is used.
User Defined Fields	The User Defined Fields affiliated with the block.

Editing Blocks

Note the edit icon () next to the block address. Click on the edit icon to see the Edit Block page.

The Edit Block screen varies, depending on whether you are viewing a Root Block or a Child Block.

Root Block

Edit Block: 10.0.0.0/12

Container(s): InControl

InControl

General Vlans

Block Name: 10.0.0.0/12

Block Description:

Current Status: Free

SWIP/Net Name:

Reason for Allocation:

Organization ID: None

Block Type: VOIP

Address Space: 10.0.0.0

Block Size: /12

Number of addresses: 1048576

Start Address: 10.0.0.1

End Address: 10.15.255.254

Parent Block: 10.0.0.0/8

Exclude from Discovery: ☐

Discovery Agent: ☐ Inherit from Parent Block ☒ Inherit from Parent Container ☐ Select Agent

Root Block: No

Allow Overlapping Address Space: No

Created on: 2007-05-03 17:11:47.0

Last Modified on: 2007-05-03 17:11:47.0

Last Modified by: incadmin (InControl Administrator)

Save Delete Block Cancel

Figure 3-44 Edit Root Block

Use this form to edit the root block, and to perform other operations on it.

Table 3-18 Edit Root Block Screen Elements

Field	Description
Block Name	The Name of the block. This defaults to the Address/Size. If you edit this, the address and size do <i>not</i> change, just the name.
Block Description	A description field for your use.
Current Status	Root blocks can only be type Aggregate.
SWIP/Net Name	For Internet Registry reporting.
Reason for Allocation	Populated if an Allocation Reason was specified when the block was created.

Field	Description
Internet Registry	Choose the Internet Registry this address was allocated from, or leave as Generic Root Block for private space.
Block Type	The current Block Type.
Address Space	The block starting address.
Block Size	The CIDR Size.
Number of Addresses	The total addresses in the block.
Start Address	The first usable address in the block.
End Address	The last usable address in the block.
Parent Block	The parent block from which this block was created.
Exclude from Discovery	Select this checkbox if you want this address space to be ignored during the discovery process.
Discovery Agent	There are three options for selecting the Discovery Agent: <ul style="list-style-type: none"> • Inherit from Parent Block – Inherits the Discovery Agent from the Parent Block • Inherit from Parent Container - Inherits the Discovery Agent from the Parent Container • Select Agent – Allows user to select Discovery Agent from the system list of Agents.
Root Block	Indicates whether this is a Root Block or not.
Allow Overlapping Address Space	If checked, this block can co-exist with another that overlaps its address range, as long as the overlapping block is not in the same container, or any of its parent containers.
Created On	The block creation date.
Last Modified On	The date/time of last modification.
Last Modified By	The administrator who last changed the block.

At the bottom of the form, a row of buttons allows you to perform several operations on blocks. Some of these buttons might be suppressed if the operation is not applicable. For more information, see the following sections of this chapter.

Child Block

Edit Block: 172.18.1.0/24

Container(s): USVA

InControl / Americas / Caribbean / USVA

General Policies Vlans

Block Name:	172.18.1.0/24									
Block Description:										
Current Status:	In-Use/Deployed ▼									
SWIP/Net Name:										
Reason for Allocation:										
Organization ID:	None ▼									
Block Type:	Data ▼									
Address Space:	172.18.1.0									
Block Size:	/24									
Number of addresses:	256									
Start Address:	172.18.1.1									
End Address:	172.18.1.254									
Parent Block:	Americas									
Exclude from Discovery:	<input type="checkbox"/>									
Discovery Agent:	<input type="radio"/> Inherit from Parent Block <input checked="" type="radio"/> Inherit from Parent Container <input type="radio"/> Select Agent Executive Agent ▼									
Root Block:	No									
Allow Overlapping Address Space:	No									
Contact Name:										
Contact Phone:										
Contact Email:										
Created on:	2011-10-21 07:34:43.0									
Last Modified on:	2011-10-21 07:34:43.0									
Last Modified by:	incadmin (InControl Administrator)									

Address Allocation:

Allocation Template: -- Please Select -- ▼

Starting Offset	Starting Offset From	Ending Offset	Ending Offset From	Address Type	Create Individual IP Objects	Create Resource Records	Default Gateway	Device Type	Network Service	Shared Network Name
<div>Save Delete Block Split Block Join Block Move Block Cancel</div>										

Figure 3-45 Child Block

Table 3-19 Child Block Screen Elements

Field	Description
General	General information about the block.
Block Name	The Name of the block. This defaults to the Address/Size. If you edit this, the address and size do <i>not</i> change, just the name. The block name will then appear in the block list.

Field	Description
Block Description	A description field for your use.
Current Status	Choose one of Aggregate, Reserved, Free, In-Use/Deployed, In-Use/Fully Assigned. Note that your choices might be constrained according to how the block was allocated. In some cases you will not be able to change the Status once assigned (that is, you cannot later change an In-Use block to Aggregate).
Interface IP Address	This appears for Device Containers. It displays the Containers, Interfaces, and IP Addresses in use for this block.
SWIP/Net Name	For Internet Registry reporting.
Reason for Allocation	Populated if an Allocation Reason was specified when the block was created.
Block Type	The current Block Type
Address Space	The block starting address
Block Size	The CIDR Size
Number of Addresses	The total addresses in the block
Start Address	The first usable address in the block
End Address	The last usable address in the block
Parent Block	The parent block from which this block was created.
Exclude from Discovery	Select this checkbox if you want this address space to be ignored during the discovery process.
Discovery Agent	There are three options for selecting the Discovery Agent: <ul style="list-style-type: none"> • Inherit from Parent Block – Inherits the Discovery Agent from the Parent Block • Inherit from Parent Container - Inherits the Discovery Agent from the Parent Container • Select Agent – Allows user to select Discovery Agent from the system list of Agents.
Root Block	Indicates that this is not a root block.
Allow Overlapping Address Space	Indicates whether overlapping address space is allowed.
Created On	The block creation date
Last Modified On	The date/time of last modification
Last Modified By	The administrator who last changed the block
Allocation Template	The name of a template to be applied to a Deployed block, or to be applied when modifying the block status to Deployed. See “Address Pool Allocation Template” on page 281 for instructions on creating these templates.
Policies	Policy settings used when defining individual IP addresses in this block and when generating DHCP configuration files. For more information on the fields in this tab, refer to Table 3-5 on page 37.
Vlans	Provides read-only VLAN details when a Switch Discovery runs and updates the database successfully.

At the bottom of the form, there is a row of buttons that allow you to perform several operations on blocks. Some of these buttons might be suppressed if the operation is not applicable. For more information, see the following section of this chapter.

Delete Block

Click this button to delete the block from the system. You are prompted for a confirmation. When you delete a block, IPControl automatically reclaims free space, and merges adjacent free space into larger blocks.

Split Block

Click this button to split the current block into smaller pieces. You see the screen below:

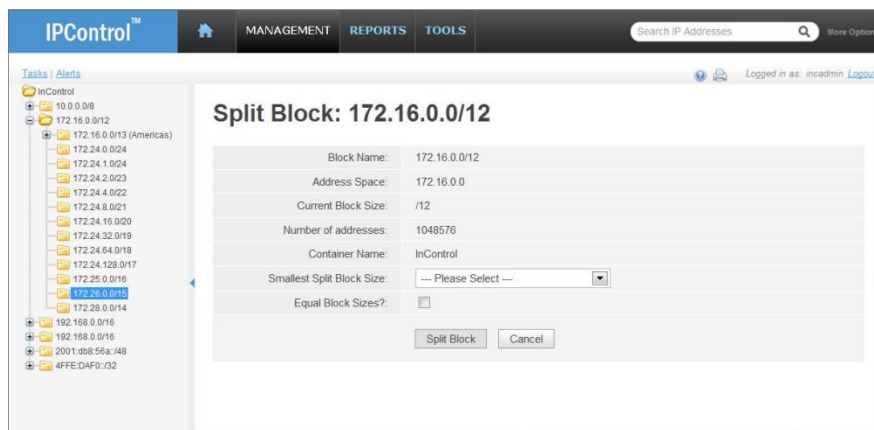


Figure 3-46 Split Block

Select the size of the smallest block you need. IPControl keeps the remaining blocks as large as possible while ensuring the smallest block size is available.

Join Block

This operation merges the current block with an adjacent block of the same size. To be successful, the combined block must satisfy the following criteria:

- Must be of identical size
- Must be contiguous
- Must reside in the same container
- Must have the same block type

Move Block

This operation moves the current block to a new container.

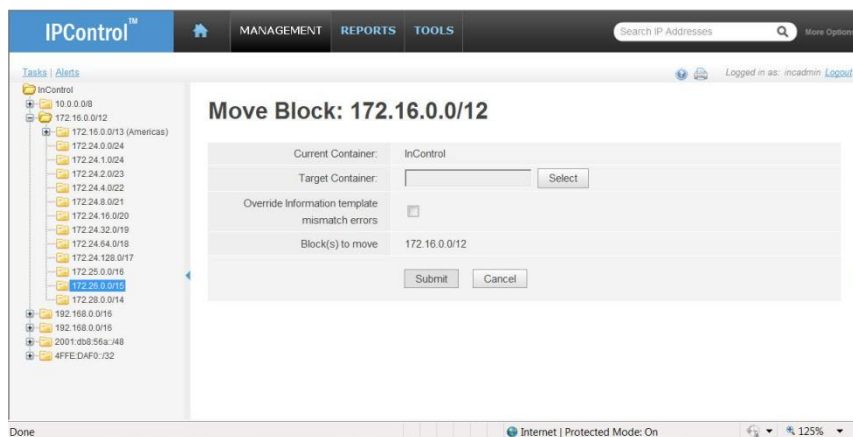


Figure 3-47 Move Block

Select the target container. If you select a Device container, another field appears for the target Interface. Click **Submit** to move the block. Note that the Block must be allowed in the target container, according to its Block Type rules. In addition, you cannot move blocks between Logical and Device containers.

Block type edit

A block's block type may be changed under certain conditions. A block type must first be accessible to the current user for it to be available as the new block type. Rules governing Block Type access can be found in "Block Type Access" on page 332. Below are the conditions when a block's block type can be edited and to what block types it can be changed.

Business rules governing *when* a block's block type may be modified:

- A block's block type may be modified when it contains no children *or* only children of block status 'Free'.

Business rules governing *what* block types are available to a block being modified:

- Only block types allowed by rules governed by Admin ACLs are available.
- The block type of a root block can be modified to any block type in the system.
- The block type of a non root block can be modified to its parent's block's block type or this block type's children.

Block type edit example

Assume the following block types are defined in the system, the current user has no Admin ACL restrictions, and the block's block type may be modified.


- A root block could be changed to any block type in the system.
- A child block whose parent's block's block type is 'Any' could be changed to:
 - ▶ Any
 - ▶ Any_East

- ▶ Any_West
- ▶ Private
- A child block whose parent's block's block type is 'Any_East' could be changed to:
 - ▶ Any_East
 - ▶ 3rdGen

Pending Approvals

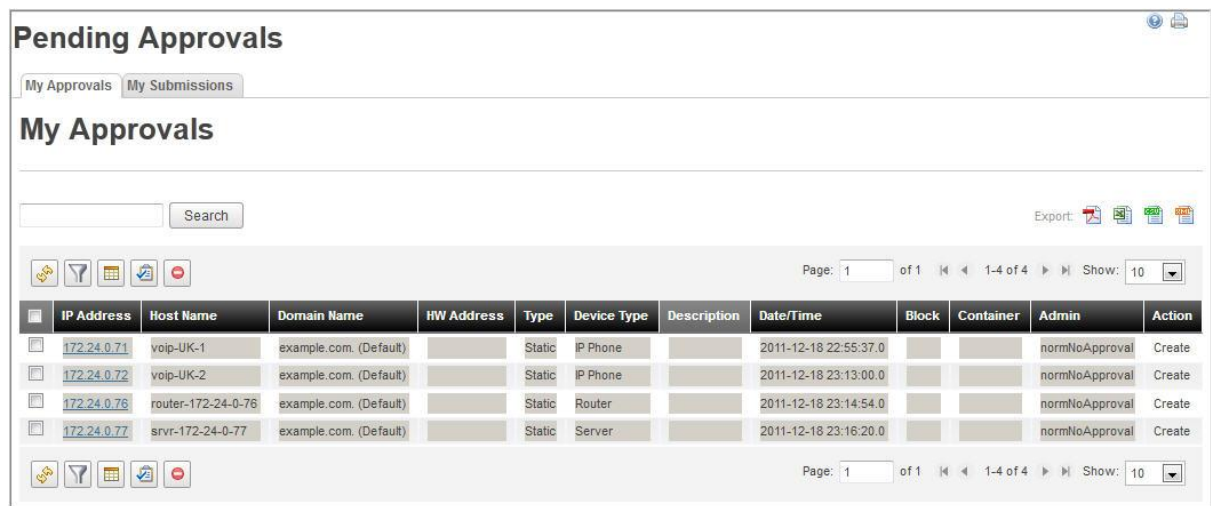
The Pending Approvals screen allows you to view two sets of data related to device workflow:

- Devices that require your approval
- Devices you have submitted for approval

You can filter the display results by the Create and Delete actions. If there are Internationalized Domain Names, a  dropdown icon appears on the far right of the display, where you can select how you want the Domain Name column to be displayed.

To access the Pending Approvals screen, select **Pending Approvals** from the IPAM section of the **Management** menu. A list of device changes submitted for your approval appears in the **My Approvals** tab, as shown in Figure 3-48.

My Approvals





IP Address	Host Name	Domain Name	HW Address	Type	Device Type	Description	Date/Time	Block	Container	Admin	Action
172.24.0.71	voip-UK-1	example.com. (Default)		Static	IP Phone		2011-12-18 22:55:37.0			normNoApproval	Create
172.24.0.72	voip-UK-2	example.com. (Default)		Static	IP Phone		2011-12-18 23:13:00.0			normNoApproval	Create
172.24.0.76	router-172-24-0-76	example.com. (Default)		Static	Router		2011-12-18 23:14:54.0			normNoApproval	Create
172.24.0.77	srvr-172-24-0-77	example.com. (Default)		Static	Server		2011-12-18 23:16:20.0			normNoApproval	Create

Figure 3-48 My Approvals Tab

Refer to Table 3-20 for a description of the columns in the My Approvals tab.

Table 3-20 My Approvals Columns

Field	Description
IP Address	The IP address assigned to the device.

Field	Description
Host Name	The host name of the device.
Domain Name	The domain on which the device is located.
HW Address	The MAC address of the device.
Type	The IP address type.
Device Type	The device type assigned to the device. Device Types are maintained in the IP/DEVICES section of the Tools menu.
Description	The description (if any) that was entered for the device.
Date/Time	Date and time of the action that was performed on the device.
Block	The block where the device is located.
Container	The container where the device is located.
Action	The action that is awaiting approval (that is, Create, Delete or Update)
Approvers	<i>My Submissions tab only.</i> Click  to display the Login ID of the administrator who can approve the action taken on the device. Click  to remove the name from the display.
Admin	<i>My Approvals tab only.</i> Displays the Login ID of the administrator that last modified the device.

You can take the following actions on changes that require your approval:



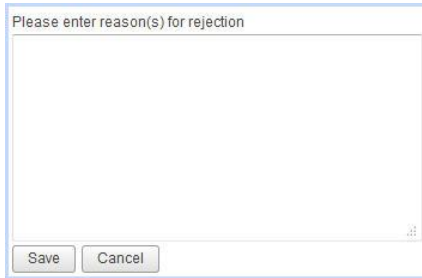
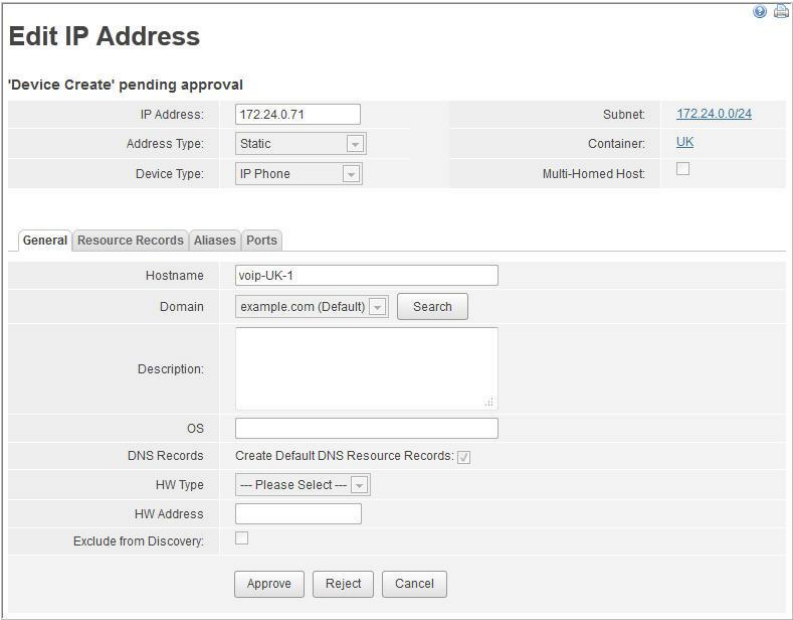

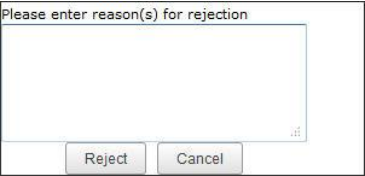
To ...	Then ...
Approve a submission	<ol style="list-style-type: none"> 1. Select the actions that you want to approve. 2. Click . The Approval Reason dialog opens, as shown in Figure 3-49. <div data-bbox="480 1205 902 1482" data-label="Image"> </div> 3. Enter up to 256 alphanumeric characters to indicate why you approve the action taken on the selected devices. 4. Click Save.

Figure 3-49 Approval Reason

To ...	Then ...
Reject a submission	<ol style="list-style-type: none">1. Select the actions that you want to approve.2. Click . The Rejection Reason dialog opens, as shown in Figure 3-49.<div data-bbox="557 443 976 718">The Rejection Reason dialog box is a small window with a title bar. Inside, there is a text area with the prompt "Please enter reason(s) for rejection". At the bottom of the dialog, there are two buttons: "Save" and "Cancel".</div> <p>Figure 3-50 Rejection Reason</p> <ol style="list-style-type: none">3. Enter up to 256 alphanumeric characters to indicate why you reject the action taken on the selected devices.4. Click Save.

To ...	Then ...
Review more details of a specific entry	<div>1. Select the IP address link of the device. The Edit IP Address screen opens, as shown in Figure 3-51.</div> <div></div> <div>Figure 3-51 Review Pending Approval IP Address Details</div> <div>2. Choose from the following actions:</div> <div><div>a. To approve, click Approve. The Approval Reason dialog opens.</div><div></div><div>Enter up to 256 alphanumeric characters to indicate why you approve of the action taken on the device and click Approve.</div><div>b. To reject, click Reject. The Rejection Reason dialog opens.</div><div></div><div>Enter up to 256 alphanumeric characters to indicate why you reject the action taken on the selected devices and click Reject.</div></div>

My Submissions

To review the resource record changes that you have submitted for approval from another administrator, select the **My Submissions** tab, shown in Figure 3-52.

IP Address	Host Name	Domain Name	HW Address	Type	Device Type	Description	Date/Time	Block	Container	Action	Approvers
172.24.0.71	voip-UK-1	example.com. (Default)		Static	IP Phone		2011-12-18 22:55:37.0			Create	
172.24.0.72	voip-UK-2	example.com. (Default)		Static	IP Phone		2011-12-18 23:13:00.0			Create	
172.24.0.76	router-172-24-0-76	example.com. (Default)		Static	Router		2011-12-18 23:14:54.0			Create	
172.24.0.77	srvr-172-24-0-77	example.com. (Default)		Static	Server		2011-12-18 23:16:20.0			Create	

Figure 3-52 My Submissions Tab

Refer to Table 3-20 on page 81 for more information on the display.

Discovery/Collectors

The Discovery/Collectors option allows you to create on-demand, scheduled, or recurring scheduled tasks for collection of utilization, configuration information on network devices (such as routers), and host information on your network. IPControl can capture the following actual configuration information and then compare it with the planned view that is defined in the database:

- Network elements (such as which subnets have been configured on a router)
- Network services (such as what address pools are configured on a DHCP server)
- Hosts on a specific subnet
- IP and MAC addresses (by scanning the ARP table on network elements, such as routers and switches)
- Ports configured on a network switch including port names, speeds, VLAN membership, and devices attached to the ports

Discovery/Collector Task Definition Options

To collect host, configuration, or utilization information from the network, select the “task type”, “network element” or “network service”, and then specify when to run the task. Depending upon the selection of when you will be running the task, different options will be displayed on the screen for you to select. Refer to the sections below for additional information about each option. Note that once you click **Submit**, a new task is created, and

submitted to the system. Once tasks have been created, they can be managed using the **Task** menu option.

Figure 3-53 Discovery/Collector Task Definition

Table 3-21 Discovery/Collector Task Definition Screen Elements

Field	Description
Task Type	<p>Select the type of task that you would like to run.</p> <ul style="list-style-type: none"> • Collect DHCP Utilization collects utilization information from the DHCP server by address pool. Note that Fully Qualified Domain names can be collected for Windows 2003/2008 DHCP servers, but not MS Windows 2000 Servers. • Discover Router Subnets collects the subnets assigned to a router. • Discover Switch Ports collects information about the ports defined on a network switch or all of the switches defined within a branch of the container hierarchy. • Discover Subnet Hosts discovers the hosts that are connected to a single subnet, or all the hosts for all subnets within a Container. • Discover Router ARP Hosts discovers the hosts that connected to a network element such as a router or switch, by scanning the ARP table defined on the element. Or discover all hosts on all subnets on all network elements within a given branch of the Container hierarchy. • Global Utilization Rollup performs the rollup of all utilization data. This includes the following steps: <ul style="list-style-type: none"> ○ Address Pool utilization rolled into associated blocks. ○ Block utilization rolled up into root blocks. ○ All block utilization rolled into container utilization by block type (and interface for device containers) ○ Address pool history snapshot taken ○ Block history snapshot taken ○ Container history snapshot taken ○ Address pool days left regression

Field	Description
	<ul style="list-style-type: none"> ○ Block days left regression ○ Block and Address Pool Threshold checks • Global Synchronization of DHCP Servers collects utilization information from all DHCP servers that participate in the Global Synchronization i.e., have the “Include during Global Synchronization Task” field checked. • Global Synchronization of Network Elements collects subnets assigned to all routers or CMTs that participate in the Global Synchronization, that is, have the Include during Global Synchronization Task field checked.
The following options are based on which type of task is selected	
Network Service	Select Search and select a network service to perform this task against.
Network Element	Select Search and select a network element to perform this task against.
Regression Periods	Enter in the regression number of periods, and select the regression period type.
Create History Records	Check this option to create history records as a part of the task.
Include Alert Threshold Checking	Check this option to include alert threshold checking during the task process.
Subnet Address	Select Search and select a subnet to perform this task against.
Container	Select Search and select a container to perform this task against.
Ping Hosts	Check this option to ping hosts during discovery.
Lookup Hostname	Check this option to perform a DNS lookup during host discovery.
Determine Host Operating System	<i>Not currently supported in IPControl 5.0.</i> Check this option to perform Operating System fingerprinting during discovery. Note that using this option causes the discovery to run slowly, but provide additional OS data regarding each host.
Perform net host additions	Check this option to automatically add new hosts that are found during discovery. Note this will only add new hosts to the system, and will not automatically overwrite existing hosts defined within the system.
Perform net resource record additions	Check this option to automatically add DNS resource records for new hosts that are found during discovery. Note: This option only adds resource records for new hosts to the system, and does not automatically overwrite existing host resource record information defined within the system.
Ignore Duplicate Warnings	If duplicate host name information is found while adding new hosts, you can choose this option to ignore any warnings.
Update Reclaim Statistics	Update the last discovered counters for blocks and hosts defined within a network element for purposes of including this discover in the reclaim criteria. This option is provided because an ARP discover is less accurate than the Subnet Host Discover in determining if a host is up or not.

On-demand (Immediate) Collection Task

To define an immediate task, define the task parameters, and select **Immediate** from the **When to run task** options. Click on **OK** to create the task. A new task is created and submitted to the system. Once tasks have been created, they can be managed using the **Task** menu option.

Scheduled Collection Task

To schedule a future task, define the task parameters, and select **Scheduled** from the **When to run task** selections. Schedule options are displayed as shown in Figure 3-54.

Discovery/Collector Task Definition

Task Type	--- Please Select ---		
When to run task	<input type="radio"/> Immediate <input checked="" type="radio"/> Scheduled <input type="radio"/> Recurring		
Select the date and time that this task is to begin	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="text"/> (hh:mm)
<input type="button" value="Submit"/>			

Figure 3-54 Scheduled Collection Task

To select the future date to run the task, click on the calendar icon and select a date, as described in “Discovery/Collector Task Definition Options” on page 85.

After all parameters have been entered, click **OK**. A new task is created, and submitted to the system. After tasks have been created, you can manage them using the **Task** menu option.

Recurring Collection Task

A recurring task enables you to define tasks to run on a pre-determined schedule. This option allows you to define tasks (such as Utilization Collection) that will occur at regular intervals, providing you with up to date information. To schedule a recurring task, set the task parameters, and select **Recurring** from the **When to run task** selections. Recurring options are displayed as shown in Figure 3-55.

Figure 3-55 Recurring Collection Task

Select the date and time that this recurring task is to begin. This is the first occurrence of the recurring task. Click on the calendar icon and select a date, as described in “Discovery/Collector Task Definition Options” on page 85.

Table 3-22 Discovery/Collector Task Definition Screen Elements

Field	Description
Sub-Daily	Select this option if the task is to occur more than once per day.
Daily	Select this option if the task is to occur once per day at the specified time.
Weekly	Select this option if the task is to run weekly, or on the specified day(s).
Monthly	Select this option to run this task on a specified day of the month.
Yearly	Select this option to run this task on a specified day of the year.

After all the parameters have been selected or entered, click **OK**. A new task is created and submitted to the system. After tasks have been created, you can manage them using the **Task** menu option.

Address Space Reclaim

The Reclaim option allows you to free unused IP addresses and subnets from the IPControl database.

IP Address managers need to monitor the actual usage of IP Addresses. “Actual” means that a particular IP Address is configured on a device interface, and used for network traffic. It is not uncommon for an administrator to allocate addresses to a user and those addresses are never used. Addresses can also become stale and unused over time. This does not refer to Dynamic DHCP addresses, which are managed by the DHCP server. Address reclaim is targeted at static and Manual DHCP addresses only. An Administrator needs to identify allocated addresses that are unused, and reclaim them for use by other users. In some cases, entire subnets are allocated for use only during a limited period of time. In such cases, this feature

supports reclaiming entire subnets (in-use/deployed blocks) when it is discovered that there are zero hosts on that subnet.

IPControl provides two methods for performing reclaim – manual and automatic.

Manual Reclaim

Manual reclaim allows the administrator to selectively reclaim objects that meet the given criteria. This operation involves these basic steps:

1. Run network discovery tasks periodically. Select **Discover** from the IPAM section of the **Management** menu, and then select **Discover Subnet Hosts** from the **Task Type** drop-down list.

Note: The task must *not* include the **Determine Host Operating System** option.

2. Choose from a number of criteria and filters and then run a report that analyzes the results of Step 1 and proposes individual addresses or subnets for reclaim.
3. Choose from suggested output and reclaim addresses or subnets. Freed subnets are returned to the free block pool. Freed addresses are deleted and available for other allocations.

Automatic Reclaim

Automatic reclaim allows the administrator to schedule tasks to perform automatic reclaim of objects that meet the given criteria. This operation involves these basic steps:

1. Run network discovery tasks periodically. Select **Discover** from the IPAM section of the **Management** menu, and then select **Discover Subnet Hosts** from the **Task Type** drop-down list.

Note: The task must *not* include the **Determine Host Operating System** option.

2. Run an Automatic Reclaim task – immediate, scheduled, or recurring – where the parameters for a reclaimable addresses or subnets are supplied and applied in bulk.
3. Review the results of the reclaim task in the Task display.

Ignoring Specific Device Types during Subnet Reclaim

When creating or editing Device Types, you can specify which device types can be ignored for the purposes of Subnet discovery by selecting the **Ignore devices of this type for Subnet Reclaim** check box, shown in Figure 3-56.

Name:		Router
Description:		Router
Ignore devices of this type for Subnet Reclaim:		<input checked="" type="checkbox"/> (Checked=Yes)
		Submit Cancel

Figure 3-56 Ignore devices of this type for Subnet Reclaim

When a Host Discovery is run for a subnet, devices of the specified type are not counted towards the number of devices discovered. For example, if the Router device type had been set up to be ignored and was the only IP address found during discovery, then that subnet could be reclaimed. This does *not* affect the IP Address Reclaim feature, which supports Device Type filtering, as shown in Figure 3-57. Note that the number of ignored hosts is counted and tracked for the subnet.

IP Address Space Reclaim

To reclaim address space, select **Address Space Reclaim** from the IPAM section of the **Management** menu. The Reclaim screen appears, as shown in Figure 3-57, where you can choose between Manual/Automatic reclaim types, and IP Addresses/Subnets reclaim objects.

Reclaim Type		<input checked="" type="radio"/> Manual <input type="radio"/> Automatic
Reclaim Objects		<input checked="" type="radio"/> IP Addresses <input type="radio"/> Subnets/Blocks
IP Addresses Reclaim Criteria		
Scope:	<input checked="" type="radio"/> Block <input type="radio"/> Container	Search
	<input checked="" type="checkbox"/> Include Children	
Days Since Last Contact:		
Minimum Discover Attempts:		
Block Type:	-- ALL Block Types --	
Address Status:	-- ALL Address Statuses --	
Device Type:	-- ALL Device Types --	
Hostname:	<input checked="" type="radio"/> Begins With <input type="radio"/> Contains <input type="radio"/> Ends With	
Submit		

Figure 3-57 Reclaim

Performing Manual IP Address Reclaim

To perform a manual reclaim on IP addresses, ensure that the Manual Reclaim Type and the IP Addresses option buttons are selected.

IP Address reclaim supports the following criteria and filters:

Reclaim Criteria (required)

- **Scope** - The Scope of the IP Address Reclaim may be either a Block or a Container, interpreted as follows:
 - ▶ If the scope is a Block without children, then the reclaim analysis will be performed on the IP addresses in that Block only if it is an In-Use/Deployed Block (that is, a Subnet), otherwise an error will be displayed.
 - ▶ If the scope is a Block with children, then the reclaim analysis will be performed on IP addresses in all child Subnets under the selected aggregate Block.
 - ▶ If the scope is a Container without children, then the reclaim analysis will be performed on IP addresses in all Subnets in the selected Container.
 - ▶ If the scope is a Container with children, then the reclaim analysis will be performed on IP addresses in all Subnets in the selected Container and its sub-containers.
- **Days Since Last Contact** - Defines the window to look for unreachable hosts. That is, the number of days that have elapsed since the last time that an IP address was found to be online.
- **Minimum Discover Attempts** - The minimum number of Discover Subnet Hosts tasks that have been run within the window defined by Days Since Last Contact. That is, the number of times that a Discover Task has been run over the last X number of days, where X is the value of the Days Since Last Contact.

Additional Filters (optional)

- **Block Type** - Default is ALL types. If scope is Block, then list includes the selected Block's type and any sub-types.
- **Address Status** - Default is ALL statuses. Generally useful only for Manual DHCP objects.
- **Device Type** - Default is ALL types.
- **Hostname match** - Default is any hostname but you can enter a string and select from **Begins With**, **Contains**, or **Ends With** options.

After you have entered criteria, click **Submit**. The reclaim analysis is performed and a list is displayed showing all reclaimable addresses, as shown in Figure 3-58.

Reclaim IP Addresses

IP Addresses Reclaim Criteria	
Scope:	block = 10.0.0.0/8
Include Children:	true
Days Since Last Contact:	100
Minimum Discover Attempts:	1
Block Type:	ALL
Address Status:	ALL
Device Type:	ALL
Hostname:	begins

Select	Container	Block	IP Address	Hostname	Domain	Hardware Address	Address Type	Address Status	Device Type	Last Update	Last Reachable	Discover Attempts
<input type="checkbox"/>	China	10.30.5.0/24	10.30.5.8	fileserv-48	diamondip.com		Static	In Use	File Server	2007-04-01 10:01:28.0		28
<input type="checkbox"/>	China	10.30.5.0/24	10.30.5.13	corp-pc-10-30-5-13	diamondip.com		Static	In Use	PC	2007-04-02 09:15:59.0		31

1 - 2 of 2

Page size: 10

Figure 3-58 Reclaimable IP Addresses

You can then select some or all of the addresses and click the **Reclaim Selected** button. By default, the list is ordered by IP Address, but you can choose a different sort order by clicking on the appropriate column header. The columns specific to the reclaim analysis are as follows:

- **Last Update** – this is the date/time stamp of the time this device was created or last updated. If this column is blank, then the device was created before this information was tracked in IPControl.
- **Last Reachable** – this is the date/time stamp of the time this device was last determined to be “up” via a Subnet Host Discovery task.
- **Discover Attempts** – this is the number of Subnet Host Discover tasks that have been attempted for this device since the Last Reachable date.

Performing a Manual Subnet Reclaim

To perform a manual subnet reclaim, select the **Subnet/Blocks** option button in the Reclaim screen. The screen updates to show subnet reclaim settings, as shown in Figure 3-59.

Figure 3-59 Manual Subnet Reclaim

Subnet reclaim supports the following criteria and filters:

Reclaim Criteria (required)

- **Scope** - The Scope of the Subnet Reclaim may be either a Block or a Container.
 - ▶ If the scope is a Block without children, reclaim analysis is performed on that Block only if it is an In-Use/Deployed Block (that is, a Subnet); otherwise an error is displayed.
 - ▶ If the scope is a Block with children, reclaim analysis is performed on all child Subnets under the selected aggregate Block.
 - ▶ If the scope is a Container without children, reclaim analysis is performed on all Subnets in the selected Container.
 - ▶ If the scope is a Container with children, reclaim analysis is performed on all Subnets in the selected Container and its sub-containers.
- **Days Since Last Contact** - Defines the window to look for unused subnets. That is, the number of days that have elapsed since the last time that at least one IP address in the subnet was found to be online.
- **Minimum Discover Attempts** - The minimum number of Discover Subnet Hosts tasks that have been run the since the device was last reachable. That is, the number of times that a Discover Task has been run over the last X number of days, where X is the value of the Days Since Last Contact.

Additional Filters (optional)

- **Block Type** - Default is ALL types. If scope is Block, then list includes selected Block's type and any sub-types.

After you have entered your criteria and clicked **Submit**, reclaim analysis is performed and a list is displayed showing all reclaimable subnets, as shown in Figure 3-60.

Reclaim Subnets/Blocks

Subnet/Blocks Reclaim Criteria	
Scope:	container = Americas
Include Children	true
Days Since Last Contact:	240
Minimum Discover Attempts:	1
Block Type:	ALL

New Criteria

Select	Name	Type	Container	Parent Block	Created By	Last Update	Last Reachable	Hosts Ignored	Discover Attempts
<input type="checkbox"/>	192.168.0.0/24	Data	extonhub	192.168.0.0/16		2007-05-08 14:59:11.0	2007-05-08 08:58:49.0	0	2

Check All

Reclaim Selected

1 - 1 of 1

Page size: 10

Figure 3-60 Reclaimable Subnets

You can then select some or all of the subnets and click the **Reclaim Selected** button. By default, the list is ordered by Subnet name, but you can choose a different sort order by clicking on the appropriate column header. The columns specific to the reclaim analysis are as follows:

- **Last Update** – this is the date/time stamp of the time this block was created or last updated. If this column is blank, then the device was created before this information was tracked in IPControl.
- **Last Reachable** – this is the date/time stamp of the time a device on this subnet was last determined to be “up” via a Subnet Host Discovery task, and that device was not a device type that is to be ignored as described above.
- **Hosts Ignored** – this is the number of devices that were determined to be “up” during the last Subnet Host Discover task, but were ignored because their device type was defined to be ignored as described above.
- **Discover Attempts** – this is the number of Subnet Host Discover tasks that have been attempted for this subnet since the Last Reachable date.

Performing Automatic Reclaim Tasks

Choosing the Automatic reclaim type allows the administrator to create a task that performs reclaim processing automatically on an immediate, scheduled, or recurring basis. Automatic Reclaim is supported for both IP Address and Subnet reclaim. In both cases, the additional task scheduling parameters appear at the bottom of the page.

Immediate Reclaim

To run a reclaim task now, select **Immediate** from the **When to run task** options. Click on **OK** to create the task. A new task is created and submitted to the system. Once tasks have been created, they can be managed using the **Task** menu option.

Scheduled

To schedule a future reclaim task, select **Scheduled** from the **When to run task** selections.

To select the future date to run the task, click on the calendar icon and select a date, as described in “Discovery/Collector Task Definition Options” on page 85.

Once all parameters have been entered, click **Submit**. A new task is created and submitted to the system. After tasks have been created, you can manage them using the **Task** menu option.

Recurring

A recurring reclaim task enables you to define the reclaim task to run on a pre-determined schedule. To schedule a recurring task, select **Recurring** from the **When to run task** selections.

Select the date and time that this recurring task is to begin. This is the first occurrence of the recurring task. Click on the calendar icon and select a date, as described in “Discovery/Collector Task Definition Options” on page 85.

After all the parameters have been selected or entered, click **Submit**. A new task is created and submitted to the system. Once tasks have been created, you can manage them using the **Task** menu option.

Container Maintenance

The Container Maintenance menu option allows you to maintain IPControl containers. Containers are organizational units that IPControl administrators use to create a hierarchy of their company’s network structure. Rules that govern the IP Address allocation policies of your organization are assigned to each container.

Container Maintenance Layout

When you select **Container Maintenance** from the IPAM section of the **Management** menu, your network tree is displayed in the left frame of your browser. IPControl recommends that you click the **Refresh** link above the hierarchy display after adding or deleting containers.

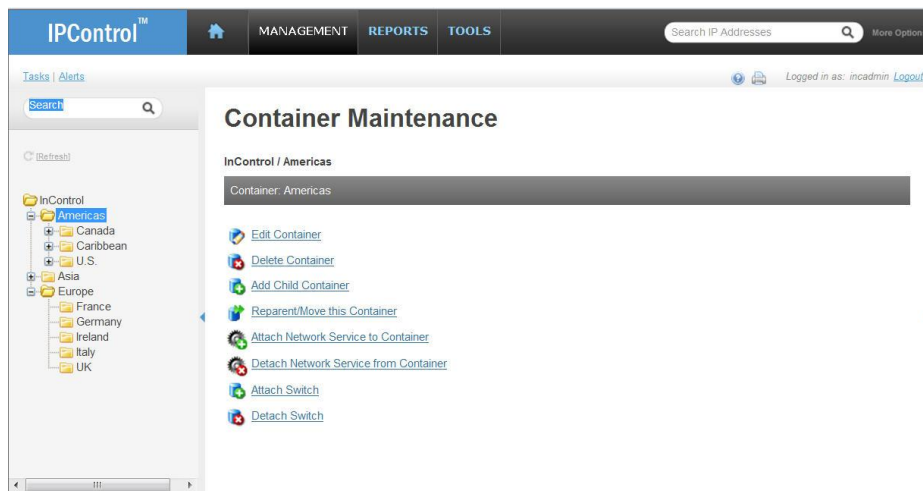


Figure 3-61 Container Tree

The right-hand side of the screen lists the container maintenance options, described in Table 3-23. Refer to the following sections for information on each option.

Table 3-23 Container Maintenance Features

Option	Description
Edit Container	Edit the currently selected container.
Delete Container	Delete the currently selected container.
Add Child Container	Add a container below the currently selected container. The currently selected container becomes a parent of the new container.
Reparent/Move this Container	Move this container underneath a different parent.
Attach Network Service to Container	Attach a DHCP Server to this container. The DHCP Server must have previously been defined in Servers/Services in the DHCP section of the Management menu.
Detach Network Service from Container	Remove a DHCP Server assignment from this container.
Attach Switch	Attaches a switch to this container. A Network Element with an Element Type of “Switch” must be defined first.
Detach Switch	Detaches a switch from this container.

Edit Container

Use the **Edit Container** option to edit the attributes of a container. Note that you cannot change a container type after you have created it. For information on the fields in each tab, refer to Table 3-24 and Table 3-25 on page 100.

Delete Container

Use the **Delete Container** option to delete a container. Note that deletes are not allowed in the following cases:

- Container is the root container (top of the container hierarchy)
- Container has child containers

Note: If child containers are moved or deleted first, the container can then be deleted.

- Container has blocks assigned within it

When you select this option, an Are you sure you want to delete this container? confirmation window displays. Select **OK** to delete the container or **Cancel** to leave the container unchanged.

Add Child Container

Select the **Add Child Container** option to create a child container for the parent container you have selected in the container hierarchy. The Add Child Container screen shown in Figure 3-62 appears.

Add Child Container

Parent Container: Americas

General Information:

Type: Logical Search

Name:

Discovery Agent: ☒ Inherit from Parent Container ☐ Select Agent Executive Agent

Description:

Information Template: Asset Contact Geolocation Press Ctrl-Click to select multiple information templates

Maintain History Records: ☒ (Checked=Yes)

Submit Cancel

Valid Block Types Valid Device Types Allow Root Block Creation Allow Allocation from Parent Require SWIP / Net Name Block Type Information Templates Device Type Information Templates

Policy: Valid Block Types

☒ **Enable or disable all Block Types** - This screen allows you to configure the valid Block Types that can be used with this Management Container. Select the valid Block Types below by selecting the checkbox next to the type.

Block Types	Select
Any	<input checked="" type="checkbox"/>
Data	<input checked="" type="checkbox"/>
IPv6 Lab	<input checked="" type="checkbox"/>
Management	<input checked="" type="checkbox"/>
Video	<input checked="" type="checkbox"/>
VOIP	<input checked="" type="checkbox"/>

Submit

Figure 3-62 Add Child Container

This screen is divided into two sections: General Information and Rules.

General Information Section

The General Information section captures basic information about the new child container.

Table 3-24 General Information Parameters

Option	Description
Type	<p>Select Logical or Device.</p> <p>Logical containers are user-defined organizational views of how your address space is managed (such as regions, divisions, ISP, organizations, etc.).</p> <p>Device containers represent actual Network Devices such as Routers and CMTSS. To add a Device, click the Search button and select a Device from the IPControl Device Search window, where you can search on a specific text or IP address string if necessary. The device you select appears in the Name field and its IP address is shown in the Device Specific Information area.</p>
Name	Provide a name for the new container, which is displayed in the container tree.
Discovery Agent	Select the InControl Agent (defined in Agents in the SYSTEM section of the Tools menu) to be used to perform Network Discovery for blocks within this container.
Description	Provide a description for the new container.
IP Address	<i>Read-only for Device containers.</i> Displays the IP Address of the Network device selected in the IPControl Device Search window.
Information Template	Choosing an Information Template for this container adds the User Defined Fields in that Information Template to this container. The fields from the selected Information Template appear on the right side of the screen.
Maintain History Records	Select this check box if you want to run accurate Container Utilization Reports.

Rules Tabs

The tabs allow policies or rules to be established for this container. The rules established for a container govern the use and allocation of address space for this container.

Table 3-25 Rules

Rule	Description
Valid Block Types	Selecting one or more block types on this policy allows child blocks of these types to be created in this container. All other block types are prohibited.
Valid Device Types	Selecting one or more device types on this policy allows devices of these types to be created in subnets that are defined within this container. All other device types are prohibited.
Allow Root Block Creation	Selecting one or more block types on this policy allows root blocks of these types to be created in this container. All other block types are prohibited.
Allow Allocation from Parent	Selecting one or more block types on this policy allows child containers to search in this container's Parent for blocks of the selected types. For all non-selected block types, the search is not allowed to proceed beyond this container.

Rule	Description
Require SWIP/Net Name	Selecting one or more block types on this policy makes entry of the SWIP/Net Name parameter a required field for these block types, within this container. For all non-selected block types, entry of the SWIP/Net Name parameter is not required.
Block Type Information Template	Choosing an Information Template for a block type adds the User Defined Fields in that Information Template to any block of that type within this container. You can see the fields from the Information Template on the Add Child Block screen.
Device Type Information Template	Choosing an Information Template for a device type adds the User Defined Fields in that Information Template to any device of that type within this container. You can see the fields from the Information Template on the Add IP Address screen.

Reparent/Move this Container

Select the **Reparent/Move this Container** option to move this container (and the blocks associated with it) to another parent. The Reparent/Move Container screen opens.

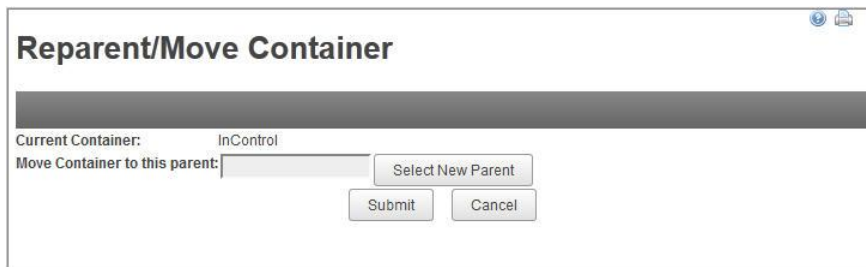


Figure 3-63 Reparent/Move Container

Click the **Select New Parent** button to display the Container Search dialog box.

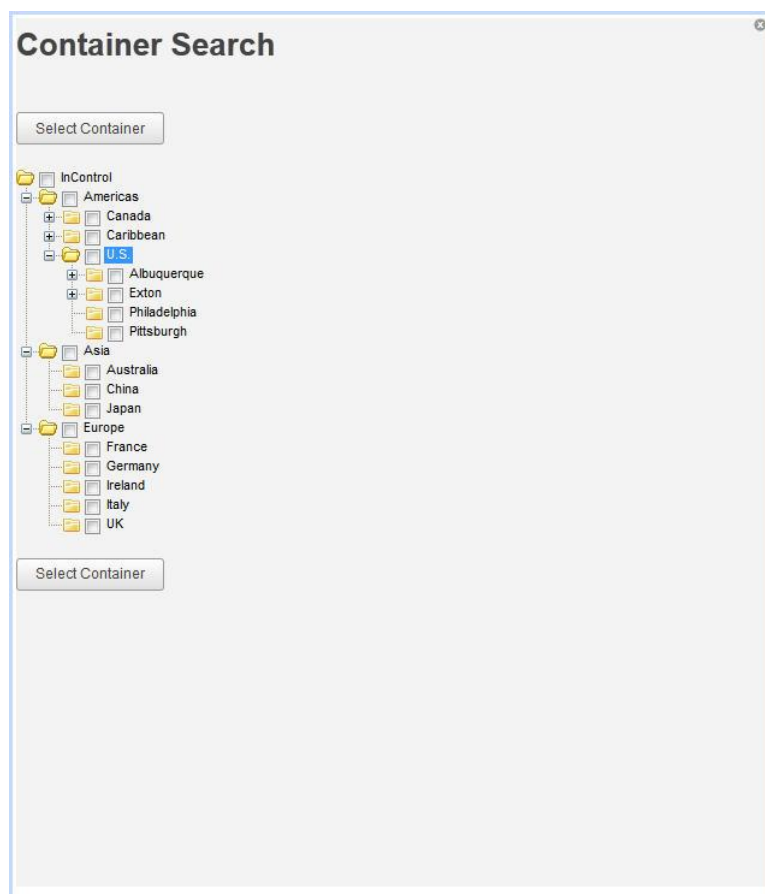


Figure 3-64 Container Search

Navigate the tree, expanding nodes as needed, and then check the new parent container. Note that you can only check a single container. Once you have selected a container, click the **Select Container** button. The name of the new parent is displayed in the **Move Container to this parent** field. Click **Submit** to move the container to this new parent, or click **Cancel** to return to the Container Maintenance screen.

Attach Network Service to Container

Use this option to attach a Network Service to this container. By attaching a network service to this container, you establish default “network services” for this container and its children containers. These defaults display when you are creating address pools using Address allocation pool templates within the Add Child Block display.

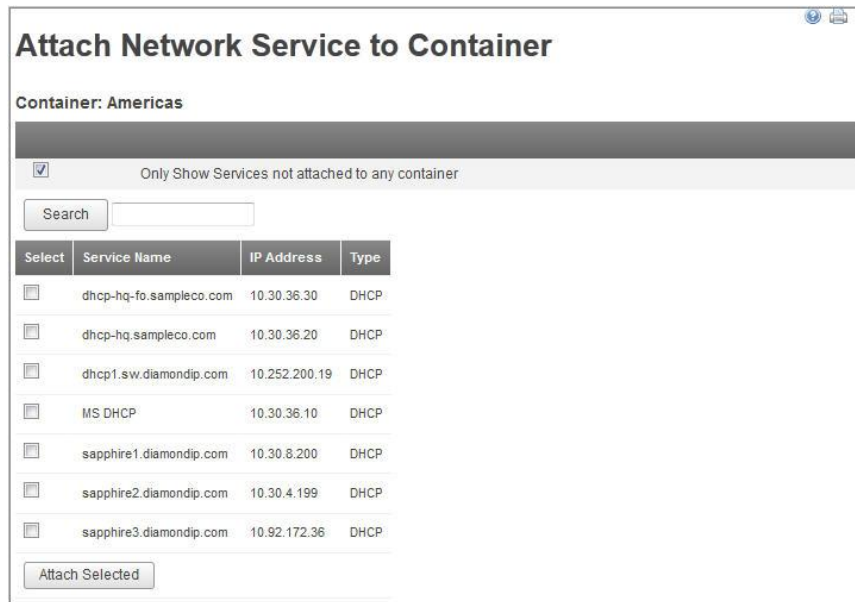


Figure 3-65 Attach Network Service to Container

To attach a network service to the container, check the select box of the network services to attach, and then click on the **Attach Selected** button. You can limit the display of network services by using the search filter, or by clicking on the **Only Show Services not attached to any container** check box.

Detach Network Service from Container

Use the **Detach Network Service from Container** option to remove an attached network service from the container selected in the container hierarchy.

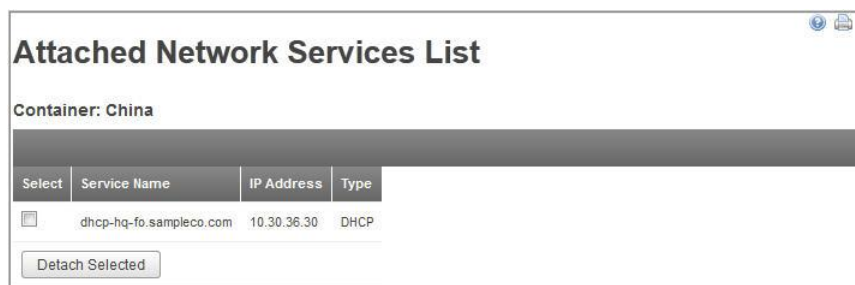


Figure 3-66 Attached Network Services List

To detach one or more network services from the container you have previously selected in the container hierarchy, select the network services to be detached and click **Detach Selected**. A confirmation message appears on the screen.

Attach Switch

Select the **Attach Switch** option to attach a Switch to the container previously selected in the container hierarchy.

Attach Switch to Container: Americas

☐ Only show Switches not attached to any container

Search

Select	Switch Name	IP Address
<input type="checkbox"/>	exton-sw01.diamondip.com	10.30.8.8
<input type="checkbox"/>	wayne-sw01.diamondip.com	10.30.8.9
<input type="checkbox"/>	exton-sw02.diamondip.com	10.30.8.5

Attach Selected Cancel

Figure 3-67 Attach Switch to Container

To search for a particular Switch, enter a search string into the text block and click **Search**. To filter your search criteria to only Switches in the system that are not attached to a Container, click the **Only show Switches not attached to any container** checkbox.

To attach one or more Switches, click the checkbox in the **Select** column for each item you wish to attach, and click **Attach Selected**. Click **Cancel** to cancel and return to the previous screen.

Detach Switch

Use the Detach Switch option to detach a Switch from a container.

Attached Switch List: Australia

Select	Switch Name	IP Address
<input type="checkbox"/>	exton-sw01.diamondip.com	10.30.8.8
<input type="checkbox"/>	exton-sw02.diamondip.com	10.30.8.5

Detach Selected Cancel

Figure 3-68 Attached Switch List

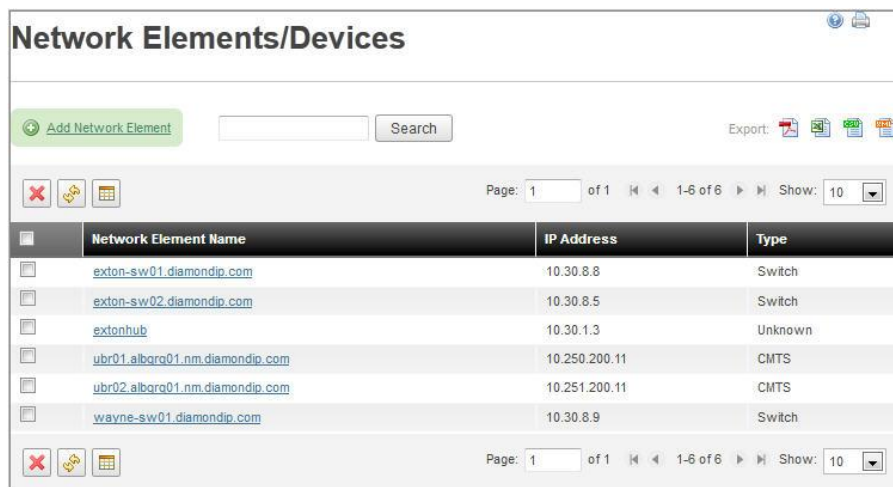
This menu allows you to detach one or more Switches from a Container. All Switches currently attached to the selected Container in the tree view are listed.

To detach one or more Switches, click the checkbox in the Select column for each item you wish to detach, and click **Detach Selected**. You are prompted for confirmation. Click **OK** to detach the selected Switch, or **Cancel** to return to the previous screen.

Network Elements/Devices

The Network Elements/Devices screen allows you to maintain network elements (managed devices) within the IPControl system. A network element represents a physical device on your

network such as a router. IPControl can be used to manage and plan the IP Address space that is allocated to a physical device. This planned allocation can then be compared to the device's actual configured address space by using the collection facility provided by IPControl.




The screenshot shows the 'Network Elements/Devices' interface. At the top, there is a title bar and a toolbar with an 'Add Network Element' button, a search input field, and a 'Search' button. Below the toolbar, there are icons for delete, add, and refresh, and a pagination bar showing 'Page: 1 of 1' and 'Show: 10'. The main content is a table with the following data:

	Network Element Name	IP Address	Type
<input type="checkbox"/>	exton-sw01.diamondip.com	10.30.8.8	Switch
<input type="checkbox"/>	exton-sw02.diamondip.com	10.30.8.5	Switch
<input type="checkbox"/>	extonhub	10.30.1.3	Unknown
<input type="checkbox"/>	ubr01.albora01.nm.diamondip.com	10.250.200.11	CMTS
<input type="checkbox"/>	ubr02.albora01.nm.diamondip.com	10.251.200.11	CMTS
<input type="checkbox"/>	wayne-sw01.diamondip.com	10.30.8.9	Switch

At the bottom of the table, there are icons for delete, add, and refresh, and a pagination bar showing 'Page: 1 of 1' and 'Show: 10'.

Figure 3-69 Network Elements List

To search for a particular Network Element, enter a search string into the text block and click **Search**.

To delete one or more Network Element, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected Network Elements, or **Cancel** to return to the previous screen.

Adding a Network Element

To add a network element, click the **Add Network Element** link. The Add Network Element screen appears.

Add Network Element



Name	<input type="text"/>
Description	<input type="text"/>
IP Address	<input type="text"/>
Element Type	--- Please Select ---
Vendor	--- Please Select ---
Model	--- Please Select ---
SNMP sysName	
SNMP sysDescr	
SNMP sysLocation	
SNMP sysServices	0
Telnet Username	<input type="text" value="incadmin"/>
Telnet Password	<input type="password" value="*****"/>
Enable Password	<input type="password"/>
SNMP Version	<input checked="" type="radio"/> V1 <input type="radio"/> V3
SNMP Read Community String	<input type="text"/>
SNMP Timeout (milliseconds)	<input type="text"/>
SNMP Retries	<input type="text"/>
Collection Agent	 Add Agent
Include during Global Synchronization Task	<input type="checkbox"/>
Device Interface Template	--- Please Select ---
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Figure 3-70 Add Network Element

Table 3-26 Add Network Element Parameters

Field	Description
Name	Enter the name of the device. Typically, this will be the fully qualified domain name.
Description	Enter a description of this device.
IP Address	Enter the IP Address of this device. This is required if you will use IPControl to collect configuration information from this device.
Element Type	Select the type of this device.
Vendor	Select the vendor of this device.
Model	Select the model of this device.
Telnet Username	Enter the Telnet user name used to telnet into this device. This user name will be used to optionally update the device's configuration with changes in the address space.
Telnet Password	Enter the Telnet password used to telnet into this device.
Enable Password	Enter the Enable password.

Field	Description
SNMP Read Community String	Enter the SNMP read community string used to read the device's MIB II information. This is required if you will use IPControl to collect configuration information for planned vs. actual comparisons.
SNMP Timeout (milliseconds)	Enter the number of milliseconds the SNMP Agent will wait without receiving any messages from its partner before it assumes that the connection to its partner has failed.
SNMP Retries	Enter the number of connection retries that the SNMP Agent will attempt..
Collection Agent	Select the Agent that will be used to collect information from this device. This is required if you want to use IPControl to collect configuration information for planned vs. actual comparisons. Click  or select the Add Agent link to open the Agents screen where you can select an agent from the Agent Name list, as described in “Agents” on page 265.
Include during Global Synchronization Task	Select if you want to include this device in the global synchronization task. The device's configuration information is then collected when the task runs.
Device Interface Template	Select a device interface template to assign to this device. The device template is used to model and attach interfaces to this device. If a template is selected, and there are interfaces defined for this device, interfaces are displayed and can be assigned a status of ENABLED, DISABLED, or BEING DEPLOYED, as described in “Adding a Device Template” on page 305.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen. If the network element was successfully added, the Network Element List screen displays `Network Element <element-name> created`, and the new network element appears in the network element list.

Editing a Network Element

To modify an existing network element, click on the network element name in the Network Element List. This takes you to the Edit Network Element Screen.

Edit Network Element

Name	extonhub		
Description	Extong Router		
IP Address	10.30.1.3		
Element Type	Unknown		
Vendor	Unknown		
Model	Unknown		
SNMP sysName	extpasw2		
SNMP sysDescr	Cisco Internetwork Operating System Software IOS (tm) L3 Switch/Router Software (CAT2948G-IN-M), Version 12.0(25)W5(27) RELEASE SOFTWARE Copyright (c) 1986-2003 by cisco Systems, Inc. Compiled Fri 28-Mar-03 13:42 by integ		
SNMP sysLocation			
SNMP sysServices	6		
Telnet Username	incadmin		
Telnet Password	••••••••		
Enable Password			
SNMP Version	<input checked="" type="radio"/> V1 <input type="radio"/> V3		
SNMP Read Community String	ren		
SNMP Timeout (milliseconds)	1000		
SNMP Retries	3		
Collection Agent	Add Agent Executive Agent 127.0.0.1 Delete		
Include during Global Synchronization Task:	<input checked="" type="checkbox"/>		
Edit Interfaces			
Interface: BVI230	Enabled		
Interface: BVI180	Enabled		
Interface: BVI150	Enabled		
Interface: BVI160	Enabled		
Interface: BVI220	Enabled		
Interface: BVI36	Enabled		
Interface: BVI48	Enabled		
Interface: BVI222	Enabled		
Interface: BVI100	Enabled		
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>			

Figure 3-71 Edit Network Element

Edit the network element fields as needed. You can change the attributes of the network element, or add/remove interfaces using the **Edit Interfaces** link. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Server Pairs

The Server Pairs screen allows you to maintain network service to network service communications. It allows you to configure the following:

- Transaction keys that are used to secure communications between ISC BIND-based DNS servers.
- Transaction keys that are used to secure dynamic updates from ISC-based DHCP servers to ISC BIND-based DNS servers.
- GSS Credentials that are used to secure dynamic updates from IPControl to Microsoft DNS servers.
- Override of default behavior of BIND-based DNS server communications, such as turning off incremental zone transfers.

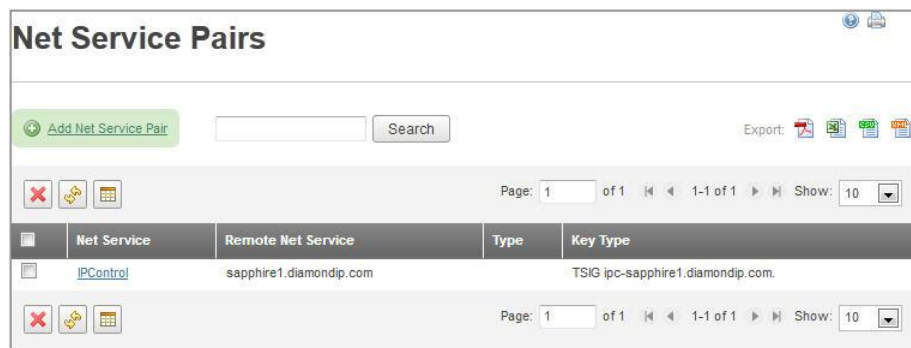


Figure 3-72 Net Service Pairs

To delete one or more server to server definitions, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected pairs, or **Cancel** to return to the previous screen.

Adding a Network Service Pair

To add a Net Service Pair, click the **Add Net Service Pair** link. The Add Net Service Pair screen appears.

The screenshot shows the 'Add Net Service Pair' form. It has a title bar and a toolbar with a 'Cancel' button. The form contains two dropdown menus:

Net Service:

Remote Net Service:

At the bottom, there are 'Submit' and 'Cancel' buttons.

Figure 3-73 Add Net Service Pair

Table 3-27 Net Service Pair Parameters

Field	Description
Net Service	<p>Select the network service for which you want to add server to server communications statements.</p> <ul style="list-style-type: none"> • If IPControl is selected, you are configuring the security credentials for dynamic DNS updates to a remote DNS Server. You must select a DNS server for the Remote Net Service option. If the remote DNS server is BIND based, then you choose a TSIG key. If the DNS server is Microsoft based, you choose GSS TSIG credentials. • If a DHCP server is selected, you are configuring the transaction key to be used for dynamic DNS updates from this DHCP server to the DNS server selected in the Remote Net Service option. You must select a DNS server for the Remote Net Service option. • If a DNS server is selected, you can configure the server to server configuration settings between this DNS server and the entity that you select in the Remote Net Service option. If the Remote Net Service option is “IPControl”, you are configuring the server to server configuration between the DNS server and the InControl DNS Listener. If the Remote Net Service option is another DNS server, you are configuring the server to server configuration between these two DNS servers. <p>When configuring DNS to DNS server pairs, a list of DNS options appears. These options are used to configure the Server configuration section of the <i>named.conf</i> file.</p>
Remote Net Service	<p>Select the remote network service that you want to communicate with the “Net Service”.</p> <ul style="list-style-type: none"> • If IPControl is selected, you are configuring the server to server configuration between the DNS server (specified in the “Net Service” selection) and the InControl DNS Listener. • If a BIND-based DNS server is selected, you can configure the server to server configuration settings between this DNS server and the entity that you select in the Net Service option. If the Net Service option is another DNS server, you are configuring the server to server configuration between these two DNS servers. • If a Microsoft DNS server is selected, you can configure the GSS-TSIG credentials to use for dynamic updates.
Enable TSIG Key	Checked indicates that communications between these two network services should use Transaction Keys.
TSIG Key	Choose a Key from the list of keys, or Generate a Key on the fly by entering in a key name. The key name must conform to fully qualified domain name rules, including a trailing dot for example: <i>key45.ins.com.</i>
Enable GSS-TSIG Key	<i>Microsoft DNS Server Only.</i> Checked indicates that the communications between these two network services should be secured using GSS-TSIG.

Field	Description
Realm Name	<i>Microsoft DNS Server Only.</i> For GSS-TSIG, enter the Microsoft Realm name. This is typically the same as the Microsoft AD domain name. By convention, it is entered in uppercase.
Principal Name	<i>Microsoft DNS Server Only.</i> For GSS-TSIG, enter the principal name that has authorization to update zones on the chosen DNS Server. By convention, this name has the format: “host/<agent-hostname>”, where <agent-hostname> is the FQDN of the agent associated with this Net Service. This field should match the Principal name configured in Active Directory. See “Creating GSS-TSIG enabled account in Microsoft MMC” on page 373 for instructions on how to set up this user.
Principal Password	<i>Microsoft DNS Server Only.</i> Enter the password associated with the Principal name in Active Directory.
Confirm Password	<i>Microsoft DNS Server Only.</i> Confirm the Principal password by re-entering it here.

Enter the desired attributes once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen. If the Net Service Pair was successfully added, the new product appears in the Net Service Pair list.

Editing a Network Service Pair

To modify an existing Network Service Pair definition, follow these steps.

1. On the Net Service Pairs screen (shown in Figure 3-72), click on a service name link in the Net Service list. The Edit Net Service Pair screen opens.

Edit Net Service Pair

Net Service: sapphire1.diamondip.com (BIND9 DNS) ▼

☐ Bogus: ☐ Yes ☐ No

☐ EDNS: ☐ Yes ☐ No

☐ Support IXFR: ☐ Yes ☐ No

☐ Provide IXFR: ☐ Yes ☐ No

☐ Request IXFR: ☐ Yes ☐ No

☐ Number of Transfers:

☐ Transfer Format: ☐ one-answer ☐ many-answers

Remote Net Service: sapphire2.diamondip.com (BIND9 DNS) ▼

☐ Bogus: ☐ Yes ☐ No

☐ EDNS: ☐ Yes ☐ No

☐ Support IXFR: ☐ Yes ☐ No

☐ Provide IXFR: ☐ Yes ☐ No

☐ Request IXFR: ☐ Yes ☐ No

☐ Number of Transfers:

☐ Transfer Format: ☐ one-answer ☐ many-answers

☒ Enable TSIG Key

TSIG Key: ☒ Choose a Key ▼

☐ Generate a Key 128 Bits ▼

Figure 3-74 Edit Net Service Pair

2. Edit the pair definition as needed. Refer to Table 3-27 for information on the fields or check boxes you wish to update.
3. Choose one of the following actions:
 - Click **Submit** to save your changes.
 - Click **Cancel** to return to the previous screen.

Chapter 4 Managing DNS

In IPControl 5.0, all the features you need to set up DNS servers are located in the DNS section of the Management menu. This chapter describes how to use each selection on the DNS menu.

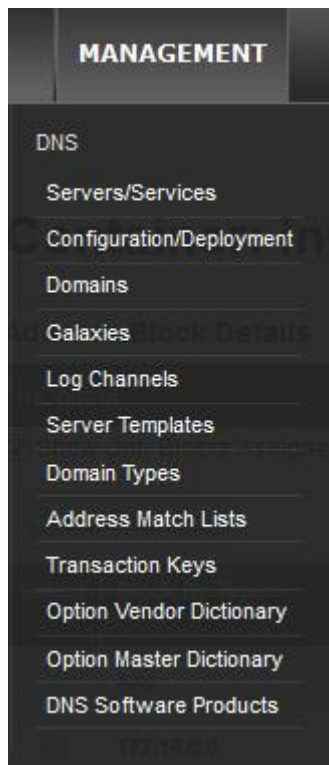


Figure 4-1 DNS Menu Selections

Servers/Services

The **Servers/Services** option in the DNS section of the **Management** menu allows you to define and maintain a layer 3 network DNS service. Use IPControl to manage and plan the IP address space, policies, options, and/or resource records that are allocated to your DNS network service. Then use IPControl to create the configuration files necessary for DNS services.

Managing DNS Servers/Services

To manage your DNS servers and services, follow these steps.

1. Select **Servers/Services** from the DNS section of the **Management** menu. The DNS Servers/Services window appears and the hierarchy changes to display your existing domain structure. Figure 4-2 shows an expanded hierarchy that illustrates the forward/reverse domains as well as the forward/reverse master zones.

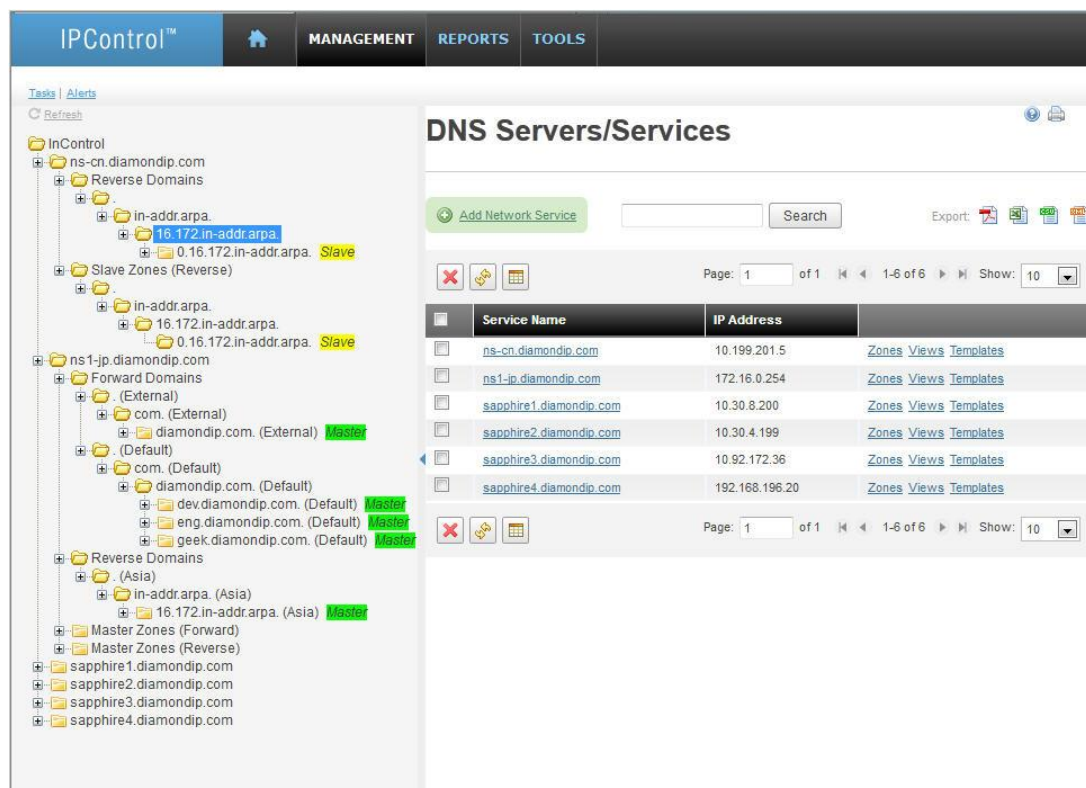



Figure 4-2 DNS Servers/Services Server List and DNS Domain Hierarchy

2. Choose from the following actions.

To ...	Then ...
Search for a particular DNS Network Service	<ol style="list-style-type: none"> 1. Enter a search string into the text block. 2. Click Search. The list of servers changes to match the search string.
Add a DNS Network Service	Refer to “Adding a DNS Network Service” on page 115.
Edit a DNS Network Service	<ol style="list-style-type: none"> 1. Click on the service entry in the Service Name list. The Edit DNS Server screen opens. 2. Edit fields and tab entries as needed. Refer to the descriptions in the following sections for more information.

To ...	Then ...
Add or edit a zone on an existing DNS Network Service	Refer to “Zones on a DNS Server” on page 122.
Add or edit a DNS View on an existing DNS Network Service	Refer to “Configuring DNS Views on a DNS Server” on page 128.
Add or edit a DNS Template on an existing DNS Network Service	Refer to “Configuring Zone Templates on a DNS Server” on page 131.
Delete one or more DNS Network Services	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Network Services, or Cancel to return to the previous screen.

3. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen. If the DNS server was successfully added or modified, the DNS server appears in the **Service Name** list.

Adding a DNS Network Service

To add a DNS Network Service, follow these steps:

1. Select the **Add Network Service** link. The Choose DNS Template screen appears, as shown in Figure 4-4.



Figure 4-3 Choose Network Service Type

2. Select a DNS template from the drop-down list. For more information on DNS Server templates, refer to “Server Templates” on page 151.

Note: Keep this value set to “None” when adding a Microsoft or CNR DNS server.

3. Click **Submit**. If a template was selected, the Add DNS Server from template <DNS Template Name> screen appears, as shown in Figure 4-4.

Add DNS Server from template "Standard for INS Sapphire DNS (BIND 9.6)"

General Logging Extensions Root Hints File Advanced Options

Name:	<input type="text"/>
IP Address:	<input type="text"/>
Create db.127.0.0 Loopback Address File:	<input checked="" type="checkbox"/>
Configuration Directory:	<input type="text" value="/opt/incontrol/dns/etc"/>
Data Directory:	<input type="text" value="/opt/incontrol/dns/db"/>
Product:	INS Sapphire DNS (BIND 9.6) ▼
Agent:	Executive Agent ▼
Start Script:	<input type="text" value="/opt/incontrol/etc/named_start"/>
Stop Script:	<input type="text" value="/opt/incontrol/etc/named_stop"/>
Configuration File Check Script:	<input type="text" value="/opt/incontrol/etc/named_check_conf.sh"/>
Zone File Check Script:	<input type="text" value="/opt/incontrol/etc/named_check_zone.sh"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Figure 4-4 Add DNS Server

General Tab Settings

Table 4-1 General Tab Parameters

Field	Description
Name	Enter the name of this DNS Server. Typically, this is the fully qualified domain name of the system where the service is running.
IP Address	Enter the IP Address of this service. This is required if you use IPControl to collect configuration information from this service, or create configuration files for this service.
Create db.127.0.0 Loopback Address File	Check this box to automatically create the db.127.0.0 loopback file during a DNS Configuration File creation task. This file contains the information that is needed by the server for it to direct traffic to itself.
Configuration Directory	Enter the fully qualified pathname of where the configuration file named.conf will be created. The typical entries are listed below: UNIX DNS: /opt/incontrol/dns/etc Windows DNS: C:\Program Files\Diamond IP\InControl\dns\etc
Data Directory	Enter the fully qualified pathname of where the data files (zone files) are created. The typical entries are listed below: UNIX DNS: /opt/incontrol/dns/db Windows DNS: C:\Program Files\Diamond IP\InControl\dns\db

Field	Description
Product	Select the Product from the drop-down list of DNS products available within this system. Use the DNS Software Products option on the Management > DNS menu to manage products defined within the system.
Agent	Select the Agent that is used to collect and distribute information to this service. This is required if you use IPControl to collect configuration information for planned <i>vs.</i> actual comparisons.
Start Script	The script that is used to start the DNS server. This script will be called by IPControl to start a DNS server. UNIX: /opt/incontrol/etc/named_start WINDOWS: C:\Program Files\Diamond IP\InControl\etc\named_start.bat
Stop Script	The script that is used to start the DNS server. This script will be called by IPControl to start a DNS server. UNIX: /opt/incontrol/etc/named_stop WINDOWS: C:\Program Files\Diamond IP\InControl\etc\named_stop.bat
Configuration File Check Script	The script that verifies the DNS server's configuration file (named.conf). When creating a configuration task for this server, the administrator can have IPControl call this script to ensure that a valid configuration has been generated for the server. The configuration file is copied to the DNS server and the check script runs against the file in a temporary directory. If the check is successful, the server is stopped and the new configuration file replaces the existing file, and then the DNS server is restarted. UNIX: /opt/incontrol/etc/named_check_conf.sh WINDOWS: C:\Program Files\Diamond IP\InControl\etc\named_check_config.cmd
Zone File Check Script	The script that verifies the DNS server's zone files. When creating a configuration task for this server, the administrator can have IPControl call this script to ensure that valid zone files have been generated for the server. The zone files are copied to the DNS server and the check script runs against the files in a temporary directory. If the check is successful, the server is updated with the new zone files. UNIX: /opt/incontrol/etc/named_check_zone.sh WINDOWS: C:\Program Files\Diamond IP\InControl\etc\named_check_zone.cmd

Logging Tab Settings

The **Logging** tab allows the configuration of the logging statements for the DNS server. Logging for BIND DNS servers is accomplished with two main concepts: *channels* and *categories*. A channel specifies where logged data goes (that is, syslog, to a file, and so on). A category specifies what data is logged. In a BIND-based DNS server, most messages are categorized by function.

The **Logging** tab displays when you edit a server only.

This option allows you to select logging channels for each category that is defined for the server. Refer to “Adding a Logging Channel” on page 149 to create a selectable list.

Add DNS Server from template "Standard for INS Sapphire DNS (BIND 9.6)"

General **Logging** Extensions Root Hints File Advanced Options

Categories	Channels
<input type="checkbox"/> EDNS Disabled	Choose
<input type="checkbox"/> Query Errors	Choose
<input type="checkbox"/> Default	Choose
<input type="checkbox"/> Dispatch	Choose
<input type="checkbox"/> Delegation Only	Choose
<input type="checkbox"/> Lame Servers	Choose
<input type="checkbox"/> Notify	Choose
<input type="checkbox"/> Queries	Choose
<input type="checkbox"/> Security	Choose
<input type="checkbox"/> Inbound Zone Transfers	Choose
<input type="checkbox"/> Dynamic Updates	Choose
<input type="checkbox"/> General	Choose
<input type="checkbox"/> Outbound Zone Transfers	Choose
<input type="checkbox"/> Configuration	Choose
<input type="checkbox"/> Client	Choose
<input type="checkbox"/> Network	Choose
<input type="checkbox"/> DNSSEC	Choose
<input type="checkbox"/> Database	Choose
<input type="checkbox"/> Resolver	Choose
<input type="checkbox"/> Update Security	Choose
<input type="checkbox"/> Unmatched	Choose

Submit Cancel

Figure 4-5 Logging Tab

To add a channel to a category, click the **Choose** button next to the category. The Logging Channels screen opens.

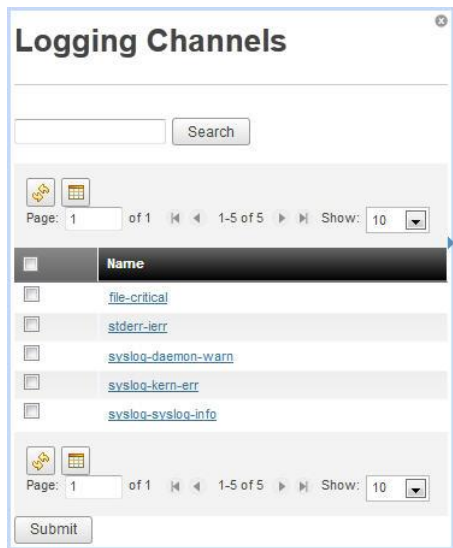


Figure 4-6 Select Logging Channels

Click on the checkbox next to the Channels that you want to assign to this category, and once finished, click **Submit** to save your changes.

Extensions Tab Settings

Click on the **Extensions** tab to display the configuration file extensions area. The extensions area allows you to create free form text to add to the beginning or the end of the named.conf configuration file.

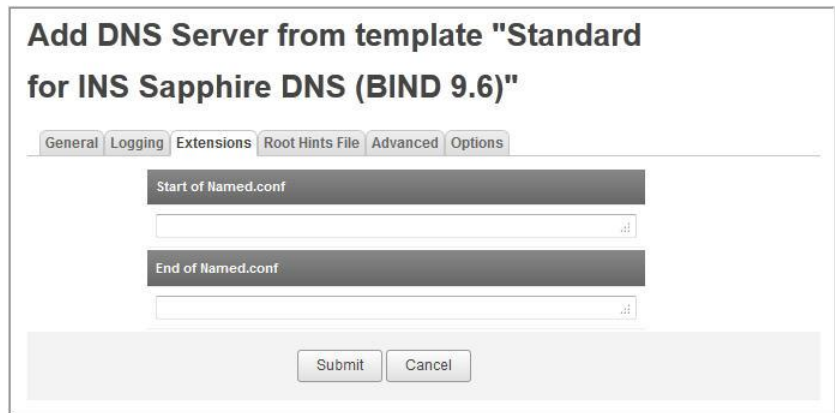


Figure 4-7 Extensions Tab

Table 4-2 Extensions Tab Parameters

Field	Description
Start of named.conf	A free text area that appears at the beginning of the named.conf file when the file is automatically generated. Note: The extensions are limited to 32000 characters.

Field	Description
End of named.conf	A free text area that appears at the end of the <code>named.conf</code> file when the file is automatically generated. Note: The extensions are limited to 32000 characters.

Root Hints Tab Settings

Click on the **Root Hints** tab to display the configuration of the Root Hints file. The Root Hints file tells the DNS server where the name servers for the root zone are.

Figure 4-8 Roots Hints File Tab

Table 4-3 Root Hints Tab Parameters

Field	Description
Create Root Hints File	Check this item on if you want to automatically create the Root Hints file when generating the DNS Configuration files.
Use Standard InterNIC supplied content	Only valid if you have checked the Create Root Hints file option. Select this option if you would like to use the InterNIC supplied content when generating this file.
Use Custom Root Hints file	Only valid if you have checked the Create Root Hints file option. Select this option if you would like to use custom content that you enter for the Roots Hints file.

Advanced Tab Settings

Click on the **Advanced** tab to display the available advanced options. These options include configuration of the “controls” section of the configuration file.

Traditionally, DNS administrators controlled the BIND DNS server with UNIX signals. The DNS server interprets certain signals as an instruction to take a particular action, such as reloading changed zones. Due to a limited number of signals, BIND has introduced a method of controlling the name server by sending messages to it on a special control channel. The

control channel can be either a UNIX socket, or a TCP port that the name server listens on for messages.

Figure 4-9 Advanced Tab

Table 4-4 Advanced Tab Parameters

Field	Description
TCP Port Control Channel Settings:	Select this option to send messages to the name server via a TCP/IP Port.
Listen on IP Address	Enter the IP Address for the name server to listen on for messages.
Listen on Port	Enter the Port that the name server will listen on for messages. Typically, this is port 953.
Allow Message From	Enter an IP Address or Address Match List name that specifies where messages are allowed to come from.
UNIX Domain Socket Channel Settings:	Select this option to send messages to the name server via a UNIX Domain Socket.
UNIX Domain Socket	Enter the name of the socket that will be used for communicating with the name server. Typically this is <code>/var/run/ndc</code> , though some operating systems use a different pathname. The socket is usually owned by root and readable and writable only by the owner.
Permissions (octal)	The permission value must be specified as an Octal number (with a leading zero to indicate an octal quantity). For example; 0660
Owner	Enter the Owner identifier.
Group	Enter the Group identifier.

Options Tab Settings

Click on the **Options** tab to display the options and directives that are available. The options displayed are dependent upon the Product selected and the items configured in the Option Vendor Dictionary. For more information on DNS option vendors, refer to “DNS Option Vendor Dictionary” on page 168.

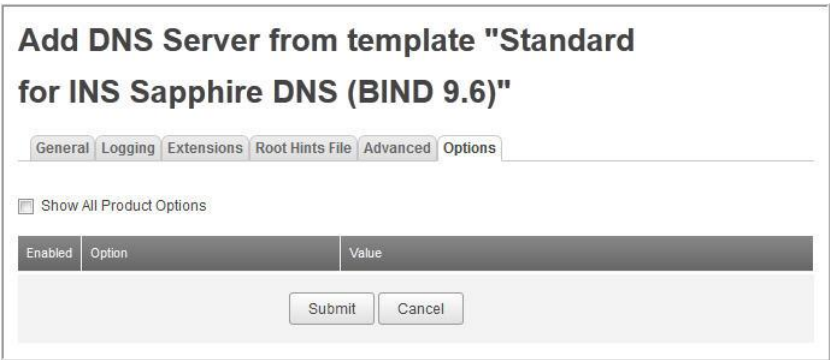


Figure 4-10 Options Tab

To view all available options for this product, select **Show All Product Options**. All options configured for the product selected on the **General** tab are displayed.

Configure each option that you want to appear in the named.conf configuration file.

Important! If this server is running on a Sapphire TwinMirror Appliance, there are some options that should be configured for proper operation. Refer to “Configuring DNS on a TwinMirror Appliance” on page 390 for more details.




Zones on a DNS Server

DNS Zones is the mechanism that is used to link DNS domains to DNS Servers. IPControl provides you with complete control over DNS zones in order to provide you with the capability to model complex DNS infrastructure if needed. Click on the **Zones** link on the Network Services List to display the DNS Zones for the selected server.



Figure 4-11 DNS Zones

Choose from the following actions.

- To delete one or more DNS Zones from this server, click the checkbox in the **Select** column for each item you wish to delete, and click . At the confirmation prompt, click **OK** to delete the selected zones, or **Cancel** to not delete any zones.
- To refresh the DNS Zones list, click .
- To exit the DNS Zones list and return to the list of servers, click .
- To add a DNS Zone, refer to the following section.
- To edit a DNS Zone, refer to “Editing a DNS Zone” on page 128.

Adding a DNS Zone

To add a DNS Zone, follow these steps.

1. Click the **Add DNS Zone** link. The Add DNS View screen appears.

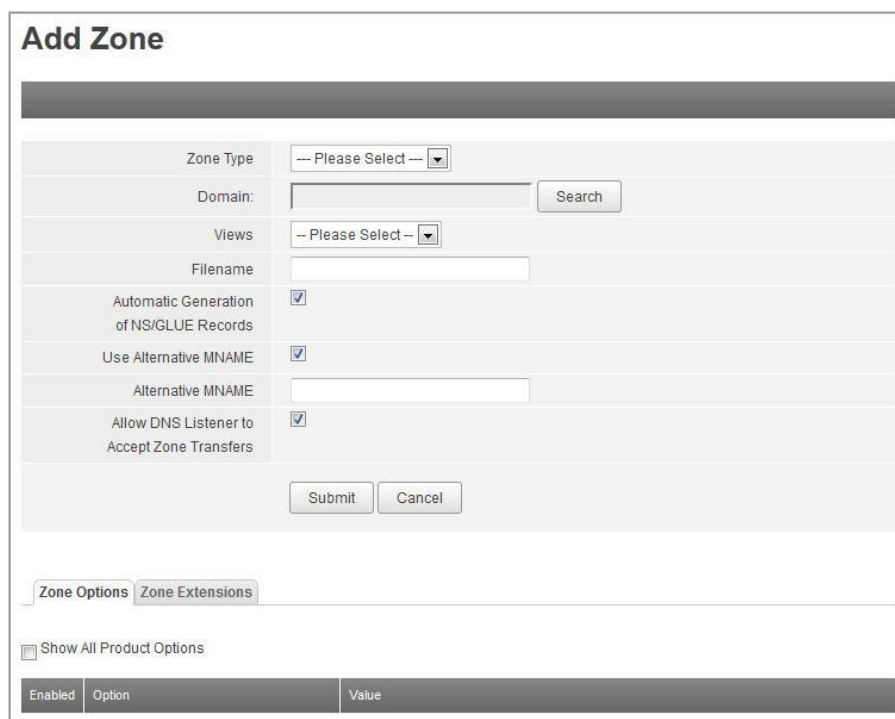


Figure 4-12 Zone Options

2. Select the type of zone you want to create. The choices are:
 - master
 - slave
 - forward
 - stub

The **Show All Product Options** checkbox is automatically selected and different zone options appear depending on the selected zone type.

3. In the **Domain** field, select the domain you want to attach to the DNS server. Click **Search** to open the Domain Search screen, where you can refine your search to **Forward** and **Reverse** servers, in addition to **All**.
4. *Optional for non-master zones.* Enter the filename to contain the DNS zone data that is automatically created. The data can be overwritten, if necessary.
5. Choose from the following actions.
 - If you select **master**, enter the data described in Table 4-5.

Table 4-5 Master Zone Type Parameters

Field	Description
Automatic Generation of NS/Glue Records	Checked indicates that you will let IPControl automatically create the NS and Glue Records for this zone/domain. If you uncheck this option, the IPControl system will not automatically create these records, and you may enter your own NS and Glue records. Please refer to your DNS administrative manual for correct creation of the required records. Failure to create the proper NS and Glue records potentially will prohibit the DNS server from starting, or loading this zone.
Use Alternative MNAME	Select this checkbox to indicate that you want to use an alternative MNAME within the SOA record. Enter that MNAME in the Alternative MNAME field.
Allow DNS Listener to Accept Zone Transfers	<i>Applicable only for master zones.</i> Select this checkbox to ensure that the IPControl DNS Listener accepts zone transfers from this server for this zone, if the zone is dynamic.

- ▶ If you select **slave** or **stub**, enter the IP addresses of the master DNS servers for this slave/stub zone in the **Masters** field. These addresses map to the “masters” option on the zone. For example: 10.0.0.2; 10.0.0.6.
 - a. Select the necessary zone options, described in Table 4-6.
 - b. To add zone extensions, click the **Zone Extensions** tab and enter extension data as needed in the **Insert Prior to Resource Records** and **Insert After Resource Records** columns.
 - c. When your definition of the zone for the selected server is complete, click **Submit** to save your changes.

Table 4-6 Zone Options

Field	Description
Allow notify	<i>Slave only.</i> Specifies which hosts are allowed to notify this server, a slave, of zone changes in addition to the zone masters. When used in the zone statement, it overrides the options allow-notify statement. If not specified, the default is to process notify messages only from a zone's master. Click Address List to select a match list.
Allow query	<i>Master, Slave, Stub.</i> Specifies which hosts are allowed to ask ordinary DNS questions. When used in the zone statement, it overrides the options allow-query statement. If not specified, the default is to allow queries from all hosts. Click Address List to select a match list.
Allow transfer	<i>Master, Slave, Stub.</i> Specifies which hosts are allowed to receive zone transfers from the server. When used in the zone statement, it overrides the options allow-transfer statement. If not specified, the default is to allow transfers to all hosts. Click Address List to select a match list.
Allow update	<i>Master only.</i> Defines an address match list of IP addresses that are allowed to send updates to the zone. When set, the zone is considered to be a dynamic zone and will appear for DDNS task types. Click Address List to select a match list.
Also notify	<i>Master, Slave.</i> Defines a global list of IP addresses of name servers that are also sent NOTIFY messages whenever a fresh copy of the zone is loaded, in addition to the servers listed in the zone's NS records. This helps to ensure that copies of the zones will quickly converge on stealth servers. When used in a zone statement, it overrides the options also-notify statement. When a zone notify statement is set to no , the IP addresses in the global also-notify list will not be sent NOTIFY messages for that zone. The default is the empty list (no global notification list). Click Edit and then Add Row to add a list of IP addresses and ports.
Check names	<i>Forward, Master, Slave, Stub.</i> This option is used to restrict the character set and syntax of certain domain names in master files and/or DNS responses received from the network. The default varies according to zone type. For master zones the default is fail . For slave zones the default is warn .

Field	Description
Dialup	<p>Master, Slave, Stub. When selected, the server treats all zones as if they are doing zone transfers across a dial on demand dialup link, which can be brought up by traffic originating from this server. This has different effects according to zone type and concentrates the zone maintenance so that it all happens in a short interval, once every heartbeat-interval and hopefully during the one call. It also suppresses some of the normal zone maintenance traffic.</p> <p>If the zone is a master zone then the server will send out a NOTIFY request to all the slaves (default). This should trigger the zone serial number check in the slave (providing it supports NOTIFY) allowing the slave to verify the zone while the connection is active. The set of servers to which NOTIFY is sent can be controlled by notify and also-notify.</p> <p>If the zone is a slave or stub zone, then the server will suppress the regular “zone up to date” (refresh) queries and only perform them when the heartbeat-interval expires in addition to sending NOTIFY requests.</p> <p>Finer control can be achieved by using notify which only sends NOTIFY messages, notify-passive which sends NOTIFY messages and suppresses the normal refresh queries, refresh which suppresses normal refresh processing and sends refresh queries when the heartbeat-interval expires, and passive which just disables normal refresh processing.</p>
Forward	<p>Forward, Master, Slave, Stub. This option is only meaningful if the forwarders list is not empty. A value of first, the default, causes the server to query the forwarders first, and if that does not answer the question, the server will then look for the answer itself. If only is specified, the server will only query the forwarders.</p>
Forwarders	<p>Forward, Master, Slave, Stub. Specifies the IP addresses to be used for forwarding. The default is the empty list (no forwarding). Click Edit and then Add Row to add a list of IP addresses and ports.</p>
Max refresh time	<p>Master, Slave, Stub. Specifies the maximum amount of refresh time in seconds that a server can refresh a zone (querying for SOA changes).</p>
Max retry time	<p>Master, Slave, Stub. Specifies the maximum number of times that a server can retry failed transfers.</p>
Max transfer idle in	<p>Slave, Stub. Inbound zone transfers making no progress in this many minutes will be terminated. The default is 60 minutes (1 hour). The maximum value is 28 days (40320 minutes).</p>
Max transfer idle out	<p>Master, Slave, Stub. Outbound zone transfers making no progress in this many minutes will be terminated. The default is 60 minutes (1 hour). The maximum value is 28 days (40320 minutes).</p>
Max transfer time in	<p>Slave, Stub. Inbound zone transfers running longer than this many minutes will be terminated. The default is 120 minutes (2 hours). The maximum value is 28 days (40320 minutes).</p>
Max transfer time out	<p>Master, Slave, Stub. Outbound zone transfers running longer than this many minutes will be terminated. The default is 120 minutes (2 hours). The maximum value is 28 days (40320 minutes).</p>

Field	Description
Min refresh time	<i>Master, Slave, Stub.</i> Specifies the minimum amount of refresh time in seconds that a server can refresh a zone (querying for SOA changes).
Min retry time	<i>Master, Slave, Stub.</i> Specifies the maximum number of times that a server can retry failed transfers.
Notify	<p><i>Master, Slave.</i> DNS NOTIFY is a mechanism that allows master servers to notify their slave servers of changes to a zone's data. In response to a NOTIFY from a master server, the slave will check to see that its version of the zone is the current version and, if not, initiate a zone transfer.</p> <p>If yes is selected, DNS NOTIFY messages are sent when a zone the server is authoritative for changes, see the section called “Notify”. The messages are sent to the servers listed in the zone's NS records (except the master server identified in the SOA MNAME field), and to any servers listed in the also-notify option.</p> <p>If explicit is selected, notifies are sent only to servers explicitly listed using also-notify. If no is selected, no notifies are sent.</p>
Notify source	<p><i>Master, Slave.</i> Determines which local source address, and optionally UDP port, will be used to send NOTIFY messages. This address must appear in the slave server's masters zone clause or in an allow-notify clause. This statement sets the notify-source for all zones, but can be overridden on a per-zone / per-view basis by including a notify-source statement within the zone or view block in the configuration file.</p> <p>Click Edit and then Add Row to add a list of IP addresses and ports.</p>
Notify source v6	<p><i>Master only.</i> Like notify-source, but applies to notify messages sent to IPv6 addresses.</p> <p>Click Edit and then Add Row to add a list of IP addresses and ports.</p>
SIG validity interval	<i>Master only.</i> Specifies the number of days into the future when DNSSEC signatures automatically generated as a result of dynamic updates will expire. The default is 30 days. The maximum value is 10 years (3660 days). The signature inception time is unconditionally set to one hour before the current time to allow for a limited amount of clock skew.
Transfer source	<p><i>Slave, Stub.</i> Determines which local address will be bound to IPv4 TCP connections used to fetch zones transferred inbound by the server. It also determines the source IPv4 address, and optionally the UDP port, used for the refresh queries and forwarded dynamic updates. If not set, it defaults to a system controlled value which will usually be the address of the interface “closest to” the remote end.</p> <p>This address must appear in the remote end's allow-transfer option for the zone being transferred, if one is specified. This statement sets the transfer-source for all zones, but can be overridden on a per-view or per-zone basis by including a transfer-source statement within the view or zone block in the configuration file.</p> <p>Click Edit and then Add Row to add a list of IP addresses and ports.</p>

Field	Description
Transfer source v6	<i>Slave, Stub.</i> The same as transfer-source , except zone transfers are performed using IPv6. Click Edit and then Add Row to add a list of IP addresses and ports.

Editing a DNS Zone

To modify an existing DNS Zone, click on the Zone name in the DNS Zone List. The Edit DNS Zone screen opens.

Edit Zone: 0.16.172.in-addr.arpa

Zone Type	slave
Domain:	0.16.172.in-addr.arpa (Asia)
Filename	
Masters	172.16.0.254

Submit Cancel

Zone Options Zone Extensions

☐ Show All Product Options

Enabled	Option	Value
---------	--------	-------

Figure 4-13 Edit Zone

Edit the DNS Zone as needed. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Configuring DNS Views on a DNS Server

DNS Views are very useful in a firewalled environment since they allow you to present one name server configuration to one community of hosts and a different configuration to another community. This is particularly handy if you're running a name server on a host that receives queries from both internal and external hosts.

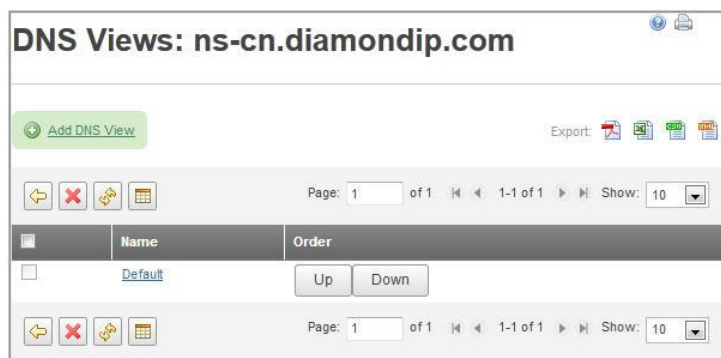


Figure 4-14 DNS View List

Choose from the following actions:

- To delete one or more DNS Views, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected channels, or **Cancel** to not delete the selected channels.
- To refresh the DNS Views list, click .
- To exit the DNS Views list and return to the list of servers, click .
- To add a DNS View, refer to the following section.
- To edit a DNS View, refer to “Editing a DNS View” on page 130.

Adding a DNS View

To add a DNS View, click the **Add DNS View** link. The Add DNS View screen appears.

Figure 4-15 Add DNS View

Table 4-7 Add DNS View Parameters

Field	Description
General Tab	
Name	Enter a unique name for the DNS View.
Class	Select the appropriate Class that will be assigned to this view.
Match Clients	Specify the hosts that will 'see' the view using this statement. Any hosts that are part of this group will see this view. You may use an ACL name to make this option more readable. This options checks the source IP Address of the host.
Match Destinations	Specify the hosts that will 'see' the view using this statement based on the destination IP Address of the packet.
Match Recursive Only	Checked indicates that only recursive requests from matching clients will match this view.
Options Tab	
Show all options	Click on this option to display all DNS options that are available to be associated with this view. Many of the options are described in Table 4-6 on page 125.
Zones Tab	
Search	Displays the zones that are associated with this view. Use the search function to filter the list of zones that are displayed on this page. To associate a zone with a view, select it in the list.

Enter the desired attributes and then click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Once created, you may reorder the DNS Views by pressing the corresponding **Up** and **Down** buttons.

Editing a DNS View

To modify an existing DNS View, click on the view name in the DNS View List. This takes you to the Edit DNS View list Screen.

The screenshot shows a window titled "Edit : Default". At the top, there are three tabs: "General", "Options", and "Zones". The "General" tab is selected. Below the tabs, there are several input fields and a checkbox:

- Name: Default
- Class: IN
- Match Clients: any
- Match Destinations: any
- Match Recursive Only: ☐

At the bottom left of the window, there are two buttons: "Save" and "Cancel".

Figure 4-16 Edit DNS View

Edit the DNS View as needed. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Configuring Zone Templates on a DNS Server

In some cases, if you are dealing with large numbers of domains, you may want create a “template” zone data file that allows you to use a single data file for multiple zones. IPControl supports this feature using this “template” domain menu item. It allows you to create a “template” domain, associate resource records within that domain, and then utilize that single domain over and over for various zones.

Make sure that all of the owner names of records within the zone are “@” (short for origin), or relative, and do not include a trailing dot.

Configuration/Deployment

The Configuration/Deployment option allows you to create on-demand, scheduled, or recurring scheduled tasks for deployment of configuration information to your DNS network services.

Configuration/Deployment Task Definition Options

To deploy configuration information to a network service, select the “task type”, select the “network service”, and then specify when to run the task. Depending upon the selection of when you will be running the task, different options will be displayed on the screen for you to select. Refer to the sections below for additional information about each option. Note that

once you click **Submit**, a new task will be created, and submitted to the system. Once tasks have been created, they can be managed using the **Task** menu option.

Figure 4-17 Configuration/Deployment

Table 4-8 Configuration/Deployment Screen Elements

Field	Description
Task Type	<p>Select the type of task that you want to run.</p> <ul style="list-style-type: none"> • DNS Configuration – All Files creates all configuration files (configuration and zones) for the DNS server that you selected. • DNS Configuration – Changed Zones Only creates the configuration file and only the changed zone files for the DNS server that you selected. • DNS Configuration – Selected Zones Only creates the configuration file and only the selected zone for the DNS server that you have selected. <p>Note: For more information, refer to “Configuring INS DNS for Selected or Changed Zone Push” on page 349.</p> <ul style="list-style-type: none"> • DNS Configuration – Configuration Only creates only the configuration file for the DNS server that you selected. • DNS Configuration – Changed Resource Records Only (via DDNS) sends all changed resource records to the selected DNS server via RFC2136 dynamic DNS updates. • DNS Configuration – All Resource Records (via DDNS) sends all resource records for the selected zone, or all zones, for the selected DNS server via RFC2136 dynamic DNS updates. • DNS Configuration - - All User-created Resource Records (via DDNS) is similar to the previous option. However, the resource records selected are limited to those created on IP Control via the GUI or a CLI/API. This enables the refreshing of these records in Microsoft AD DNS to prevent their scavenging, while not interfering with the intended scavenging of dynamic records.
The following options are based on which type of task is selected	
Perform DNS configuration file check	If checked, then the configuration file check script specified when the DNS net service was created will be run against the <code>named.conf</code> file created for DNS Configuration tasks.
Perform DNS zone file check	If checked, then the zone file check script specified when the DNS net service was created will be run against the zone files created for DNS Configuration tasks.

Field	Description
Stop on Critical Errors	For DNS Configuration tasks, if either the Perform DNS Configuration File Check or Perform DNS Zone File Check options are selected, selecting this task option causes the configuration task to abort if either of the check scripts returns a non-zero value, indicating an error has been found in the configuration or zone file. If aborted, the DNS server is not stopped or restarted, and the current DNS configuration remains unchanged.
Hold files for preview	If checked, the configuration files will be created, but not deployed. You can view the files from the Task List.
Delete Task if No Zone to Generate	If checked, indicates that the task will be deleted when there are no changes to the configuration.
Delete Task if No Resource Records to Generate	If checked, indicates that the task will be deleted when there are no changes to the configuration.
Network Service	Select Search and select a network service to perform this task against.
Zone	Select Search and select a Zone to perform this task against.
When to run task	<ul style="list-style-type: none"> • Immediate – Run the task immediately • Scheduled – Run the task on the predetermined date and time specified • Recurring – Run this task multiple times

On-demand (Immediate) Config/Deployment Task

To define an immediate task, define the task parameters and select **Immediate** from the **When to run task** options. Click **Submit** to create the task. A new task is created and submitted to the system. Once tasks have been created, they can be managed using the **Task** menu option. This is the default selection for all task types.

Scheduled Config/Deployment Task

To schedule a future task, define the task parameters and select **Scheduled** from the **When to run task** selections. Schedule options are displayed, as shown in Figure 4-18.





Figure 4-18 Scheduled Configuration/Deployment

To select a future date to run the task, type in the desired date in mm/dd/yyyy format or click the calendar icon to select a date. A calendar is displayed, as shown in Figure 4-19, with today's date selected by default.



Figure 4-19 Calendar Utility

You can use the following navigation links to change to another month and/or year and then select a date in the month to close the utility:

-  Previous Year
-  Previous Month
-  Next Year
-  Next Month

Select the hours, minutes, and AM or PM to schedule a specific time for the task.

Figure 4-20 Hour and Minutes

Once all parameters have been entered, click **Submit**. A new task is created, and submitted to the system with the time scheduled. Once tasks have been created, they can be managed using the **Tasks** menu option on the **Tools** menu.

Recurring Config/Deployment Task

A recurring task enables you to define tasks to run on a pre-determined schedule. This option allows you to define tasks (such as DNS Configuration) that will occur at regular intervals, providing you with up to date information. To schedule a recurring task, set the task parameters and select **Recurring** from the **When to run task** selections. Recurring options are displayed as shown in Figure 4-21.

The screenshot shows a web form titled "DNS Configuration/Deployment". It contains several sections for configuring a task:

- Task Type:** A dropdown menu set to "DNS Configuration - Changed Zones Only".
- Checkboxes:**
 - Perform DNS configuration file check: ☒
 - Perform DNS zone file check: ☒
 - Stop on Critical Errors: ☒
 - Hold files for preview: ☐
 - Delete Task if No Zones to Generate: ☐
- Network Service:** A text input field containing "ns-cn.diamondip.com" and a "Search" button.
- When to run task:** Radio buttons for "Immediate", "Scheduled", and "Recurring". The "Recurring" option is selected.
- Select the date and time that this task is to begin:** A date picker showing "12/27/2011", time dropdowns for "01", "00", and "AM", followed by "(hh:mm)".
- Select the Options for this Recurring Task:**
 - Frequency:** Radio buttons for "Sub-Daily", "Daily", "Weekly", "Monthly", and "Yearly". The "Daily" option is selected.
 - Beginning at the Date and Time Selected Above
- Submit:** A button at the bottom of the form.

Figure 4-21 Recurring Configuration/Deployment

Select the date and time that the recurring task is to begin. This is the first occurrence of the recurring task. Click on the calendar icon to display a calendar, as shown in Figure 4-19. Refer to "Scheduled Config/Deployment Task" on page 133 for information on using the calendar utility.

Select the **Frequency** for the recurring task:

- Sub-Daily
- Daily
- Weekly
- Monthly
- Yearly

Once all the parameters have been selected or entered, click **Submit**. A new task is created and submitted to the system. Once tasks have been created, you can manage them using the **Tasks** menu option on the **Tools** menu.

To stop a recurring task, delete the next scheduled recurrence from the **Tasks** menu option on the **Tools** menu.

Domains

DNS's distributed database is indexed by domain names. Each domain name is essentially just a path in a large inverted tree, called a domain name space. The tree's hierarchical structure is similar to the structure of the UNIX file system. The tree has a single root at the top. This is called the root directory, represented by a slash. DNS simply calls it "the root", and it is represented with a dot or period ".". Like a file system, DNS's tree can branch out any number of ways at each intersection point (or node). Each node of the tree has a text label that can be up to 63 characters long.

Managing DNS Domains



To work with DNS domains, follow these steps.

1. Select **Domains** from the DNS section of the **Management** menu. The hierarchy refreshes to show the zones in the root container and a list of domains appears, as shown in Figure 4-22.

Domain	Type	Derivative	User Defined Fields
.	Default	Standard	
.	External	Standard	
.	Asia	Standard	
.	Americas	Standard	
0-127.13.30.10.in-addr.arpa	Default	Standard	
0-127.30.35.68.in-addr.arpa	Default	Standard	
0-127.46.35.68.in-addr.arpa	Default	Standard	
0.0.0.0.0.0.0.0.f.a.d.e.f.f.4.ip6.arpa	Default	Standard	
0.0.0.0.0.0.4.0.f.a.d.e.f.f.4.ip6.arpa	Default	Standard	
0.0.0.0.4.0.0.0.f.a.d.e.f.f.4.ip6.arpa	Default	Standard	

Figure 4-22 DNS Domain List

2. Choose from the following actions.

To ...	Then ...
Search for a particular DNS Domain	<ol style="list-style-type: none"> 1. Select All, Forward, or Reverse from the Search drop-down list. 2. Enter a search string in the text block. 3. Click Search. The list of domains changes to match the search string.
Add a DNS Domain	Refer to “Adding a DNS Domain” following.
Refresh the DNS Domain list	Click  .
Edit a DNS Domain	<ol style="list-style-type: none"> 1. Click on the domain name in the Domain list. The Edit DNS Domain <i><domainname></i> screen opens. 2. Edit fields and tab entries as needed. Refer to “Editing a DNS Domain” on page 140.
Delete one or more DNS Domains	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Domains, or Cancel to return to the previous screen.

3. After you have finished entering the desired attributes, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Adding a DNS Domain

To add a DNS Domain, follow these steps.

1. Click the **Add DNS Domain** link. The Create DNS Domain screen appears.

Create DNS Domain

Name	<input type="text"/>
Managed	<input checked="" type="checkbox"/>
Delegated	<input checked="" type="checkbox"/>
Reverse:	<input type="checkbox"/>
Domain Type	Default <input type="button" value="v"/>
Derivative	<input checked="" type="radio"/> Standard <input type="radio"/> Template <input type="radio"/> Alias
Serial Number:	<input type="text" value="1"/>
Refresh:	<input type="text" value="10800"/>
Retry:	<input type="text" value="3600"/>
Expire:	<input type="text" value="604800"/>
Negative Cache TTL:	<input type="text" value="86400"/>
Default TTL:	<input type="text" value="86400"/>
Contact	<input type="text" value="dns-guru@diamondip.com"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Figure 4-23 Create DNS Domain

2. Type the requisite values in the fields, as described in Table 4-9.

Table 4-9 Create DNS Domain Parameters

Field	Description
Name	Enter a unique name for this Domain. A trailing dot is not required, because IPControl automatically applies one if it is missing.
Managed	<p>Check indicates that this domain/zone is fully defined in IPControl. That is, all resource records and all other definitions about this domain/zone will be completely described in the IPControl product. A “Managed” Type (and only a Managed Type) can be associated to a DNS server as a DNS “Master”. It can also be associated to an IPControl DNS server as a “Slave”, “Stub”, or “Forward” zone, but only if the zone is associated to at least one “Master” IPControl DNS server. For example, a zone, company.com, can be defined as a Master on server DNS1, a Slave, on server DNS2 (pointing to DNS1 as its Master), a Stub on DNS3 (pointing back to DNS1 and DNS2 as authoritative), and a Forward on DNS4 (forwarding to DNS1 and DNS2). Also, a Managed domain/zone can be associated to multiple IPControl DNS servers as “Masters”. A “Delegate-Only” zone is treated exactly like a Master, but a BIND 9.2.3 server (or higher) would only respond with delegation (referral) information for child zones defined, not with any authoritative information from the zone itself. We can replicate this same behavior in pre-BIND 9.2.3 servers by never populating the zone file with anything but SOA, NS and glue records. The reason for this unorthodox label (“Managed”) for a domain/zone is to differentiate between the domain Type (Managed) and how it can be associated to DNS Servers (as Master, Slave, Stub, or Forward DNS server).</p> <p>Unchecked indicates that this domain/zone is “Un-Managed”— This domain/zone is declared to IPControl as falling outside the scope of IPControl definition. It is a way to get a zone statement into a DNS server that is a Slave, Stub or Forward for a zone defined outside of IPControl. For example, if there is a business partner that has the domain anothercompany.com, and nothing is known about this zone in IPControl, yet an IPControl DNS server will need to have some information about it, an Un-Managed domain in IPControl will allow the proper zone statement to be built in the boot file to get information from a DNS Server outside the IPControl definition sphere.</p>
Delegated	Checked indicates that this domain may be associated directly with a zone file. If the delegated flag is turned off, this domain and its resource records will be written in a zone file that is associated with a parent domain.
Reverse	Checked indicates that this is a reverse domain.

Field	Description
Derivative	<p>The role of this domain.</p> <ul style="list-style-type: none"> • Standard – indicates a standard domain. • Template – indicates that this domain is a template and can be used as a template domain for when you want to use a single data file for multiple zones. • Alias – indicates that this domain is aliased to a specified template. In this case, no resource records are attached to the alias, all resource records are inherited from the template domain. When this type of domain is specified, the user must select a “template” domain to associate with this alias.
Serial Number	DNS Serial number for this domain. Default is 1.
Refresh	The refresh interval tells a slave for the zone how often to check that the data for this zone is up to date. Default is 10800.
Retry	If the slave fails to reach the master name server after the refresh interval (the host could be down), it starts trying to connect every <i>RETRY</i> seconds. Default is 3600.
Expire	If the slave fails to contact the master name server for <i>EXPIRE</i> seconds, the slave expires the zone. Default is 604800.
Negative Cache TTL	TTL stands for “Time to Live”. This value applies to all negative responses from the name servers authoritative for the zone. Default is 86400.
Default TTL	The default Time to Live value. For BIND 8.2 and later, this will be the \$TTL value that is written in the zone file. Default is 86400.
Contact	The contact email address in dotted format. For example, an email address of ‘ root@ins.com ’, would be represented as <code>root.ins.com</code> . This field is auto-populated by the value defined for the “Domain Contact Email” policy in the Policies and Options section of the Tools menu. The auto-populated value may be changed to a custom value, if needed.

Editing a DNS Domain

To modify an existing DNS Domain, follow these steps.

1. Click on the domain name in the DNS Domain List. The Edit DNS Domain screen opens, as shown in Figure 4-24.

Edit DNS Domain: example.com.

DNS Domain

Resource Records

Edit DNS Domain: example.com (External):

Name	example.com
Managed	<input checked="" type="checkbox"/>
Delegated	<input checked="" type="checkbox"/>
Reverse:	<input type="checkbox"/>
Domain Type	External
Derivative	standard
Serial Number:	1
Refresh:	10800
Retry:	3600
Expire:	604800
Negative Cache TTL:	86400
Default TTL:	86400
Contact	dnsadmin.example.com.

Set Information Template

Save

Cancel

Figure 4-24 Edit DNS Domain

2. Choose from the following actions.

To ...	Then ...
Modify values for the currently selected domain	Refer to Table 4-9 on page 139 for information as you make your edits.

To ...	Then ...
Add additional information template data	<ol style="list-style-type: none"> 1. Click Set Information Template. The Set/Remove Information Template opens. <div data-bbox="670 426 1352 777" data-label="Image"> </div> <p>Figure 4-25 Set/Remove Information Template</p> 2. Select one of the information templates to add additional fields to the DNS Domain record. For more information on Information Templates, refer to “Information Templates” on page 318. 3. Click Submit. Extra fields for the selected information template are added to the DNS Domain record.
View and edit the DNS resource records that are associated with the current domain	Click the Resource Records tab, shown in Figure 4-26. For more information on Resource Records, refer to the section below.

Managing Resource Records

About Resource Records and Workflow

When you add or edit a resource record, resource record approval access is checked on the domain for the resource record. If you have the required access, the record is added and is eligible for pushing/deployment. If the required access is not granted to you, then the record is added in a “Pending” approval state. In this state it will need an approval from an administrator with resource record approval access on the given domain to then be eligible for pushing/deployment. The same behavior applies when you try to edit or delete a resource record. In effect, the Pending Action on a resource record may be ‘Create’, ‘Update’, ‘Delete’, or empty. An empty value for Pending Action means that the record has been approved or does not require approval.

In addition to the fields associated with a resource record such as Owner, Class, Type, and so on, this list has two additional fields, as shown in Figure 4-26 and described in Table 4-10.

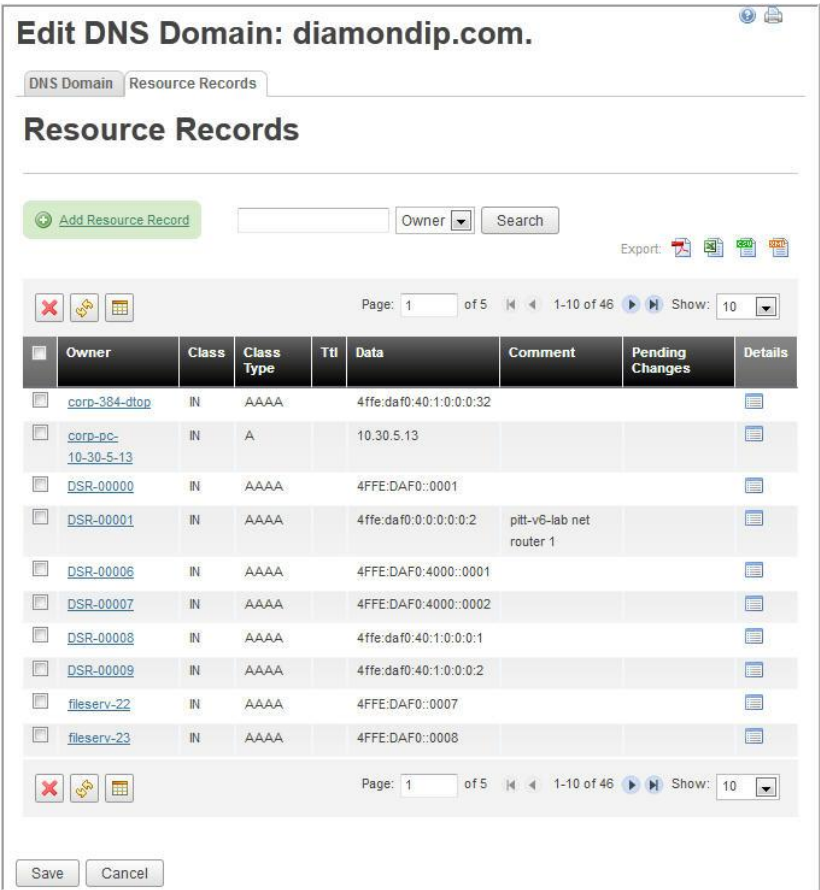


Figure 4-26 Edit DNS Domain – Resource Records Tab

Table 4-10 Resource Records Tab Screen Elements

Field	Description
Pending Changes	<div>This field can have the following values.</div> <ul style="list-style-type: none">• Empty – An empty field indicates this is an approved record.• Create – Creation of a new record is awaiting approval.• Delete – A delete on an existing record is awaiting approval.• Update – An update to an existing record is awaiting approval.

Field	Description
Details	<p>When you click on the Details icon, a pop-up appears with the details regarding the record. The fields in the pop-up include:</p> <p>Last Update time – time of the last update to the record.</p> <p>Admin – login name of the user that last updated the record.</p> <p>Create Source – source of record creation, for example, GUI, API, Host discovery.</p> <p>Update Source – source of last update, for example, GUI, API, Host discovery.</p> <p>Approvers – A list of administrators that are eligible to approve this record. This field is displayed only in the case of a pending record. An administrator needs to have resource record approval access on a given domain to be an approver.</p> <p>To close the pop-up, click the Details icon again.</p>

Adding a Resource Record

You can define a resource record for the current domain. Note that resource records for IP Addresses (devices) can also be generated automatically when IP Addresses are added to the system, by ensuring that the **Create Default DNS Resource Record** checkbox is selected on the device profile.

To add a Resource Record to a domain, follow these steps.

1. Click on the **Add Resource Record** link. The Add Resource Record screen opens.

Add Resource Record

Resource Record Type: A (IPv4 Address Record/Name-to-address)

Auto-Generate Device Record: ☐

Auto-Generate PTR Record: ☐

Owner	TTL	Class	Type	IPv4 Address
		IN	A	

Comment:

Example: localhost IN A 127.0.0.1

Current Record:

Description: Address record (code 1) - The A resource record is used to provide a hostname to IP Address mapping. It is one of the most important resource record types, since it provides the IP address of the host being looked-up. Typically, each host should have an A record unless it is an alias for another host (using the CNAME resource record). It is possible for a host to have multiple A resource records. This is common on routers and other devices with multiple network interfaces and IP addresses. Defined in RFC 1035.

Create Source:

Update Source:

Save Resource Record Cancel

Figure 4-27 Add Resource Record

2. Select the record type from the **Resource Record Type** drop-down.


3. Enter the fields associated with the resource record type, such as Owner, Class, and Data.
4. Click **Save Resource Record** to save your changes, or **Cancel** to return to the previous screen.

Editing a Resource Record

To edit a resource record, follow these steps.

1. Locate the record you want to edit. You can locate a record quickly by entering search criteria and selecting either **Owner** or **RDATA** from the **Search** drop-down.
2. Select the **Owner** link for the resource record you want to edit.
3. Make changes as required. You can change the Resource Record Type, Owner, TTL and RDATA fields.
4. Click **Save Resource Record** to save your changes, or **Cancel** to return to the previous screen.

Deleting a Resource Record

To delete resource records, click on the checkbox next to the items that you want to delete, and click .

Galaxies

A DNS Galaxy is a management technique that can be used to help automate the task of assigning Domains to DNS Servers. The concept is that you may define a group of DNS servers (known as a Galaxy) that includes a master DNS server and one or more slave DNS servers. Once the Galaxy is defined, you may assign Domains directly to a Galaxy, and when the DNS configuration is generated by the system, all DNS servers will include an entry for the domain.

This saves the DNS administrator the step of having to assign the domain to each of the DNS servers individually. If your organization uses a large number of DNS servers, or manages a large number of DNS Domains, this feature helps save considerable administrative effort.

Use this menu item to maintain DNS Galaxies within the system.

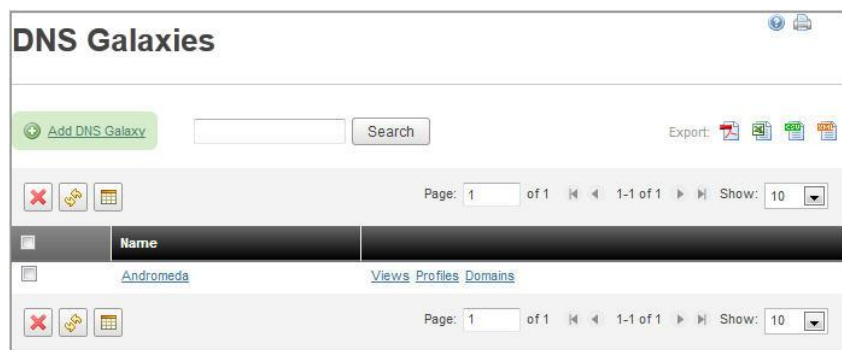


Figure 4-28 DNS Galaxies

To delete one or more DNS Galaxy, click the checkbox in the **Select** column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected domains, or **Cancel** to not delete the selected domains.

Adding a DNS Galaxy

To add a DNS Galaxy, click the **Add DNS Galaxy** link. The Create DNS Galaxy screen appears.

Figure 4-29 Add DNS Galaxy

Table 4-11 Add DNS Galaxy Parameters


Field	Description
Name	Enter a unique name for this Galaxy.
Description	Enter a description for this Galaxy.

Enter the desired attributes once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Editing DNS Views for Galaxy

DNS Views are a mechanism that is very useful in a firewalled environment. Views allow you to present one name server configuration to one community of hosts and a different configuration to another community. This is particularly handy if you are running a name server on a host that receives queries from both internal and external hosts.

To add or modify DNS Views for this Galaxy, click the **Views** option from the DNS Galaxy List. The DNS View List for this Galaxy opens, as shown in Figure 4-30. By default, a DNS

View named **GalaxyDefault** is created for each Galaxy. You can add additional views, and order them accordingly by clicking on the **Up** or **Down** buttons. You can also delete Views from the Galaxy by selecting the View you want to delete and clicking .

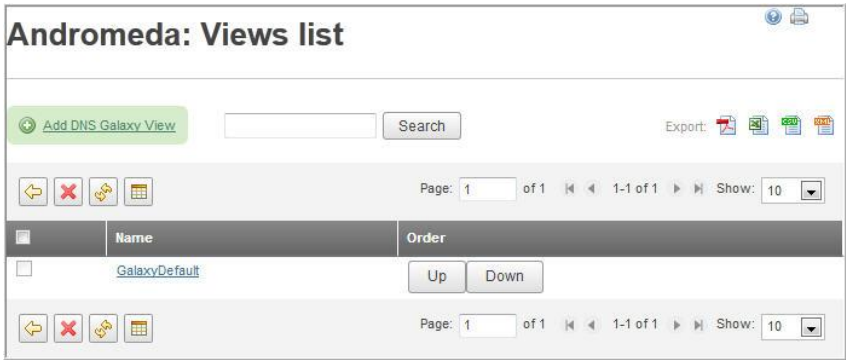


Figure 4-30 DNS View List

Editing DNS Server Profiles for Galaxy

To add or modify the DNS servers that are associated with this Galaxy, click on the **Profiles** option from the DNS Galaxy List. The DNS Profile List for this Galaxy opens, as shown in Figure 4-31. Using this screen, you can add, delete, and modify the list of DNS servers.

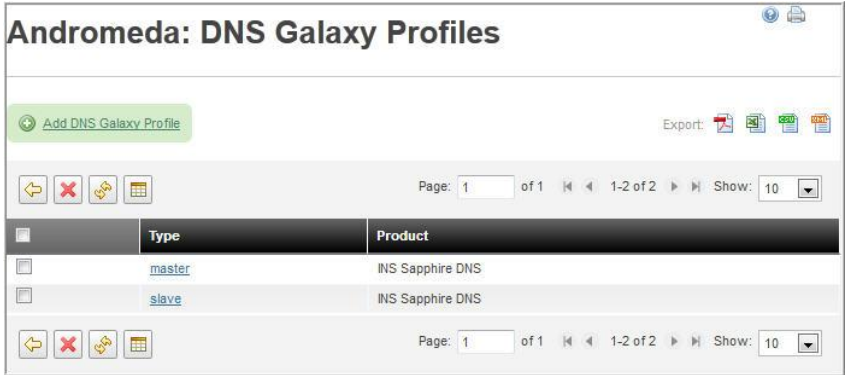


Figure 4-31 Profile List for Selected Galaxy

When you select the **Add DNS Galaxy Profile** option, you can select the DNS server, product, and specify Zone options for these servers. Use this screen to manage the list of Master and Slave Servers for this Galaxy, as well as the zone options that are available for these servers.

Figure 4-32 Add DNS Galaxy Profile

Table 4-12 Add DNS Galaxy Profile Parameters

Field	Description
Type	Select the type of DNS server(s) that you will be adding to this Galaxy.
Masters	Only appears if “slave” or “stub” is selected. Enter the IP addresses of the master DNS servers for this slave/stub, separated by semicolons. Maps to the “masters” option on the zone. For example: 10.0.0.2;10.0.0.6
Product	The DNS product type that you have selected for this group of servers.
Location	Enter the relative directory name of where the zone files for this group of servers will be created on the DNS servers. This “location” ends up as part of the path (appended to the configuration directory). Note: It needs to end with a \ or / or else it becomes part of each zone file name. For example: <code>galaxyslave/</code>
DNS Servers	Select the DNS servers to add to this Galaxy.
Zone Options	Add any zone options that you want to appear associated to this Galaxy for this type of server.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Log Channels

The Log Channels screen allows you to maintain DNS Log Channels. Logging for BIND DNS servers is accomplished with two main concepts: *channels* and *categories*. A channel specifies where logged data goes (that is, syslog, to a file, and so on.). A category specifies

what data is logged. In a BIND-based DNS server, most messages that the name server logs are categorized according to the function of the code they relate to.

This option allows you to define global (system-wide) logging channel definitions that you can use throughout the system.

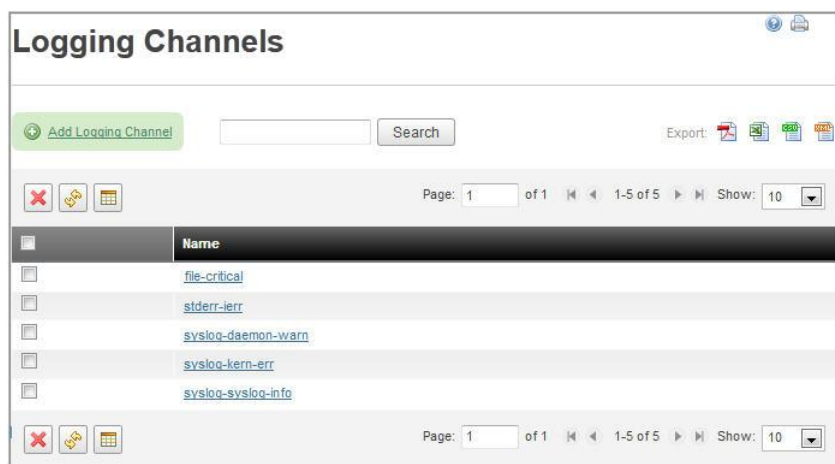


Figure 4-33 Logging Channels

To delete one or more logging channels, select the checkbox beside each item you wish to delete, and click . At the confirmation prompt, click **OK** to delete the selected channels, or **Cancel** to return to the previous screen.

Note: Make sure that the logging channels that you are deleting are not associated with a DNS server.

Adding a Logging Channel

To add a Logging Channel, click the **Add Logging Channel** link. The Add Logging Channel screen appears.

Create Logging Channels

Channel Name:	<input type="text"/>
Output Destination:	Disk File <input type="button" value="v"/>
Syslog Facility:	kern <input type="button" value="v"/>
File Path:	<input type="text"/>
File Versions:	<input type="text"/>
File Size:	<input type="text"/>
Severity:	Critical <input type="button" value="v"/>
Print Category:	Yes <input type="button" value="v"/>
Print Time:	Yes <input type="button" value="v"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Figure 4-34 Create Logging Channels

Table 4-13 Create Logging Channels Parameters

Field	Description
Channel Name	Enter a unique name for the Logging Channel.
Output Destination	Select the destination where you want to send the log output: <ul style="list-style-type: none"> • Disk File – A disk based file(s) • System Log (syslog) – The system Log • Standard Error Output (stderr) – Stderr as defined by the DNS server. • Null – Nowhere. Messages sent to this channel will be discarded.
Syslog Facility	This option is only applicable if you have selected “System Log (syslog)” as the Output Destination. Select the appropriate syslog facility based on your operating system and configuration.
File Path	This option is only applicable if you have selected “Disk File” as the Output Destination. Enter the fully qualified path and file name that will receive the log information. Example “file.msgs”
File Versions	This option is only applicable if you have selected “Disk File” as the Output Destination. Enter the number of versions of the file to keep at any point in time. For example, if you specify “3” as the File Versions, and “file” as the File Path, each time the server is stopped and restarted, it will copy the current version to a backup copy. It will increment a number and append that number to the file name of the backup file(s). Over time, you will end up with file, file.0, file.1, and file.3.

Field	Description
File Size	<p>This option is only applicable if you have selected “Disk File” as the Output Destination.</p> <p>Specifies the maximum file size of the log channel. The name server will stop writing to this channel if the maximum size is reached. You can enter the size of the file using a scaling factor such as “k” to indicate kilobytes, and “m” to indicate megabytes, or “g” to indicate gigabytes of the file.</p> <p>For Example; “10k” – 10 kilobyte file size limit, “10m” = 10 megabyte file size limit</p>
Severity	<p>Channels allow you to filter messages based on severity. Use this option to specify what severity of message will be hosted by this channel. Here is a list of the supported severities sorted by most severe to least severe:</p> <ul style="list-style-type: none"> • Critical • Error • Warning • Notice • Info • Debug (note: only level 1 is currently supported)
Print Category	If Yes, the Category of the message is printed within the log message.
Print Time	If Yes, the date/time of the message is printed within the log message.

Enter the desired attributes and click **Submit** to save your changes, or **Cancel** to return to the Logging Channels screen.

Editing a Logging Channel

To modify an existing logging channel, click on the channel name in the Logging Channel List. The Edit Logging Channel screen opens.

Edit the logging channel as needed. Once finished, click **Submit** to save your changes, or **Cancel** to return to the Logging Channels screen.

Server Templates

Use the DNS Server Templates screen to maintain Domain Name Server (DNS) definition templates. These templates allow you to standardize the definitions that are used to create similar DNS servers. When you create new DNS servers, you may alternately create them using one of the defined DNS Server Templates. This allows you to standardize on complex configuration settings, and apply them to servers in a “cookie cutter” manner.

Managing Server Templates

To work with DNS Server Templates, follow these steps.

1. Select **Server Templates** from the DNS section of the **Management** menu. The DNS Server Templates list appears, as shown in Figure 4-35.

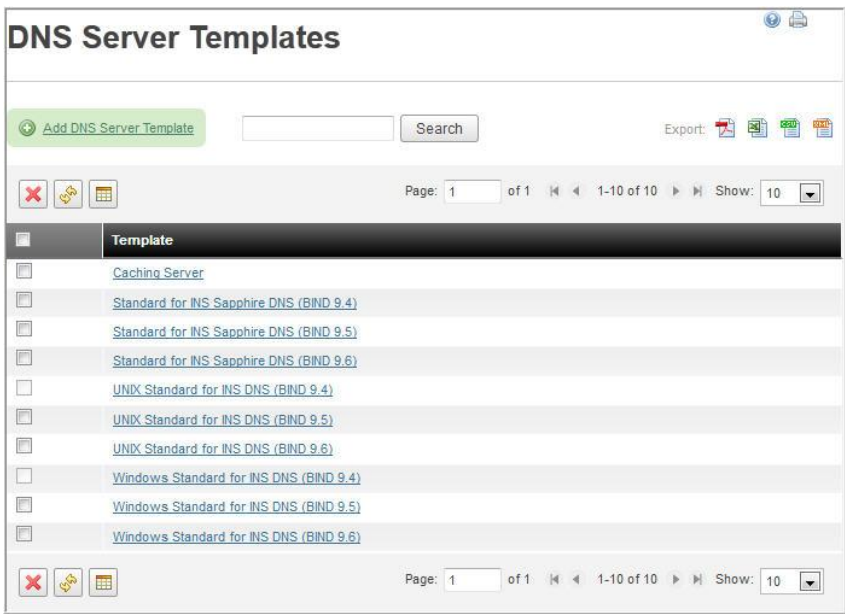



Figure 4-35 DNS Server Templates

2. Choose from the following actions.

To ...	Then ...
Search for a specific server template	<ol style="list-style-type: none">1. Enter a search string in the text block.2. Click Search. The list of server templates changes to match the search string.
Define a new server template	Refer to “Adding a DNS Server Template” following.
Modify an existing server template	<ol style="list-style-type: none">1. Select the template name in the Template list that you want to modify. The Edit DNS Server Template screen opens, with an additional tab for Logging, as shown in Figure 4-41 on page 159.2. Edit the DNS Server template fields and tabs as needed. Refer to the following sections for more information on fields and tabs.

To ...	Then ...
Delete one or more server templates	<ol style="list-style-type: none">1. Select the checkbox beside each item you wish to delete.2. Click .3. At the confirmation prompt, click OK to delete the selected server templates, or Cancel to return to the previous screen.

3. Once you have finished working with a DNS Server Template, click **Submit** to save it, or click **Cancel** to return to the previous screen.

Adding a DNS Server Template

To add a new DNS Server Template, follow these steps.

1. Click the **Add DNS Server Template** link. The Add DNS Server Template screen appears.

Add DNS Server Template

General

Extensions

Root Hints File

Advanced

Options

Template Name:

Create db.127.0.0 Loopback Address File:

☐

Configuration Directory:

Data Directory:

Product:

CNR DNS

Start Script:

Stop Script:

Configuration File Check Script:

Zone File Check Script:

Submit

Cancel

Figure 4-36 Add DNS Server Template

General Tab

2. Type values in the **General** tab, as described in Table 4-14.

Table 4-14 Add DNS Server Template Parameters

Field	Description
Template Name	The name of the DNS Server Template. This name appears in a select list when you are creating DNS Servers.
Create localhost – Create the Loopback Address db.127.0.0 file.	If this option is checked, the system automatically creates the db.127.0.0 loopback address file. Name servers need this file to be sure that they can resolve localhost correctly.

Field	Description
Configuration Directory	The directory of where the DNS configuration file “named.conf” is created.
Data Directory	The directory of where the DNS data files (that is, zone files) are created.
Product	Select the DNS Server product from the list. This controls the options that are available within this template.
Start Script	The script that is executed by the IPControl Agent to start the DNS server.
Stop Script	The script that is executed by the IPControl Agent to stop the DNS server.
Configuration File Check Script	The script that is executed to verify the Configuration File.
Zone File Check Script	The script that is executed to verify the Zone File.

Extensions Tab

- Click on the **Extensions** tab to display the configuration file extensions area. The extensions area allows you to create free form text that is added to the beginning or the end of the *named.conf* configuration file.

Figure 4-37 DNS Server Template Extensions

- Type text as needed in the **Start of Named.conf** and **End of Named.conf** text areas, as described in Table 4-15.

Table 4-15 DNS Server Template Extensions Parameters

Field	Description
Start of named.conf	A free text area that appears at the beginning of the <i>named.conf</i> file when the file is automatically generated. Note: The extensions are limited to 32000 characters.
End of named.conf	A free text area that appears at the end of the <i>named.conf</i> file when the file is automatically generated. Note: The extensions are limited to 32000 characters.

Root Hints Tab

- Click on the **Root Hints** tab to display the configuration of the Root Hints file, as shown in Figure 4-38. The Root Hints file tells the DNS server where the name servers for the root zone are located.

Add DNS Server Template

General Extensions **Root Hints File** Advanced Options

Create Root Hints File: ☒

Contents of the Root Hints File:

☒ Use Standard InterNIC supplied content (recommended)
☐ Use Custom Root Hints file (edit below)

This file holds the information on root name servers needed to initialize cache of Internet domain name servers (e.g. reference this file in the "cache . <file>" configuration file of BIND domain name servers).
 This file is made available by InterNIC.

Submit Cancel

Figure 4-38 Root Hints File

- Select the Create Root Hints File check box, if required. Refer to Table 4-16 for more information.

Table 4-16 Root Hints Parameters

Field	Description
Create Root Hints File	Check this item on if you want to automatically create the "Root Hints" file when generating the DNS Configuration files.
Use Standard InterNIC supplied content	Only valid if you have checked the "Create Root Hints" file option. Select this option if you would like to use the InterNIC supplied content when generating this file.
Use Custom Root Hints file	Only valid if you have checked the "Create Root Hints" file option. Select this option if you would like to use custom content that you enter for the Roots Hints file.

Advanced Tab

- Click on the **Advanced** tab to display the advanced options that are available, as shown in Figure 4-39. These options include configuration of the "controls" section of the configuration file.

Traditionally, DNS administrators have controlled the BIND DNS server with UNIX signals. The DNS server interprets the receipt of certain signals as an instruction to take a particular action, such as reloading zones that have changed. Because there are a limited number of signals, BIND has introduced a method of controlling the name server by sending messages to it on a special control channel. The control channel can be either a UNIX socket, or a TCP port the name server listens on for messages.

Figure 4-39 Advanced Tab

8. Type values in the Advanced tab fields, as described in Table 4-17.

Table 4-17 Advanced Tab Parameters

Field	Description
TCP Port Control Channel Settings:	Select this option to send messages to the name server via a TCP/IP Port.
Listen on IP Address	Enter the IP Address for the name server to listen on for messages.
Listen on Port	Enter the Port that the name server will listen on for messages. Typically, this is port 953.
Allow Message From	Enter an IP Address, or the name of an Address Match List that specifies where messages are allowed to come from.
Keys (Used by rndc)	Select the key to be used by rndc.
UNIX Domain Socket Channel Settings:	Select this option to send messages to the name server via a UNIX Domain Socket.
UNIX Domain Socket	Enter the name of the socket that will be used for communicating with the name server. Typically this is <code>/var/run/ndc</code> , though some operating systems use a different pathname. The socket is usually owned by root and readable and writable only by the owner.
Permissions (octal)	The permission value must be specified as an Octal quantity (with a leading zero to indicate an octal quantity). For example; 0660.
Owner	Enter the Owner identifier.
Group	Enter the Group identifier.

Options Tab

9. Click on the **Options** tab to display the options and directives that are available. The options that are displayed are dependent upon the Product Selected, as well as the items configured in the Vendor Option Dictionary.

To view all available options for this product, click on **Show All Product Options**. All options that have been configured for the product selected (on the **General** tab) are displayed, as shown (partially) in Figure 4-40.

10. Configure each option that you want to appear in the *named.conf* configuration file.

Add DNS Server Template

General Extensions Root Hints File Advanced Options

☒ Show All Product Options

Enabled	Option	Value
<input type="checkbox"/>	Additional cache cleaning interval	<input type="text"/>
<input type="checkbox"/>	Additional cache enable	<input type="radio"/> Yes <input type="radio"/> No
<input type="checkbox"/>	Additional from auth	<input type="radio"/> Yes <input type="radio"/> No
<input type="checkbox"/>	Additional from cache	<input type="radio"/> Yes <input type="radio"/> No
<input type="checkbox"/>	Allow notify	<input type="text"/> Address List
<input type="checkbox"/>	Allow query	<input type="text"/> Address List
<input type="checkbox"/>	Allow query cache	<input type="text"/> Address List
<input type="checkbox"/>	Allow query cache on	<input type="text"/> Address List
<input type="checkbox"/>	Allow query on	<input type="text"/> Address List
<input type="checkbox"/>	Allow recursion	<input type="text"/> Address List
<input type="checkbox"/>	Allow recursion on	<input type="text"/> Address List
<input type="checkbox"/>	Allow transfer	<input type="text"/> Address List
<input type="checkbox"/>	Allow update forwarding	<input type="text"/> Address List
<input type="checkbox"/>	Allow v6 synthesis	<input type="text"/> Address List
<input type="checkbox"/>	Also notify	Edit

...

<input type="checkbox"/>	Transfers in	<input type="text"/>
<input type="checkbox"/>	Transfers out	<input type="text"/>
<input type="checkbox"/>	Transfers per name server	<input type="text"/>
<input type="checkbox"/>	Treat CR as space	<input type="radio"/> Yes <input type="radio"/> No
<input type="checkbox"/>	Try TCP refresh	<input type="radio"/> Yes <input type="radio"/> No
<input type="checkbox"/>	Use ID pool	<input type="radio"/> Yes <input type="radio"/> No
<input type="checkbox"/>	Use alternate transfer source	<input type="radio"/> Yes <input type="radio"/> No
<input type="checkbox"/>	Use query port pool	<input type="radio"/> Yes <input type="radio"/> No
<input type="checkbox"/>	Use v4 UDP ports	Edit
<input type="checkbox"/>	Use v6 UDP ports	Edit
<input type="checkbox"/>	Version	<input type="text"/>
<input type="checkbox"/>	Zero no SOA TTL	<input type="radio"/> Yes <input type="radio"/> No
<input type="checkbox"/>	Zero no SOA TTL cache	<input type="radio"/> Yes <input type="radio"/> No
<input type="checkbox"/>	Zone stats	<input type="radio"/> Yes <input type="radio"/> No

Submit Cancel

Figure 4-40 Options Tab

Logging Tab

The Logging tab only appears when you modify a server template, as shown in Figure 4-41.

Categories	Channels
<input type="checkbox"/> EDNS Disabled	Choose
<input type="checkbox"/> Query Errors	Choose
<input type="checkbox"/> Default	Choose
<input type="checkbox"/> Dispatch	Choose
<input type="checkbox"/> Delegation Only	Choose
<input type="checkbox"/> Lame Servers	Choose
<input type="checkbox"/> Notify	Choose
<input type="checkbox"/> Queries	Choose
<input type="checkbox"/> Security	Choose
<input type="checkbox"/> Inbound Zone Transfers	Choose
<input type="checkbox"/> Dynamic Updates	Choose
<input type="checkbox"/> General	Choose
<input type="checkbox"/> Outbound Zone Transfers	Choose
<input type="checkbox"/> Configuration	Choose
<input type="checkbox"/> Client	Choose
<input type="checkbox"/> Network	Choose
<input type="checkbox"/> DNSSEC	Choose
<input type="checkbox"/> Database	Choose
<input type="checkbox"/> Resolver	Choose
<input type="checkbox"/> Update Security	Choose
<input type="checkbox"/> Unmatched	Choose

Submit Cancel

Figure 4-41 Logging Tab

This option allows you to select logging channels for each category that is defined for the server. To add a channel to a category, follow these steps.

1. Click the **Choose** button next to the category you have selected. The Logging Channels screen opens.

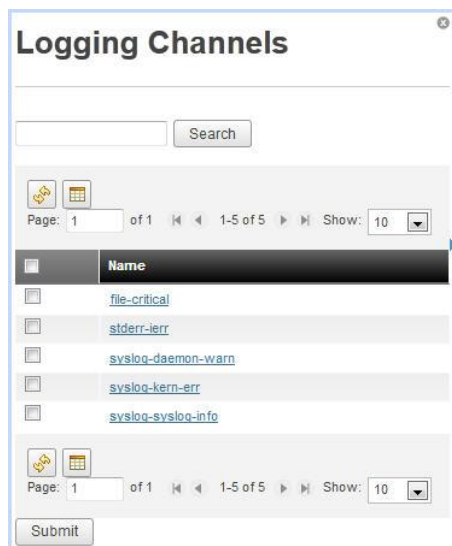


Figure 4-42 Select Logging Channels

2. Select the channels you want.
3. Click **Submit**. The channels you selected appear beside the category you selected in Step 1.

DNS Domain Types

The DNS Domain Types screen allows you to categorize DNS Domain by type. Domain Types allow you to distinguish between domains that are used within your system. For example, if you are using the same domain name more than once within your system, you would place each domain in a different DNS Domain Type. For example, `example.com` can be defined twice: once using a Domain Type of “Internal” and once using a Domain Type of “External”.

Managing DNS Domain Types

To work with DNS Domain Types, follow these steps.

1. Select **Domain Types** from the DNS section of the **Management** menu. The DNS Domain Types screen opens, as shown in Figure 4-43.

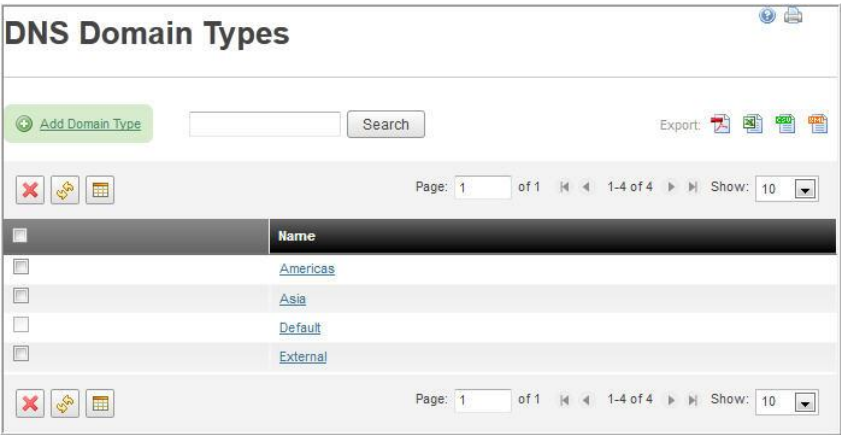



Figure 4-43 DNS Domain Types

2. Choose from the following actions.

To ...	Then ...
Search for a particular DNS Domain Type	<ol style="list-style-type: none">1. Enter a search string in the text block.2. Click Search. The list of domains changes to match the search string.
Add a DNS Domain Type	<ol style="list-style-type: none">1. Click the Add Domain Type link. The Add Domain Type screen appears.<div data-bbox="531 1094 1351 1348"><div>Add DNS Domain Type</div><div></div><div>Name: <input type="text"/></div><div><input type="button" value="Submit"/> <input type="button" value="Cancel"/></div></div>
Edit a DNS Domain Type	<ol style="list-style-type: none">1. Click on the domain type in the Name list. The Edit DNS Domain Type screen opens.2. Edit the Name as needed.
Delete one or more DNS Domains Types	<ol style="list-style-type: none">1. Select the checkbox beside each item you want to delete.2. Click .3. At the confirmation prompt, click OK to delete the selected Domain Types, or Cancel to return to the previous screen.

3. Click **Submit** to add the Domain Type, or **Cancel** to return to the previous screen.

Address Match Lists

Use the Address Match List screen to maintain Access Control Lists (ACLs). Domain Name Servers (DNS) use address match lists for nearly every security feature and even for some features that are not security-related at all. An Address Match List is a list of terms that specifies one or more IP addresses. The elements in the list can be individual IP addresses, IP Prefixes, or a named address match list.

IP prefixes have the format of (Network in dotted-octet format/bits in net mask). For example, 15.0.0.0 with a network mask of 255.0.0.0 can be represented as 15/8.

A named address match list is just that, a list of IP Addresses, IP Prefixes, and/or other named address match lists that have been associated with a name. For example; “my internal servers” name list could contain (15/8, 10.1.1.20, and 10.2.1.21).

Managing Address Match Lists

To maintain global Address Match Lists that can be used in various points within the system, follow these steps.

1. Select **Address Match Lists** from the DNS section of the **Management** menu. The Address Match List screen opens, as shown in Figure 4-45.

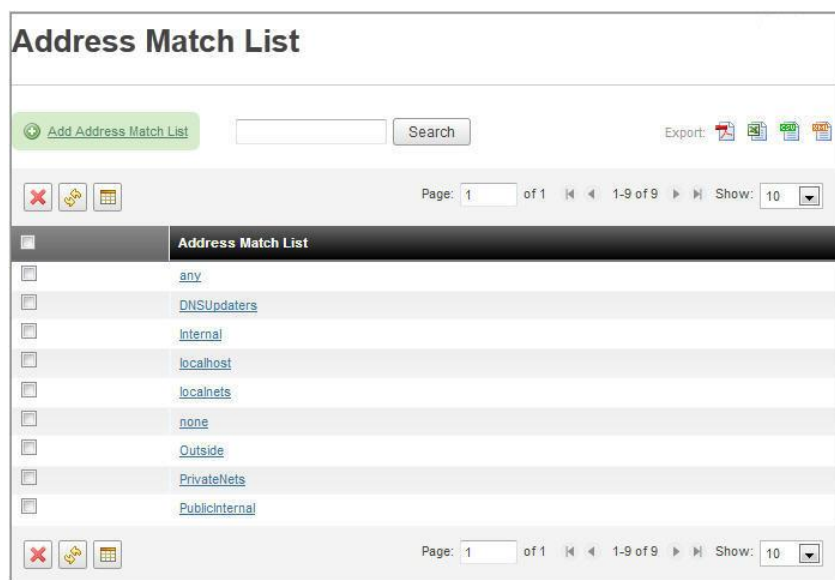



Figure 4-45 Address Match List

2. Choose from the following actions.

To ...	Then ...
Search for a specific Address Match List	<ol style="list-style-type: none"> 1. Enter a search string in the text block. 2. Click Search. The Address Match list changes to match the search string.

To ...	Then ...
Add an Address Match List	Refer to “Adding an Address Match List” following.
Edit an Address Match List	Refer to “Editing an Address Match List” on page 164.
Delete one or more an Address Match Lists	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Address Match Lists, or Cancel to return to the previous screen.

3. Click **Submit** to add the new or modified Address Match List, or **Cancel** to return to the previous screen.

Adding an Address Match List

To add a new Address Match List, follow these steps.

1. Click the **Add Address Match List** link. The Add Address Match List screen opens, as shown in Figure 4-46.

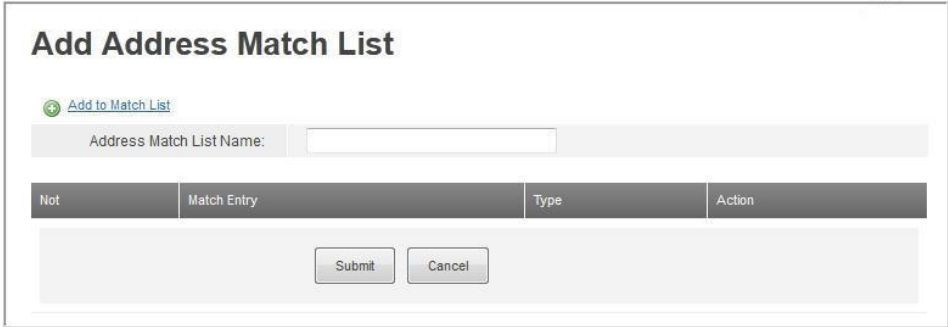


Figure 4-46 Add Address Match List

2. In the **Address Match List Name** field, enter a name for this address match list. This name is displayed in drop-down lists when you are defining options.
3. Click on **Add to Match List** to add actual values. The Add Address Match Entry screen opens, as shown in Figure 4-47.

Figure 4-47 Add Address Match Entry

- Enter values in the fields, as described in Table 4-18.

Table 4-18 Add Address Match Entry Parameters

Field	Description
IP Address	To add a single IP Address to the match list, click on the radio button next to IP Address , and then enter the IP Address. Note: You can use the exclamation mark “!” to create an exclusion, such as “!10.0.0.1”.
Address Match List	An address match list may contain references to other (previously created) match lists. To add another match list reference to the current match list, click on “Address Match List”, and select the match list you wish to add.
TSIG Key	To add a TSIG Key to the match list, click on the radio button next to TSIG Key , and then select the TSIG Key you wish to add.
Net Service	To add a Net service to the match list, click on the radio button next to Net Service , and then select the Net Service you wish to add.
Negate This Match	You can negate the query options selected by the radio buttons on this screen. To do this, check the Negate This Match checkbox. For example, if the TSIG Key “rndc-key.” is selected and the TSIG Key radio button is active, checking the Negate This Match checkbox includes all TSIG Keys <i>except</i> “rndc-key.”

- Once you have completed entering the Address Match List Name and Match List, click **Submit** to create the match list, or **Cancel** to return to the previous screen.


Editing an Address Match List

To modify an existing Address Match List, follow these steps.

- Select the match list name in the **Address Match List** that you want to modify. The Edit Address Match List screen opens, as shown in Figure 4-48.

Edit Address Match List

Match List: Internal

 [Add to Match List](#)

Address Match List Name:

Internal

Not	Match Entry	Type	Action
	PrivateNets	Address Match List	<div>UpDownDelete</div>
	PublicInternal	Address Match List	<div>UpDownDelete</div>

Submit

Cancel

Figure 4-48 Edit Address Match List

2. Choose from the following actions.

To ...	Then ...
Change the order of how match lists are written to the configuration file	Click the Up button to move the match entry up or click the Down button to move the match entry down.
Add to an Address Match List	Click on Add to Match List to add actual values. The Add Address Match Entry screen opens, as shown in Figure 4-47 on page 164.
Edit a Match Entry	<div>1. Select the item in the Match Entry list you want to edit. The Edit Address Match Entry screen opens.</div> <div>2. Make changes to the values, as described in Table 4-18 on page 164.</div> <div>3. Click Submit.</div>
Remove a Match Entry	Click the Delete button for each entry you want to remove.

3. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Transaction Keys

The Transaction Keys screen allows you to define system wide global Keys, and use these throughout the system to provide DNS security. The keys that are defined within this option can be used to help secure the following:

- Dynamic DNS updates from the INS DHCP server to an INS or BIND DNS Server.
- Dynamic DNS updates from the ISC DHCP server to an INS or BIND DNS Server.

The Transaction Keys are used to sign DNS messages with a Transaction Signature (TSIG).

Managing Transaction Keys

To work with Transaction Keys, follow these steps.

1. Select Transaction Keys from the DNS section of the Management menu. The Transaction Keys screen opens, as shown in Figure 4-49.

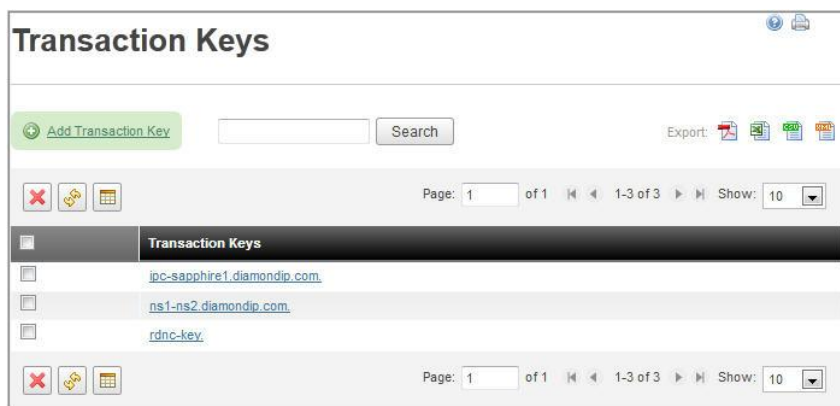



Figure 4-49 Transaction Keys

2. Choose from the following actions.

To ...	Then ...
Search for a specific Transaction Key	<ol style="list-style-type: none"> 1. Enter a search string in the text block. 2. Click Search. The Transaction Key list changes to match the search string.
Add a Transaction Key	Refer to “Adding a Transaction Key” following.
Edit a Transaction Key	<ol style="list-style-type: none"> 1. Click on the Key name in the Transaction Keys list. The Edit Transaction Key screen opens. 2. Edit the key as needed. Refer to Table 4-19 for information on the fields.
Delete a Transaction Key	<p>Note: Make sure that the keys that you are deleting are not associated with a DNS server.</p> <ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Transaction Keys, or Cancel to return to the previous screen.

- Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Adding a Transaction Key

To add a Transaction Key, follow these steps.

- In the Transaction Keys screen, click the **Add Transaction Key** link. The Add Transaction Key screen appears, as shown in Figure 4-50.

Figure 4-50 Add Transaction Key

- Type values in the fields, as described in Table 4-19.

Table 4-19 Add Transaction Key Parameters

Field	Description
Key Name	Enter a unique name for the Transaction Key. From a syntax perspective, it must have the same naming rules as a fully qualified domain name, including the trailing dot. Example: tkey1.ins.com.
Key Algorithm	Select the key algorithm to be used for this key: HMAC-MD5 – one way hash function variant of MD5.
Secret	Shared secret that is used to sign the transactions when using this key. This is a base 64 encoded value. You can use the Generate button to automatically generate a base 64 secret. If you choose your own secret, you must put in the base 64 equivalent of the secret.
Confirm Secret	Confirm the shared secret.
Unmask Secret	Unchecked indicates that the Secret and Confirm Secret fields are masked. Checked indicates that the Secret and Confirm Secret fields are not masked and you can see the secrets on the screen. You can use this option to cut and paste secrets.
Generate a Secret	Use the Generate button to generate a random secret in base 64 encoding. Select the number of Bits to use to generate the key.

DNS Option Vendor Dictionary

Use the DNS Option Vendor Dictionary screen to maintain DNS Vendor Options within the system. Vendor Options are DNS options that are specific to a vendor or type of DNS server. This menu item allows you to select a set of options (from the DNS Master Option List) that are available for use with a specific type of DNS server. In addition, the syntax for this option is (as written to the configuration file) is specified using this menu item as well.

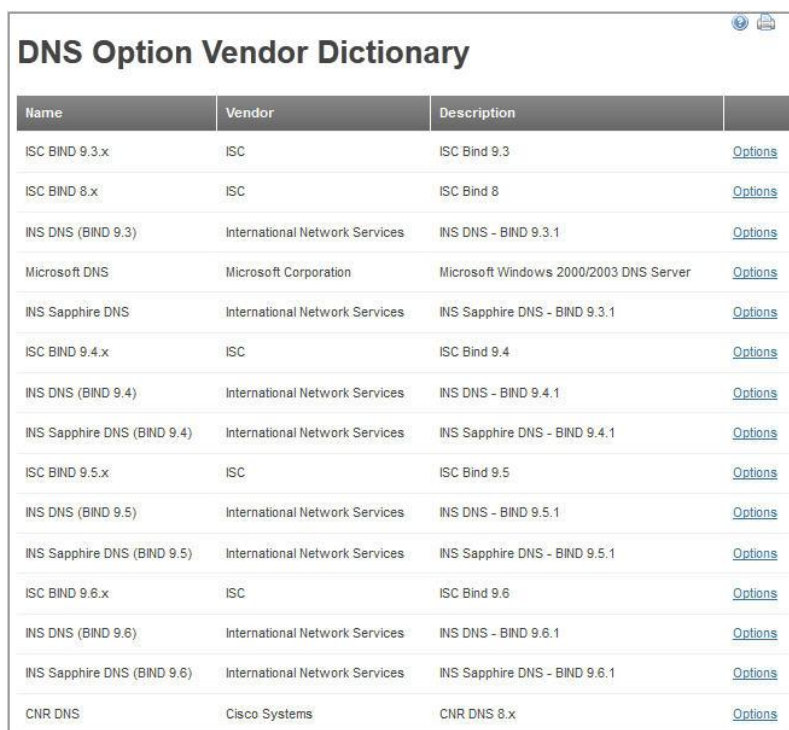
When you access the DNS Option Vendor Dictionary screen, the existing DNS Products are shown. You can add, modify, and delete DNS Products can be added, modified, or deleted, using **DNS Software Products** on the Management menu.

Managing DNS Option Vendor Dictionaries

Check with BT Diamond IP to obtain standard dictionary updates. This section should only be used to customize standard dictionary entries, if needed.

To work with DNS Option Vendor Dictionaries, follow these steps.

1. Select **DNS Option Vendor Dictionary** from the DNS section of the **Management** menu. The DNS Option Vendor Dictionary screen opens, as shown in Figure 4-51.



Name	Vendor	Description	
ISC BIND 9.3.x	ISC	ISC Bind 9.3	Options
ISC BIND 8.x	ISC	ISC Bind 8	Options
INS DNS (BIND 9.3)	International Network Services	INS DNS - BIND 9.3.1	Options
Microsoft DNS	Microsoft Corporation	Microsoft Windows 2000/2003 DNS Server	Options
INS Sapphire DNS	International Network Services	INS Sapphire DNS - BIND 9.3.1	Options
ISC BIND 9.4.x	ISC	ISC Bind 9.4	Options
INS DNS (BIND 9.4)	International Network Services	INS DNS - BIND 9.4.1	Options
INS Sapphire DNS (BIND 9.4)	International Network Services	INS Sapphire DNS - BIND 9.4.1	Options
ISC BIND 9.5.x	ISC	ISC Bind 9.5	Options
INS DNS (BIND 9.5)	International Network Services	INS DNS - BIND 9.5.1	Options
INS Sapphire DNS (BIND 9.5)	International Network Services	INS Sapphire DNS - BIND 9.5.1	Options
ISC BIND 9.6.x	ISC	ISC Bind 9.6	Options
INS DNS (BIND 9.6)	International Network Services	INS DNS - BIND 9.6.1	Options
INS Sapphire DNS (BIND 9.6)	International Network Services	INS Sapphire DNS - BIND 9.6.1	Options
CNR DNS	Cisco Systems	CNR DNS 8.x	Options

Figure 4-51 DNS Option Vendor Dictionary

2. To modify the options associated with a DNS Product, click the **Options** link next to the DNS product that you want to change. The DNS Options for <DNS Product> screen opens, as shown in Figure 4-52.

DNS Options for INS DNS (BIND 9.6)								
<input checked="" type="checkbox"/> Show all options								
Enabled	Name	Option Applies To						Option Syntax
		Options	View	Zone Master	Zone Slave	Zone Stub	Zone Forward	
<input checked="" type="checkbox"/>	Additional cache cleaning interval	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	acache-cleaning-interval integer ;
<input checked="" type="checkbox"/>	Additional cache enable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	acache-enable boolean ;
<input checked="" type="checkbox"/>	Additional from auth	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	additional-from-auth boolean ;
<input checked="" type="checkbox"/>	Additional from cache	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	additional-from-cache boolean ;
<input checked="" type="checkbox"/>	Allow notify	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	allow-notify { address_match_list ; ... };
<input checked="" type="checkbox"/>	Allow query	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allow-query { address_match_list ; ... };
<input checked="" type="checkbox"/>	Allow query cache	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	allow-query-cache { address_match_list ; ... };
<input checked="" type="checkbox"/>	Allow query cache on	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	allow-query-cache-on { address_match_list ; ... };
<input checked="" type="checkbox"/>	Allow query on	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allow-query-on { address_match_list ; ... };

Figure 4-52 DNS Options for INS (partial)

3. Choose from the following actions.

To ...	Then ...
Change the parameters for an enabled option	Refer to Table 4-20 as you decide which option to apply.
Add a new option to the product	<ol style="list-style-type: none">1. Select the Show all options checkbox. All the options in the system are displayed.2. Select the Enabled checkbox beside the option you want to add.3. Select the appropriate checkboxes in the Option Applies To section, as described in Table 4-20.
Edit the syntax for an enabled option	Refer to “Editing Syntax for DNS Options” on page 170.

To ...	Then ...
Remove an option from a DNS product	Uncheck the Enabled checkbox next to the option that you wish to remove from this option set.

- Once finished, click **Save** to save your changes, or **Cancel** to return to the previous screen.

Table 4-20 DNS Options for Bind 9.x Parameters

Field	Description
Enabled	When this box is checked, it indicates that this DNS Option is enabled for this DNS Product.
Name	The name of the DNS Option.
Option Applies To:	
Options	If this box is checked, it indicates that this option can be used when defining an “options” statement within the “named.conf” file.
View	If this box is checked, it indicates that this option can be used when defining a “view” statement within the “named.conf” file.
Zone Master	If this box is checked, it indicates that this option can be used when defining a “zone” statement within the “named.conf” file for a zone type of “master”.
Zone Slave	If this box is checked, it indicates that this option can be used when defining a “zone” statement within the “named.conf” file for a zone type of “slave”.
Zone Stub	If this box is checked, it indicates that this option can be used when defining a “zone” statement within the “named.conf” file for a zone type of “stub”.
Zone Forward	If this box is checked, it indicates that this option can be used when defining a “zone” statement within the “named.conf” file for a zone type of “forward”.
Option Syntax	Shows a sample of the syntax that is used when writing this option to the DNS configuration file. You can edit the syntax by clicking on the option Name link. For more information, refer to “Editing Syntax for DNS Options” following.

Editing Syntax for DNS Options

To edit the syntax for an option, follow these steps.

- Click on the option name in the **Name** column. The Edit DNS Dictionary Option screen opens, as shown in Figure 4-53.

Edit DNS Dictionary Option

Option Title	Allow query		
Description	Defines a match list e.g. IP address(es) which are allowed to issue queries to the server.		
Tag	<input type="text" value="allow-query {"/>	<div>Example: <pre>allow-query { address_match_list; ... };</pre></div>	
Suffix	<input type="text" value="};"/>		
Repeatable	<input type="checkbox"/>		

Add new Option Clause

Clause	Repeatable	
address_match_list : ...	<input type="checkbox"/>	<div><div>Delete</div><div>Up</div><div>Down</div></div>

Submit

Cancel

Figure 4-53 Edit DNS Dictionary Options

2. Use this screen to model the syntax for this DNS option, and click **Submit** to save your changes, or click **Cancel** to return to the list.

DNS Option Master Dictionary

Use the DNS Option Master Dictionary screen to maintain DNS Master Options within the system. Master Options are predefined with all available options that are normally configured with a BIND 8.x or a BIND 9.x server, but may be modified for your environment.

In addition, you can add your own options if they are not already defined within the system.

Managing the DNS Option Master Dictionary

To work with the DNS Option Master Dictionary, follow these steps.

1. Select **Option Master Dictionary** from the DNS section of the **Management** menu. The DNS Option Master Dictionary screen opens, as shown in Figure 4-54.

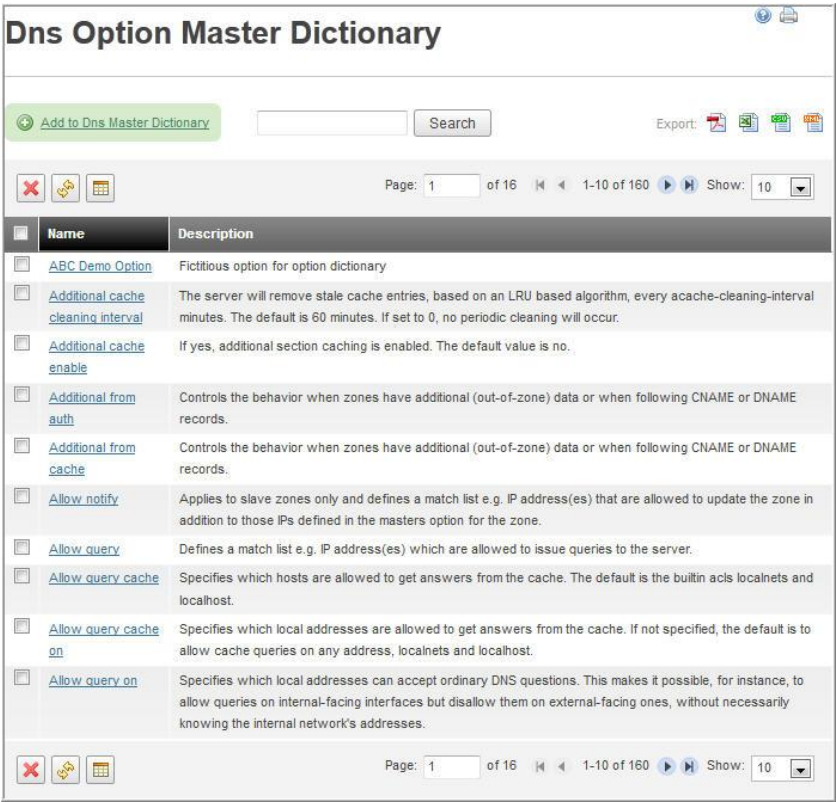




Figure 4-54 DNS Option Master Dictionary

2. Choose from the following actions.

To ...	Then ...
Search for a specific string	<ol style="list-style-type: none">1. Enter a search string in the text block.2. Click Search. The Name list changes to match the contents of the search string.

To ...	Then ...
Add a Master DNS Option	<ol style="list-style-type: none"> 1. Select the Add to DNS Master Dictionary link. The Add Master DNS Option screen appears.  <ol style="list-style-type: none"> 2. Enter a name and optional description in the Name and Description fields.
Edit a Master DNS Option	<ol style="list-style-type: none"> 1. Click on the Option name in the Name list. The Edit Master DNS Option screen opens. 2. Edit the name and description as needed.
Delete a Master DNS Option	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Options, or Cancel to return to the previous screen.

3. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

DNS Software Products

Use the DNS Software Products screen to define DNS products and the attributes that are associated with them.

A set of pre-defined products are included with the system. These products include all the definitions, options, and business logic that are needed to properly manage these network services. Additional products may be added to the system, as long as these newer products are derived from existing product definitions (that is, they share the same attributes, and so on).

Managing DNS Software Products

To work with a DNS Software Product, follow these steps.

1. Select **DNS Software Products** from the DNS section of the **Management** menu. The DNS Software Products screen opens, as shown in Figure 4-56.

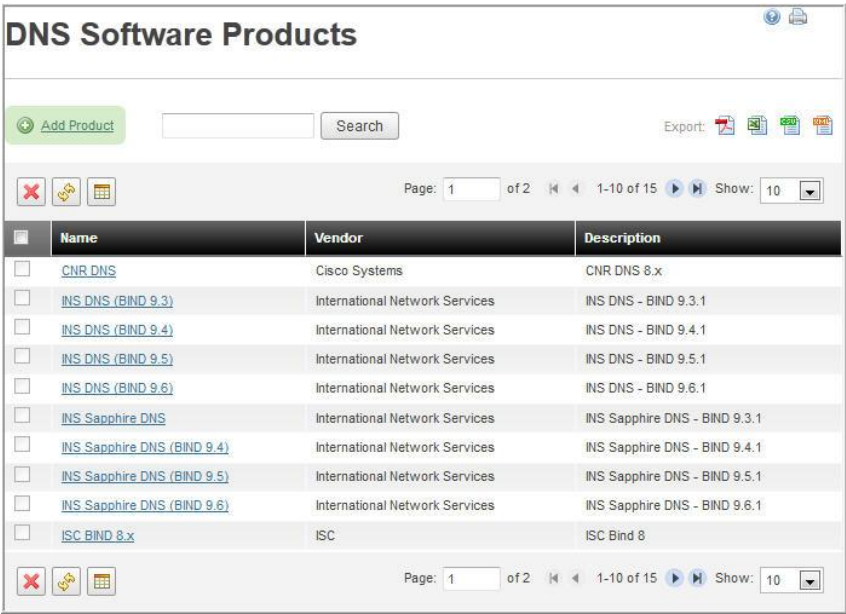



Figure 4-56 DNS Software Product List

2. Choose from the following actions.

To ...	Then ...
Search for a specific Product string	<ol style="list-style-type: none">1. Enter a search string in the text block.2. Click Search. The Name list changes to match the contents of the search string.
Add a Product	Refer to “Adding a Software Product” following.
Edit a DNS Software Product	<ol style="list-style-type: none">1. Click on the Product name in the Name list. The Edit Product screen opens.2. Edit the values as needed. Refer to Table 4-21 on page 175.
Delete a DNS Software Product	<p>Note: Make sure that this Product is not assigned to any DNS Server (Network Service) before you delete it.</p> <ol style="list-style-type: none">1. Select the checkbox beside each item you want to delete.2. Click .3. At the confirmation prompt, click OK to delete the selected Products, or Cancel to return to the previous screen.

3. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Adding a Software Product

To add a software product, follow these steps.

1. Click on the **Add Product** link. The Create Product screen opens.

Figure 4-57 Create Product

2. Enter values in the appropriate fields, as described in Table 4-21.

Table 4-21 Create Product Parameters

Field	Description
Name	The DNS Product Name that you want to create. This is a mandatory field.
Description	A description of this product. This is an optional field.
Vendor	Select the Vendor of this product.
Type	<i>Read only.</i> The DNS product type is selected.
Configuration Type	Used to tell the system which type (or syntax) of configuration files should be created during a configuration/deployment task: Supported DNS Types: BIND9 - Indicates that servers that are defined as this product type utilize BIND 9 DNS syntax for their configuration files. BIND8 – Indicates that servers that are defined as this product type utilize BIND 8 DNS syntax for their configuration files. MSFT - Indicates that servers that are defined as this product type utilize Microsoft DNS syntax for their configuration files. CNR – Indicates that servers that are defined as this product type utilize Cisco Network Registrar Command syntax for their configuration files.
Collection Type	Used to tell the system which type of collection mechanism should be used to collect information from this service. There are no supported DNS collection types, so the value is set to NONE.

Chapter 5 Managing DHCP

In IPControl 5.0, all the features you need to set up DHCP servers is located in the DHCP section of the Management menu. This chapter describes how to use each selection on the DHCP menu.

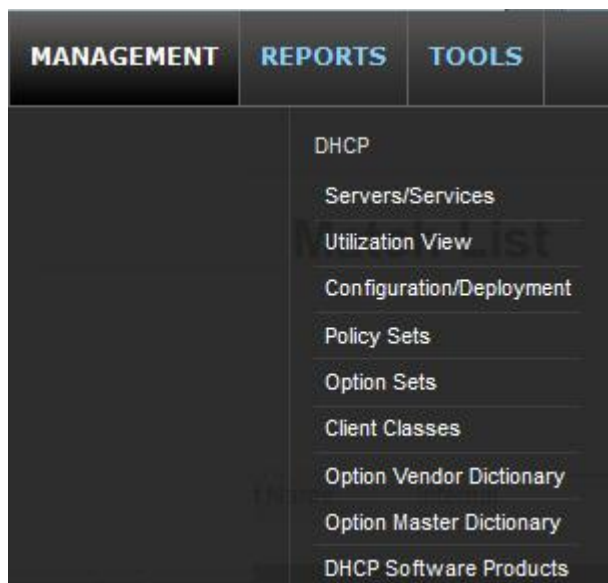


Figure 5-1 DHCP Menu Selections

Servers/Services

The **Servers/Services** option in the DHCP section of the **Management** menu allows you to define and maintain a layer 3 network DHCP service. Use IPControl to manage and plan the IP address space, policies and options that are allocated to your DHCP network service. Then use IPControl to create the configuration files necessary for DHCP services.

Managing DHCP Servers/Services

To manage DHCP servers and services, follow these steps.

1. Select **Servers/Services** from the DHCP section of the **Management** menu. The list of DHCP Servers/Services opens, as shown in Figure 5-2.

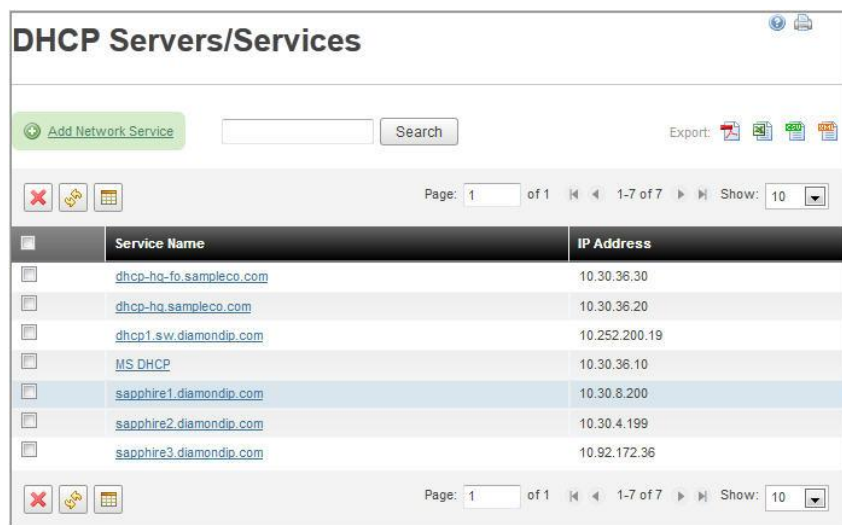


Figure 5-2 DHCP Servers/Services

2. Choose from the following actions.

To ...	Then ...
Search for a particular DHCP Network Service	<ol style="list-style-type: none"> 1. Enter a search string into the text block. 2. Click Search. The list of servers changes to match the search string.
Add a DHCP Network Service	Refer to “Adding a DHCP Server” on page 178.
Edit a DHCP Network Service	<ol style="list-style-type: none"> 1. Click on the service entry in the Service Name list. The Edit DHCP Server screen opens. 2. Edit fields and tab entries as needed. Refer to the descriptions in the following sections for more information.
Delete one or more DHCP Network Services	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click 3. At the confirmation prompt, click OK to delete the selected Network Services, or Cancel to return to the previous screen.

Adding a DHCP Server

In the DHCP servers/Services screen, select the Add Network Service link. The Add DHCP Server screen appears on the **General** tab.

Add DHCP Server

General

Name:

IP Address:

Product Name:

Agent:

Default Scope Utilization Warning Threshold:

Include during Global Synchronization Task: ☐

Configuration File Path:

Lease File Path:

Figure 5-3 Add DHCP Server

Select a product from the **Product Name** drop-down list. The screen changes to show you available options for the server product type that you selected and displays additional tabs, described in the next sections.

Add DHCP Server

General **Collection** **Configuration** **Failover Peer** **Extensions**

Name:

IP Address:

Product Name:

Agent:

Default Scope Utilization Warning Threshold:

Include during Global Synchronization Task: ☒

Configuration File Path:

Lease File Path:

Start Script:

End Script:

Figure 5-4 Product Name Selected in General Tab

General Tab

Table 5-1 General Tab Parameters

Field	Description
Name	Enter the name of this DHCP Server. Typically, this is the fully qualified domain name of the system where the service is running.
IP Address	Enter the IP Address of this service. This is required if you use IPControl to collect configuration information from this service, or create configuration files for this service.
Product Name	Select the Product Name from the drop-down list of DHCP products available within this system. Use the Management > DHCP Software Products menu option to manage products defined within the system.
Agent	Select the Agent that will be used to collect and/or distribute information to/from this service.
Default scope utilization warning threshold	The default threshold (in percent) that is used to provide warnings when usage of a pool assigned to this service is exceeded.
Include during global synchronization task	Select this checkbox if you want to include this service in the global synchronization task. If this service is included in the global synchronization task, the service's configuration and utilization information will be collected when the task runs.
Configuration File Path:	<p>Enter the fully qualified pathname of the configuration file. The typical entries are listed below:</p> <ul style="list-style-type: none"> • INS DHCP: /opt/incontrol/dhcpd/dhcpd.conf • ISC DHCP: /etc/dhcpd.conf • Lucent QIP: /opt/qip/dhcp/dhcpd.conf • Fastflow: /etc/dhcpd.conf • Cisco CNR: /opt/incontrol/tmp/dhcpd.conf • MS DHCP: c:\program files\diamond ip\incontrol\tmp\msdhcp.conf
Lease File Path:	<p>Enter the fully qualified pathname of the lease file for this DHCP server. The typical entries are listed below:</p> <ul style="list-style-type: none"> • INS DHCP: /opt/incontrol/dhcpd/dhcpd.leases • ISC DHCP: /etc/dhcpd.leases • Lucent QIP: /opt/qip/dhcp/dhcp.db • Fastflow: /etc/dhcpd.leases • Cisco CNR: /opt/incontrol/tmp/dhcpd.leases • MS DHCP: c:\program files\diamond ip\incontrol\tmp\msdhcp.lease <p>Note: Fully Qualified Domain names can be collected for MS Windows 2003/2008 DHCP servers, but not MS Windows 2000 Servers.</p>
Start Script	<p>The script that is used to start the DHCP server. This script is called by IPControl to start a DHCP server.</p> <p>INS DHCP: /opt/incontrol/etc/dhcpd_start</p>

Field	Description
End Script	The script that is used to stop the DHCP server. This script is called by IPControl to stop a DHCP server. INS DHCP: /opt/incontrol/etc/dhcpd_stop

Collection Tab

Click on the **Collections** tab to display the collection information. This area allows you to select a collection type, enter login information, and set the port used for collection.

Add DHCP Server

General Collection Configuration Failover Peer Extensions

Collection Type: --- Please Select ---

Username:

Password:

Confirm Password:

Port:

Submit Cancel

Figure 5-5 Collection Tab

Table 5-2 Collection Tab Parameters

Field	Description
Collection Type	Select the method that will be used to collect information about this service. Select “File Transfer Protocol – FTP” to use the FTP protocol. Select “Secure Copy – SCP” to use the SCP protocol. If you select SCP, you must manually configure SSH on the system that is running the service.
Username	Enter the user id that will be used for the protocol that you selected (FTP or SCP). The Agent uses this credential when communicating with the server on which the Net Service is running.
Password	Enter the password that will be used for the protocol that you selected (FTP or SCP). The Agent uses his credential when communicating with the server on which the Net Service is running.
Confirm Password	Confirm the password that will be used for the protocol that you selected (FTP or SCP).
Port	Enter the port that will be used to connect to the service (FTP or SCP). The default port for FTP is 21; the default port for SCP is 22. The defaults may be overridden if different ports are used within your network for security purposes.

Field	Description
Collect via CNR SDK	When enabled, this Network Service can communicate properly with a CNR 8 DHCP server. The CNR 8 DHCP server must be running only the IPControl Agent (without DNS and DHCP installed by BT Diamond IP), and that agent must also contain the CNR 8 SDK which must be obtained from Cisco. When this option is not selected, this Network Service can communicate properly with older CNR DHCP versions, which use the <code>nrcmd</code> and <code>cnr_exim</code> executables.
Path to the CNR Binary Executable Directory.	Enter the full path of where the CNR <code>nrcmd</code> and <code>cnr_exim</code> executables are located. Example: <code>/opt/nwreg2/usrbin</code> Note: This selection does not appear if you have the Collect via CNR SDK option selected.
CNR Userid	Enter the user ID required to allow execution of the <code>nrcmd</code> and/or <code>cnr_exim</code> utilities for this cluster.
CNR Password	Enter the password required to allow execution of the <code>nrcmd</code> and/or <code>cnr_exim</code> utilities for this cluster.
Confirm CNR Password	Confirm the CNR password.
CNR Cluster Name	Enter the CNR cluster name for this server.
Collect Failover Backup Subnets	Unchecked indicates that the collection will ignore any subnets that this DHCP server is failover for. Typically, if you are collecting DHCP information from all your DHCP server, collection of data for those subnets would be accomplished when you are performing collection against the primary DHCP server. Checked indicates that you will collect data for any subnets that this server is failover for. Typically you would leave this unchecked, so that you do not collect duplicate information from both the primary and failover DHCP servers.

Configuration Tab

Click on the **Configuration** tab to display the configuration options. This area allows you to select different DHCP Server configuration options.

Figure 5-6 Configuration Tab

Table 5-3 Configuration Tab Parameters

Field	Description
Perform Dynamic DNS Updates	Checked indicates that the system will send RFC2136 dynamic DNS updates to the primary DNS server when a lease is given out.
Option Set	Select the default option set for this DHCP server. Options that are assigned at the DHCP server level will be used system wide.
Policy Set	Select a default Policy Set for this server. A Policy set applied at the server level contains policies that are used system wide. It can contain items such as default lease times, and so on.
DHCP Client Classes	Select the DHCP Client classes that are available for use by this DHCP server. Note: You <i>must</i> define all client classes that are valid for this server. When an administrator is selecting client classes for this server, only the client classes that have been selected appear in the selection list.

Failover Peer Tab

Click on the **Failover** tab to display the failover information. This area allows you to identify the server's failover server.

Figure 5-7 Failover Peer Tab

Table 5-4 Failover Peer Tab Parameters

Field	Description
Failover IP Address	Enter the IP Address of this server that will be used for failover communications to other DHCP servers.
Failover Port	Enter the port number that will be used for Failover communications. Typically this is 847 for primary servers or 647 for failover servers.

Field	Description
My Failover Peers	<p>Peer Server – Select failover peer server(s) for this server that will be used to implement DHCP failover. Refer to the appendix for more information regarding DHCP Failover. Select a Failover Peer Server, and enter the following:</p> <p>Contact Timeout – Determines how long a server will wait without receiving any messages from its partner before it assumes that the connection to its partner has failed.</p> <p>Max Pending Updates – The maximum number of pending updates that the server can accept without blocking the input.</p> <p>Max Client Lead Time (MCLT) – The amount of time by which either server can extend a lease without contacting the other server.</p> <p>Load Balance Split – Tells the primary server what portion of all clients it should serve in a load balancing scenario. A value of “255” indicates that the primary server serves all clients and the failover server serves no clients (this is typical Primary DHCP and Failover behavior without load balancing). A value of “128” indicates that approximately 50% of the clients will be served by the primary DHCP server, and 50% of the clients will be served by the failover DHCP server.</p> <p>Load Balance Override – Determines when the primary or failover server will bypass load balancing and respond to the client even if the client is supposed to be served by the other server. Every message from a DHCP client includes a field that indicates for how many seconds the DHCP client has been trying to contact the DHCP server. If the value of that field is higher than the configured “Load Balance Override” seconds, the DHCP server always attempts to respond to the client, regardless of the “Load Balance Split”.</p>

Field	Description
My Primary Peers	<p>Peer Server – Select a Primary peer server(s) for this server that will be used to implement DHCP failover. Refer to the appendix for more information regarding DHCP Failover. Select a Primary Peer Server, and enter the following:</p> <p>Contact Timeout – Determines how long a server will wait without receiving any messages from its partner before it assumes that the connection to its partner has failed.</p> <p>Max Pending Updates – The maximum number of pending updates that the server can accept without blocking the input.</p> <p>Max Client Lead Time (MCLT) – The amount of time by which either server can extend a lease without contacting the other server.</p> <p>Load Balance Split – Tells the primary server what portion of all clients it should serve in a load balancing scenario. A value of “255” indicates that the primary server serves all clients and the failover server serves no clients (this is typical Primary DHCP and Failover behavior without load balancing). A value of “128” indicates that approximately 50% of the clients will be served by the primary DHCP server, and 50% of the clients will be served by the failover DHCP server.</p> <p>Load Balance Override – Determines when the primary or failover server will bypass load balancing and respond to the client even if the client is supposed to be served by the other server. Every message from a DHCP client includes a field that indicates for how many seconds the DHCP client has been trying to contact the DHCP server. If the value of that field is higher than the configured “Load Balance Override” seconds, the DHCP server always attempts to respond to the client, regardless of the “Load Balance Split”.</p>

Extensions Tab

Click on the **Extensions** tab to display the configuration file extensions area. This area allows you to create free form text to add to the beginning or the end of the *named.conf* configuration file.

The screenshot shows a web-based configuration window titled "Add DHCP Server". At the top, there are five tabs: "General", "Collection", "Configuration", "Failover Peer", and "Extensions". The "Extensions" tab is currently selected. Below the tabs, there are two text input areas. The first is labeled "Insert at beginning of configuration file:" and the second is labeled "Append to end of configuration file:". Both input areas are empty. At the bottom of the window, there are two buttons: "Submit" and "Cancel".

Figure 5-8 Extensions Tab

Table 5-5 Extensions Tab Parameters

Field	Description
Insert at beginning of configuration file	Enter any free text options that you want to appear at the beginning of the configuration file. Note: The extensions are limited to 32000 characters.
Append to end of configuration file	Enter any free text options that you want to appear at the end of the configuration file. Note: The extensions are limited to 32000 characters.

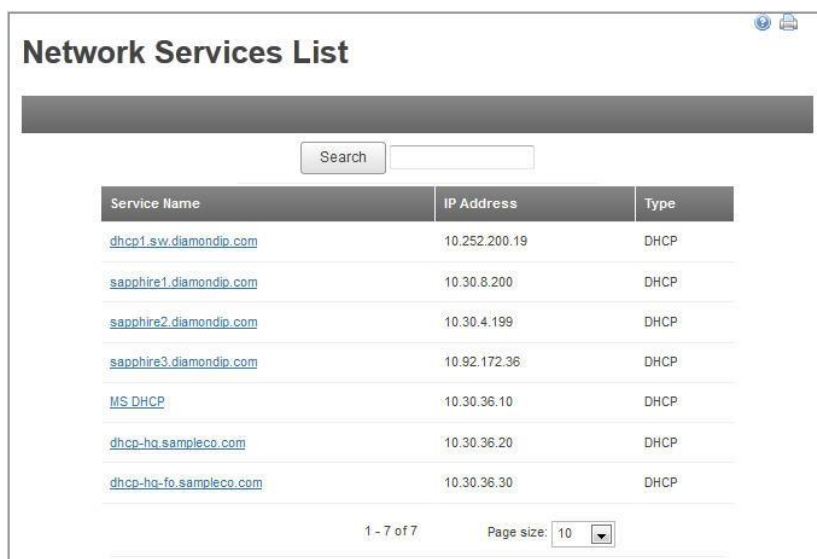
Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen. If the DHCP server was successfully added, the new DHCP server appears in the DHCP Servers/Services list.

Utilization View

To determine network usage details for a DHCP server, use the Utilization View feature, where you can review usage by Pool Type and Block Type. You can also review a chart showing the allocation history of available vs. used space for a selected DHCP server.

Network Services List

To review network usage details for a DHCP server, select **Utilization View** from the DHCP section of the **Management** menu. The Network Services List screen is displayed, as shown in Figure 5-9.



Service Name	IP Address	Type
dhcp1.sw.diamondip.com	10.252.200.19	DHCP
sapphire1.diamondip.com	10.30.8.200	DHCP
sapphire2.diamondip.com	10.30.4.199	DHCP
sapphire3.diamondip.com	10.92.172.36	DHCP
MS DHCP	10.30.36.10	DHCP
dhcp-hq.sampleco.com	10.30.36.20	DHCP
dhcp-hq-fo.sampleco.com	10.30.36.30	DHCP

1 - 7 of 7 Page size: 10

Figure 5-9 Network Services List

To review network usage details, click the Service Name you want to review, or search for a specific Service Name as follows:

1. Type a search string in the text block

2. Click **Search**.
3. Select the Service Name you want to review from the search results.

The Utilization Display appears, as shown in Figure 5-10.

Utilization Display

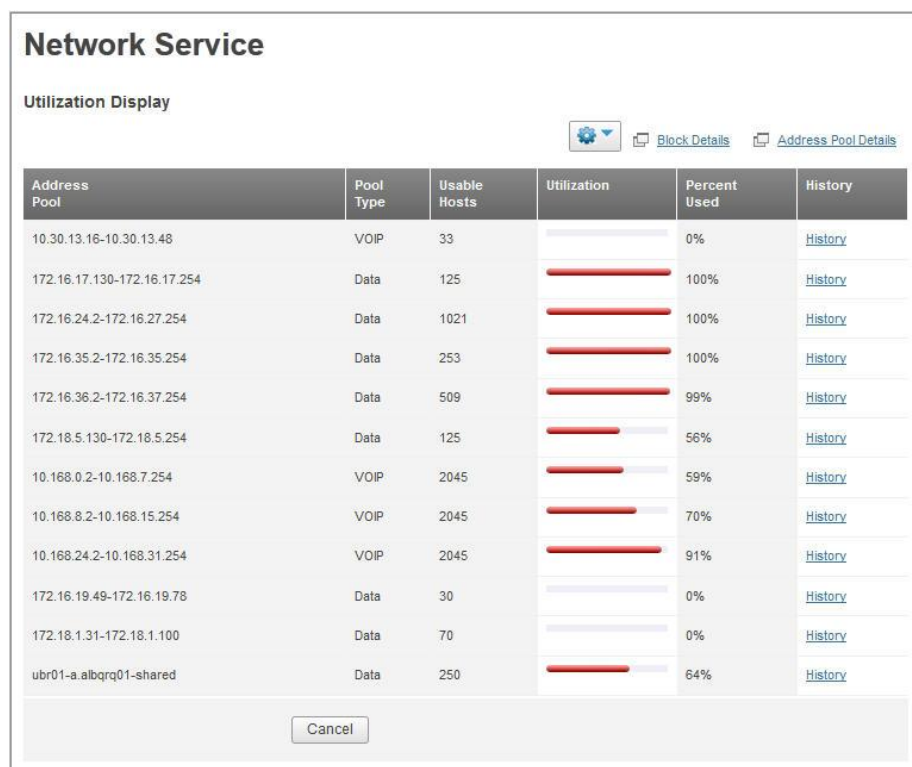


Figure 5-10 Network Service Utilization Display

The columns in the Utilization Display are described in Table 5-6.

Table 5-6 Network Service Utilization Display Elements

Field	Description
Address Pools	The starting and ending address of the address pool, or the “shared network” name of a group of address pools.
Pool Type	The block type of the pool.
Usable Hosts	The number of usable hosts that are contained within the current block
Utilization	A graph of the current utilization of the block.
Percent Used	The percentage of this block that is currently utilized.
History	Select this link to display a history graph of the utilization for the current address pool.
and	Displayed when IPV6 address pools are listed. Used to change the display format of IPV6 hosts. See “Displaying IPV6 Capacities” on

Field	Description
	page 14 for more information.

To return to the Network Service List, click **Cancel**. To review a chart showing the allocation of available vs. used space across an entire DHCP server, click the **History** link beside the pool you want to review. The Address Pool History chart appears, as shown in Figure 5-11.

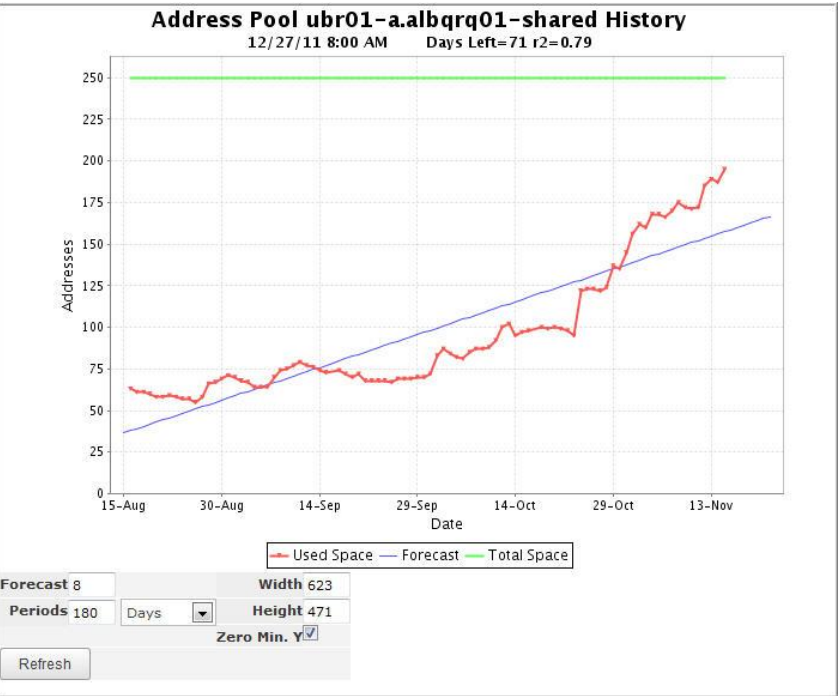



Figure 5-11 Address Pool History Chart

Block Details

To display detailed information about the blocks associated with a DHCP server, click **Block Details**. The Block Details screen opens, as shown in Figure 5-12.

Network Service

Block Details


[Utilization Display](#)
[Address Pool Details](#)

Block	Block Type	Leasable Hosts	Dynamic Hosts	Locked Hosts	Utilization	Lease %	History
10.168.0.0/21	VOIP	2045	1,201	0	<div><div></div></div>	59%	History
10.168.8.0/21	VOIP	2045	1,428	0	<div><div></div></div>	70%	History
10.168.24.0/21	VOIP	2045	1,855	2	<div><div></div></div>	91%	History
10.30.13.0/25	VOIP	0	0	0	<div><div></div></div>	0%	History
172.16.24.0/22	Data	1021	1,017	0	<div><div></div></div>	100%	History
172.16.35.0/24	Data	252	252	0	<div><div></div></div>	100%	History
172.16.36.0/23	Data	509	503	0	<div><div></div></div>	99%	History
172.18.5.128/25	Data	125	125	0	<div><div></div></div>	100%	History
172.18.5.0/25	Data	125	125	0	<div><div></div></div>	100%	History
172.16.17.128/25	Data	125	125	0	<div><div></div></div>	100%	History
172.18.17.0/25	Data	125	125	0	<div><div></div></div>	100%	History
172.18.1.0/24	Data	0	0	0	<div><div></div></div>	0%	History
172.16.19.0/24	Data	0	0	0	<div><div></div></div>	0%	History

[Cancel](#)

Figure 5-12 Network Service Block Details

The columns in the Block Details screen are described in Table 5-6.

Table 5-7 Block Details Display Elements

Field	Description
Block	The name of the block
Block Type	The block type of the block.
Leasable Hosts	The number of dynamic addresses available to DHCP for allocation.
Dynamic Hosts	The number of dynamic hosts within the subnet or block. This is inclusive of the “locked” hosts.
Locked Hosts	The number of locked addresses in this block.
Utilization	The percentage of this block that is currently utilized.
Lease %	The percentage of dynamic addresses leased to clients.
History	Click on this link to view a history graph of the utilization information for this block.

To return to the Network Service List, click **Cancel**. To review a chart showing the allocation of available vs. used space across an entire DHCP server, click the **History** link beside the block you want to review. The Block History chart appears, as shown in Figure 5-13.

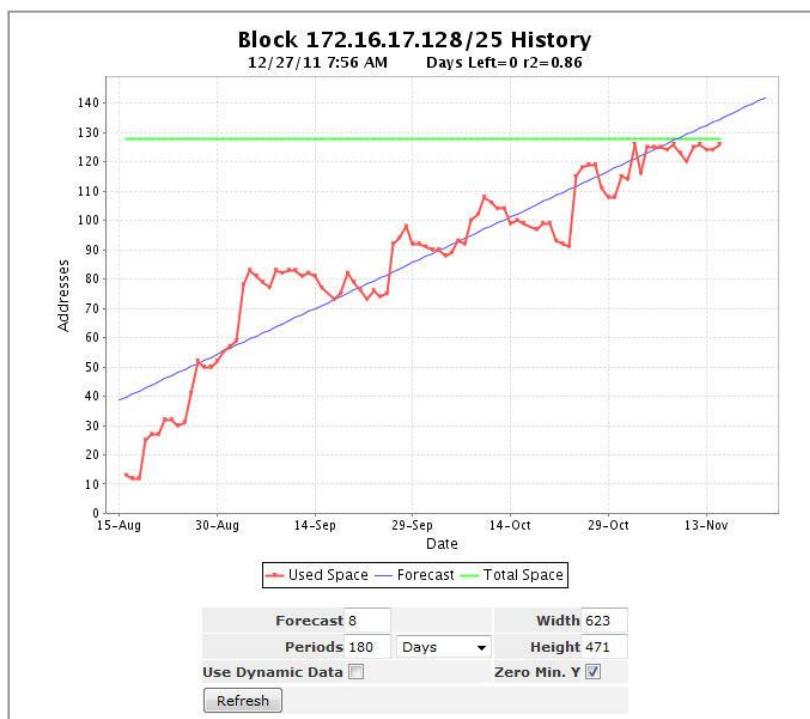


Figure 5-13 Block History Chart

Configuration/Deployment

The Configuration/Deployment option allows you to create on-demand, scheduled, or recurring scheduled tasks for deployment of configuration information to your DHCP network services.

Configuration/Deployment Task Definition Options

To deploy configuration information to a network service, select the “task type”, select the “network service”, and then specify when to run the task. Depending upon the selection of when you will be running the task, different options will be displayed on the screen for you to select. Refer to the sections below for additional information about each option. Note that once you click **Submit**, a new task will be created, and submitted to the system. Once tasks have been created, they can be managed using the **Task** menu option.

DHCP Configuration/Deployment

Task Type

When to run task ☒ Immediate ☐ Scheduled ☐ Recurring

Submit

Figure 5-14 Configuration/Deployment

Select **DHCP Configuration – All Files** from the **Task Type** drop-down. The screen expands to display additional fields, as shown in and described in Table 5-8.

DHCP Configuration/Deployment

Task Type: DHCP Configuration - All Files

Stop on Errors and Warnings: ☐

Update Failover Servers: ☐

Push only if configuration changed: ☐

Delete task if no changes: ☐

Hold files for preview: ☐

Network Service: Search

When to run task: ☒ Immediate ☐ Scheduled ☐ Recurring

Submit

Figure 5-15 Addition Configuration/Deployment Screen Elements

Table 5-8 Configuration/Deployment Screen Elements

Field	Description
Stop on Errors and Warnings	<p>Checked indicates that the system will not complete the creation and distribution of the configuration option that you selected if the system encounters any errors or warnings. Best practices should be to select this option whenever you are performing a distribution option, which will allow you to not inadvertently apply an invalid configuration to a network service.</p> <p>Unchecked overrides any errors and warnings and creates and applies the configuration regardless of issues. This allows you the opportunity to override any errors or warnings as needed.</p>
Update Failover Servers	<p>Checked indicates that when you distribute configuration information to a DHCP server, if that server has failover servers, the configuration is also created and sent to the failover servers automatically.</p> <p>Unchecked indicates that only the selected DHCP server will be sent its configuration files.</p>
Push only if configuration changed	<p>If checked, indicates that the child push task should only occur only when there are changes to the configuration.</p>
Delete task if no changes	<p>If checked, indicates that the task will be deleted when there are no changes to the configuration, and the push does not occur due to the “push only if configuration changed” option.</p>
Hold files for preview	<p>If checked, the configuration files will be created, but not deployed. You can view the files from the Task List.</p>
Network Service	<p>Select Search and select a network service to perform this task against in the DHCP Servers/Services screen.</p>

Field	Description
When to run task	<ul style="list-style-type: none"> • Immediate – run the task immediately • Scheduled – run the task on the predetermined date and time specified • Recurring – Run this task multiple times

On-demand (Immediate) Config/Deployment Task

To define an immediate task, define the task parameters and select **Immediate** from the **When to run task** options. Click **Submit** to create the task. A new task is created and submitted to the system. Once tasks have been created, they can be managed using the **Task** menu option.

Scheduled Config/Deployment Task

To schedule a future task, define the task parameters and select **Scheduled** from the **When to run task** selections. Schedule options are displayed, as shown in Figure 4-18.





Figure 5-16 Configuration/Deployment

To select a future date to run the task, type in the desired date in mm/dd/yyyy format or click the calendar icon to select a date. A calendar is displayed, as shown in Figure 4-19, with today's date selected by default.



Figure 5-17 Calendar Utility

You can use the following navigation links to change to another month and/or year and then select a date in the month to close the utility:

-  Previous Year
-  Previous Month
-  Next Year
-  Next Month

Select the hours, minutes, and AM or PM to schedule a specific time for the task.




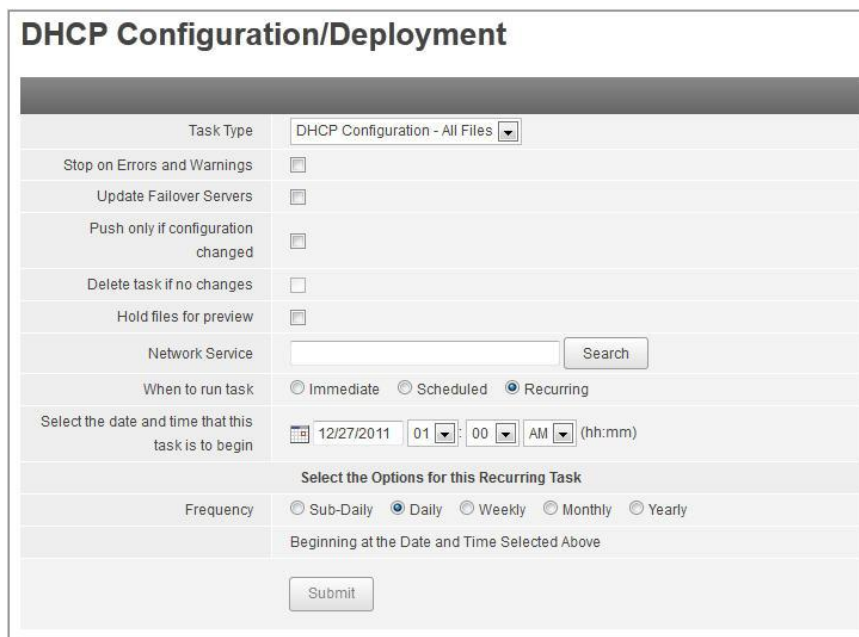
  :  (hh:mm)

Figure 5-18 Hour and Minutes

Once all parameters have been entered, click **Submit**. A new task is created, and submitted to the system. Once tasks have been created, they can be managed using the **Tasks** menu option on the **Tools** menu.

Recurring Config/Deployment Task

A recurring task enables you to define tasks to run on a pre-determined schedule. This option allows you to define tasks (such as DHCP Configuration) that will occur at regular intervals, providing you with up to date information. To schedule a recurring task, set the task parameters and select **Recurring** from the **When to run task** selections. Recurring options are displayed as shown in Figure 4-21.



The screenshot shows the 'DHCP Configuration/Deployment' utility interface. It features a table with various task configuration options. The 'Task Type' is set to 'DHCP Configuration - All Files'. Several checkboxes are present for 'Stop on Errors and Warnings', 'Update Failover Servers', 'Push only if configuration changed', 'Delete task if no changes', and 'Hold files for preview'. A 'Network Service' field with a 'Search' button is also visible. Under 'When to run task', the 'Recurring' radio button is selected. The 'Select the date and time that this task is to begin' section shows a date of '12/27/2011' and a time of '01:00 AM'. Below this, the 'Select the Options for this Recurring Task' section shows 'Frequency' set to 'Daily' and 'Beginning at the Date and Time Selected Above'. A 'Submit' button is at the bottom.





DHCP Configuration/Deployment	
Task Type	DHCP Configuration - All Files
Stop on Errors and Warnings	<input type="checkbox"/>
Update Failover Servers	<input type="checkbox"/>
Push only if configuration changed	<input type="checkbox"/>
Delete task if no changes	<input type="checkbox"/>
Hold files for preview	<input type="checkbox"/>
Network Service	<input type="text"/> Search
When to run task	<input type="radio"/> Immediate <input type="radio"/> Scheduled <input checked="" type="radio"/> Recurring
Select the date and time that this task is to begin	 12/27/2011  01  : 00  AM (hh:mm)
Select the Options for this Recurring Task	
Frequency	<input type="radio"/> Sub-Daily <input checked="" type="radio"/> Daily <input type="radio"/> Weekly <input type="radio"/> Monthly <input type="radio"/> Yearly
Beginning at the Date and Time Selected Above	
Submit	

Figure 5-19 Recurring Options

To set up a recurring task, follow these steps:

1. Select the date and time that you want the recurring task to begin.
2. Click on the calendar icon to display a calendar. Refer to “Scheduled Config/Deployment Task” on page 133 for information on using the calendar utility.
3. Select the frequency for the recurring task.
 - ▶ Sub-Daily
 - ▶ Daily
 - ▶ Weekly
 - ▶ Monthly
 - ▶ Yearly
4. Click **Submit**.

A new task is created and submitted to the system.

After tasks have been created, you can manage them using the **Task** menu option.

Policy Sets

Use the DHCP Policy Sets screen to maintain DHCP Policy Sets. DHCP Policy Sets are groups of DHCP vendor-specific policies that you implement to affect the behavior of the DHCP server.

There are two types of policies that can be configured for the DHCP server:

- “Server-specific” policies that effect the configuration of the DHCP server itself.
- “Scope-specific” policies that effect individual IP Address or IP Address pools

By using DHCP Policy Sets, you can simplify the configuration steps that are needed. DHCP Policy Sets allow you to group logical sets of policies together for specific purposes, and then allow you to apply the Policy Sets at different areas within your DHCP infrastructure.

DHCP Policy Sets allow you to define policies within your network, and then implement those policies in a consistent manner throughout your DHCP infrastructure.

To work with DHCP Policy Sets, select **Policy Sets** from the DHCP section of the **Management** menu. The DHCP Policy Sets screen opens, as shown in Figure 5-20.

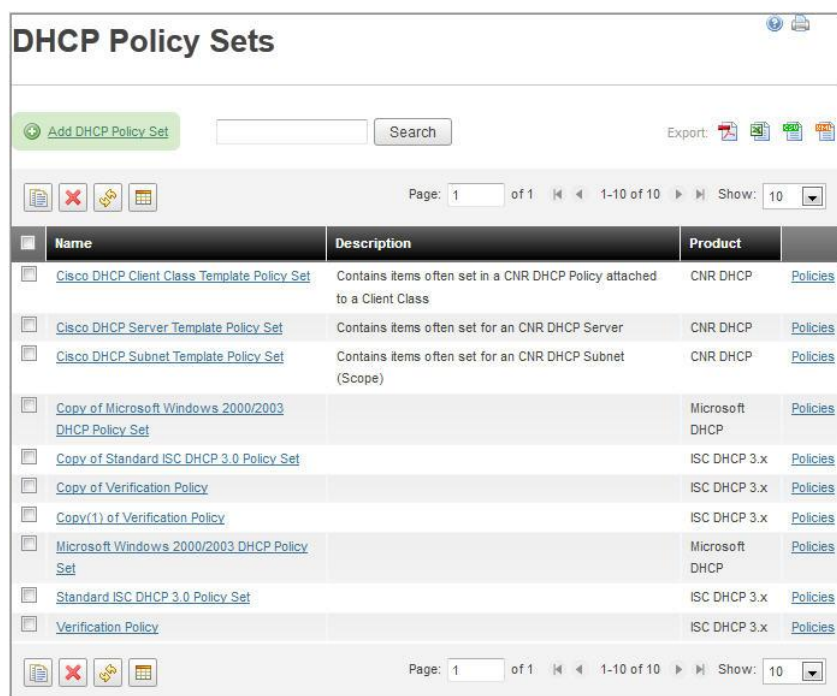




Figure 5-20 DHCP Policy Set

Choose from the following actions:

To ...	Then ...
Copy one or more DHCP Policy Sets	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you wish to copy. 2. Click .
Add a DHCP Policy Set	Refer to “Adding a DHCP Policy Set” on page 196.
Edit a DHCP Policy Set	<ol style="list-style-type: none"> 1. Click on the policy set entry in the Name list. The Edit DHCP Policy Set screen opens. 2. Edit fields and tab entries as needed. Refer to Table 5-9 for more information.
Delete one or more DHCP Policy Sets	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Policy Sets, or Cancel to return to the DHCP Policy Sets screen. <p>Note: Make sure that this Policy Set is not assigned to any DHCP Server (Network Service), Subnet Policy, IP Address, or IP Address Pool before you delete it. Any references to this Policy Set will be removed from servers, subnets, or pools, if the set is deleted.</p>

Adding a DHCP Policy Set

To add a DHCP Policy Set, click the **Add DHCP Policy Set** link. The Add DHCP Policy Set screen appears as follows:

Figure 5-21 Add DHCP Policy Set

Fill in the appropriate fields, as described in Table 5-9.

Table 5-9 Add DHCP Policy Set Parameters

Field	Description
Name	Mandatory. The DHCP Policy Set Name that you want to assign to this option set (for example, ‘Server Policy’, ‘VoIP Scope Policy’). This is a mandatory field.
Description	Optional. Enter a description of the DHCP Policy Set.
Product	Select the DHCP Vendor Product that the DHCP Policy Set represents.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the DHCP Policy Sets screen.

Working with DHCP Policy Set Policies

To review, edit, add or remove policies for an existing Policy Set, select the **Policies** link beside a policy on the DHCP Policy Sets screen (Figure 5-20). The DHCP Policies for Policy Set screen opens, as shown in Figure 5-22.

DHCP Policies for Policy Set: Microsoft Windows 2000/2003 DHCP Policy Set

Show all policies

Select	Name	Value(s)	Applies To
<input checked="" type="checkbox"/>	Audit Log File Path	C:\WINDOWS\System32\dhcp	
<input checked="" type="checkbox"/>	Database Backup Interval	60	
<input checked="" type="checkbox"/>	Database Backup Path	C:\WINDOWS\System32\dhcp\backup	
<input checked="" type="checkbox"/>	Database Cleanup Interval	1440	
<input checked="" type="checkbox"/>	Database Logging Flag	1	
<input checked="" type="checkbox"/>	Detect Conflict Retry	0	

Submit

Cancel

Figure 5-22 DHCP Policies for Policy Set

Table 5-10 DHCP Policies for Policy Set Parameters

Field	Description
Select	When checked, the policy is associated/enabled with this DHCP policy set.
Name	The name of the policy.
Value(s)	The values that has been assigned to this policy. If the text “—Same as Subnet—“appears in this field, the actual value is inherited from the Subnet’s value at the time that the configuration file is created.
Applies To	Indicates whether the policy applies to Server, Subnet, and/or Client Class.

Choose from the following actions:

To ...	Then ...
Add new policies to a selected policy set	<ol style="list-style-type: none"> 1. Select the Show all policies check box. All the policies that are defined within the system are displayed. 2. Click on the name of the policy to assign a value. The DHCP Policy screen appears. <div data-bbox="695 499 1266 1081" data-label="Form"> </div> <p>Figure 5-23 DHCP Policy</p> <ol style="list-style-type: none"> 3. Type in the requisite values. Possible data types are: <ul style="list-style-type: none"> ▶ numeric – indicates a numeric field only ▶ ipaddress – indicates an IP Address is required ▶ optionid4 – lists options that DHCP server returns to all DHCP clients ▶ selectlist – select a value from the dropdown list in the Value field ▶ quoted-string – indicates a text string between quotation marks is required ▶ string – indicates a text string is required ▶ time – indicates a time setting such as 24h or 60m is required ▶ boolean – indicates a true or false is required 4. Click Submit. The Select checkbox is checked and values are shown in the Value(s) column.

To ...	Then ...
Edit the value of a policy	<ol style="list-style-type: none"> 1. Click on the policy set entry in the Name list. The DHCP Policy screen opens. 2. Edit values as needed. 3. Click Submit. The new values are shown in the Value(s) column.
Remove policies from a policy set	<ol style="list-style-type: none"> 1. Uncheck the checkbox next to the policy that you want to remove. 2. Click Submit.

Option Sets

Use the DHCP Option Sets screen to maintain DHCP option sets that have been grouped according to DHCP RFC options that are used to send to a DHCP or Bootp client (or host). DHCP provides other configuration parameters in addition to an IP Address to a client. In fact, several additional parameters must be provided to a client before that host can communicate with other hosts. A host, at a minimum, must be configured with:

- Its local subnet mask
- The IP address of at least one router on its subnet
- The IP address of a Domain Name Server (DNS)

Using IPControl, you can simplify the configuration steps that are needed, by using DHCP Option Sets. DHCP Option Sets allow you to group logical sets of options together for specific purposes, and then apply the Option Sets at different areas within your DHCP infrastructure. DHCP Option Sets offer an advanced “subclass”-like approach to applying Option Sets by allowing you to either hardcode values for each option within the Option Set, or by allowing the use of “expressions” such as “Same As Subnet”, which will be resolved at the time the configuration file is created.

DHCP Option Sets allow you to define policies within your network, and then utilize those policies in a consistent manner throughout your DHCP infrastructure.

When you select this option, the following list appears:

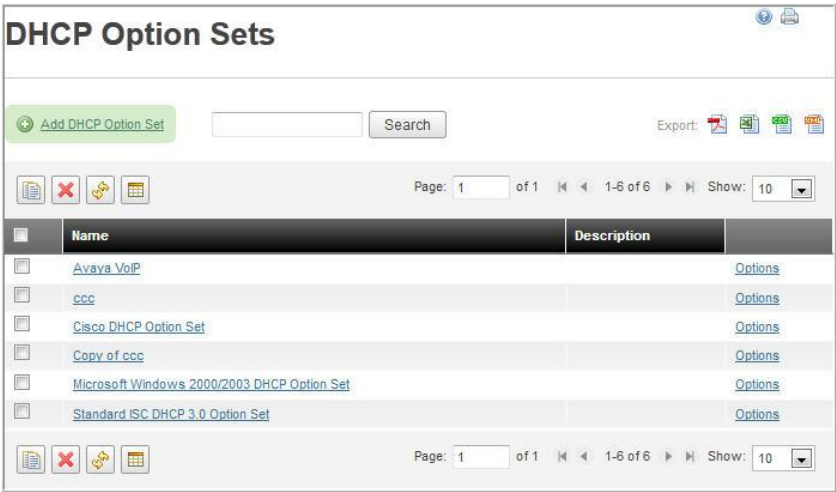


Figure 5-24 DHCP Option Sets

To delete one or more DHCP Option Sets, select the checkbox beside each item you wish to delete, and click . You are prompted for confirmation.

Note: Make sure that this Option Set is not assigned to any DHCP Server (Network Service), Subnet Policy, IP Address, or IP Address Pool before you delete it. Any references to this Option Set will be removed from servers, subnets, or pools, if the set is deleted.

Click **OK** to delete the selected DHCP Option Sets, or **Cancel** to return to the previous screen.

To copy one or more DHCP Option Sets, select the checkbox beside each item you wish to copy, and click .

Adding a DHCP Option Set

To add a DHCP Option Set, click the **Add DHCP Option Set** link. The Add DHCP Option Set screen appears as follows:

Figure 5-25 Add DHCP Option Set

Table 5-11 Add DHCP Option Set Parameters

Field	Description
Name	The DHCP Option Set Name that you want to assign to this option set (for example, 'Windows Clients', 'VoIP Devices'). This is a

	mandatory field.
Description	An optional description of this option set.

Fill in the appropriate fields. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

DHCP Option Set Options

Selected configuration options for an Option Set are defined and set using the **Options** link on the DHCP Option Set screen. Clicking the **Options** link opens the DHCP Options for Option Set screen.

DHCP Options for Option Set: Standard ISC
DHCP 3.0 Option Set

Show all options

Enabled	Code	Name	Value(s)
<input checked="" type="checkbox"/>	1	Subnet Mask	-- Same as Subnet --
<input checked="" type="checkbox"/>	3	Routers	-- Same as Subnet --
<input checked="" type="checkbox"/>	6	Domain Name Servers	-- Same as Subnet --
<input checked="" type="checkbox"/>	15	Domain Name	-- Same as Subnet --
<input checked="" type="checkbox"/>	44	NetBIOS over TCP/IP Name Servers	-- Same as Subnet --

Submit Cancel

Figure 5-26 DHCP Options for Option Set

Table 5-12 DHCP Options for Option Set Parameters

Field	Description
Enabled	When checked, this option is associated with this DHCP option set.
Code	The option code as defined by the RFC. Refer to RFC.2132 .
Name	The name of the option.
Value(s)	The values that have been assigned to this option. If -Same as Subnet- appears in this field, the actual value is inherited from the Subnet's value as the configuration file is created.

From here you can view all options assigned to this option set, edit the values of individual options within this set, add new options to this option set, and remove options from this option set.

Once finished, click **Submit** to save all changes on this Options screen, or **Cancel** to discard all changes and return to the previous screen.

Viewing all options assigned to this option set

When you first enter this screen, any options that are assigned to this option set have the **Enabled** checkbox selected. To add new options to this option set, click on the **Show all options** checkbox at the top of the screen. This displays all options that are defined within the system.

To add a new option to this option set, click the **Enabled** checkbox, and then click on the name of the option to assign a value. The DHCP Option screen appears as follows:

Figure 5-27 DHCP Options

Table 5-13 DHCP Options Parameters

Field	Description
Option name	The DHCP Option name assigned to this option.
Code	The option code as defined by the RFC. Refer to RFC 2132 .
Description	A description of this option.
Data Type	The data type that is required for this option: Numeric – indicates a numeric field only IP Address – indicates an IP Address is required String – indicates a text string is required Boolean – indicates a true or false is required
Minimum Value	Numeric data types only – the minimum value that is allowed.
Maximum Value	Numeric data types only – the maximum value that is allowed.
Same as Subnet Policy	On some specific options where it is appropriate, the value of the option can be set with the expression “Same as Subnet”. This will cause the value to be resolved during the configuration file creation.

Field	Description
Multiple Values Allowed	Specifies if multiple values are allowed for this option. True indicates that multiple values are allowed. False indicates that multiple values are not allowed. If multiple values are allowed, then the button “Append Value” will appear. Click on this button to append values to this option. For multi-valued options, you can reorder the option using the Up or Down buttons, and delete individual options by clicking Delete .
Value(s)	Enter the value for this option.

Fill in the appropriate fields. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Editing values of options assigned to this option set

To edit the value of an option that is assigned to this option set, click on the name of the option in the option list.

The DHCP Option screen appears as follows. Edit the value of the option and click **Submit** to save your changes, or click **Cancel** to return to the list.

DHCP Option

Option Name:	Routers
Code:	3
Description:	The router option specifies a list of IP addresses for routers on the client's subnet. Routers SHOULD be listed in order of preference.
Data Type:	ipaddress
Multiple Values Allowed:	true
Same as Subnet Policy:	<input checked="" type="checkbox"/> (Checked=Yes)

Value 1:

Figure 5-28 DHCP Option

Removing options from this option set

To remove options from an option set, uncheck the **Enabled** checkbox next to the option that you wish to remove from this option set.

Once finished, click **Submit** to save all changes on this Options screen, or **Cancel** to discard all changes and return to the previous screen.

Client Classes

The DHCP Client Classes screen allows you to maintain criteria that are used to group clients together for applying specific conditional behavior to the device, such as sending specific options to the device.

For example, sometimes it is useful to be able to provide an IP Address for a client from a specific address pool (or range) based on the type of client (or device). Or, you may need to provide extra DHCP options to a device because it is a specific type of device, such as sending special options to a VoIP phone. Or, you may need to supply a short lease time only to a specific group of MAC addresses, because you are moving these devices to another area within the network.

IPControl supports this capability in a powerful way, by allowing groups of devices to be specified either by MAC Address, Client Identifier, Hostname, User Class Identifier, Vendor Class Identifier, or by a custom expression.

Using DHCP Client Classes you can accomplish the following types of tasks:

- You can use this option to create groups of included or excluded devices based on MAC Address, Client Identifier, Hostname, User Class Identifier, or Vendor Class Identifier.
- You can use this option to provide specific options to groups of devices.
- You can use this option to change lease times for specific groups of devices.
- You can specify a logical expression that can be used to evaluate the attributes of a specific client, and then apply specific policies or options to that client.
- You can use this option to implement various “Quality of Service” schemes based on selecting which address pool (with corresponding options and policies) will service a specific client.

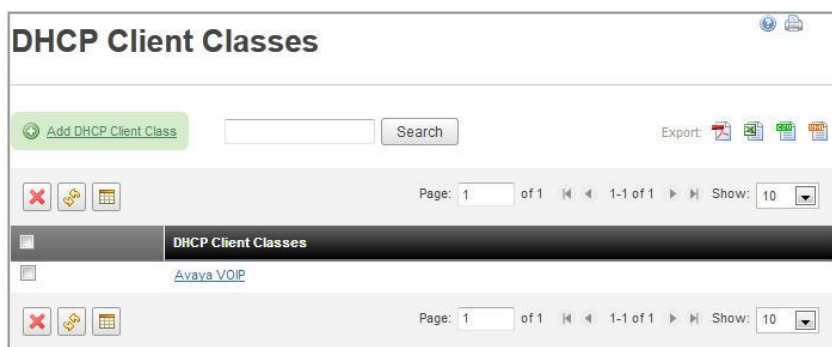



Figure 5-29 DHCP Client Classes

To delete one or more DHCP Client Classes, click the checkbox in the Select column for each item you wish to delete, and click .

Note 1: Make sure that the DHCP Client Class you are deleting are not associated with a DHCP server. Any references to this Client Class will be removed from servers or pools if the set is deleted.

Note 2: When you define a DHCP server, all Client Classes that you want to use on that DHCP server must be associated to the DHCP server within the DHCP Server definition screen.

Adding a DHCP Client Class

To add a Client Class, click the **Add DHCP Client Class** link. The Add DHCP Client Classes screen will appear.

Figure 5-30 Add DHCP Client Class

Table 5-14 Add DHCP Client Class Parameters

Field	Description
Name	The name associated with this DHCP Client Class.
Type	The type of client class restriction. This cannot be changed after saving the client class. Valid types are: <ul style="list-style-type: none"> - MAC Address - Client Identifier - Hostname - User Class Identifier - Vendor Class Identifier - Custom Expression
DHCP Policy Set	<i>Optional.</i> The DHCP Policy Set that will apply to clients in this DHCP Client Class.
DHCP Option Set	<i>Optional.</i> The DHCP Option Set that will apply to clients in this DHCP Client Class.

Enter the desired attributes. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Editing a DHCP Client Class

To modify an existing Client Class, click on the name in the Client Class List to open the Edit Client Classes screen.

Edit DHCP Client Classes

Name	Avaya VOIP
Type	Vendor Class Identifier
DHCP Policy Set	Verification Policy
DHCP Option Set	Avaya VoIP
Option Definition:	--- Same as Subnet ---

[Add Vendor Class Identifier](#)

Filter Criteria:

Identifiers: ☒ Begins With ☐ Contains ☐ Exact

Identifiers	Options
AVAYA	<input type="radio"/> Exact Match <input checked="" type="radio"/> Begins With <input type="button" value="Delete"/>

1 - 1 of 1 Page size: 10

Figure 5-31 Edit Client Class

Edit Client Classes as needed. Choose from the following actions:

- To add another vendor identifier, select the Add Vendor Class Identifier link. A data entry line appears in the Identifiers list where you can enter another vendor class identifier. Repeat as needed.
- To remove an identifier entry, select Delete.
- To search for identifiers that match your criteria, enter a string in the Filter Criteria field, choose from one of the Identifiers options and click Search. The Identifiers list is refreshed to match your criteria.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Option Vendor Dictionary

Use the Option Vendor Dictionary screen to maintain DHCP Vendor Options within the system. Vendor Options are DHCP options that are specific to a vendor or type of DHCP server. This menu item allows you to select a set of options (from the DHCP Master Option List) that are available for use with a specific type of DHCP server. In addition, the syntax for this option (as written to the configuration file) is specified using this menu item as well.

DHCP Option Vendor Dictionary		
Product List		
Name	Description	Options
ADC DHCP	ADC/BigBand Fastflow DHCP	Options
CNR DHCP	CNR DHCP 6.x	Options
INS DHCP	INS DHCP - DHCP 3.0.1	Options
INS DHCP (4.1)	INS DHCP - DHCP 4.1	Options
INS Sapphire DHCP	INS Sapphire DHCP - DHCP 3.0.2	Options
INS Sapphire DHCP (4.1)	INS Sapphire DHCP - DHCP 4.1	Options
ISC DHCP 3.x	ISC DHCP 3	Options
ISC DHCP 4.1	ISC DHCP 4.1	Options
Microsoft 2008 DHCP	Microsoft Windows 2008 DHCP Server	Options
Microsoft DHCP	Microsoft Windows 2000/2003 DHCP Server	Options
QIP DHCP	QIP DHCP 5.x	Options

Figure 5-32 DHCP Option Vendor Dictionary Product List

When the DHCP Option Vendor Dictionary icon or link is selected, the existing DHCP Products will be shown. DHCP Products can be added, modified, or deleted, using the **DHCP Software Products** menu item from the **Management** menu.

To modify the options associated with this DHCP Product, click the **Options** link next to the DHCP product that you want to maintain. The DHCP Vendor Option Dictionary screen appears.

DHCP Option Dictionary for INS DHCP (4.1)

☐ Show All Options

Enabled	Code	Name	Option Tag	Suffix	Render Definition
<input checked="" type="checkbox"/>	1	Subnet Mask	<input type="text" value="subnet-mask"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	2	Time Offset	<input type="text" value="time-offset"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	3	Routers	<input type="text" value="routers"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	4	Time Servers	<input type="text" value="time-servers"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	5	Name Servers	<input type="text" value="ien116-name-servers"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	6	Domain Name Servers	<input type="text" value="domain-name-servers"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	7	Log Servers	<input type="text" value="log-servers"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	8	Cookie Servers	<input type="text" value="cookie-servers"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	9	LPR Servers	<input type="text" value="lpr-servers"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	10	Impress Servers	<input type="text" value="impress-servers"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	11	Resource Location Servers	<input type="text" value="resource-location-servers"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	12	Host Name	<input type="text" value="host-name"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	13	Boot File Size	<input type="text" value="boot-size"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	14	Merit Dump File	<input type="text" value="merit-dump"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	15	Domain Name	<input type="text" value="domain-name"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	16	Swap Server	<input type="text" value="swap-server"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	17	Root Path	<input type="text" value="root-path"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	18	Extensions Path	<input type="text" value="extensions-path"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	19	IP Forwarding Enable/Disable	<input type="text" value="ip-forwarding"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	20	Non-Local Source Routing Enable/Disable	<input type="text" value="non-local-source-routing"/>	<input type="text" value=""/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	21	Policy Filter	<input type="text" value="policy-filter"/>	<input type="text" value=""/>	<input type="checkbox"/>

Figure 5-33 DHCP Vendor Option Dictionary (partial)

Table 5-15 DHCP Vendor Option Dictionary Parameters

Field	Description
Enabled	When checked, indicates that this DHCP Option is enabled for this DHCP Product.
Code	The code or number of the option as defined by RFC2132 or an RFC draft.
Name	The name of the DHCP Option.
Option Tag	The tag for this option that is written to the configuration file when a DHCP deployment task is created.
Suffix	The suffix for this option that is written to the configuration file after the “Option Tag” and “value” have been written.
Render Definition	Toggle to render the option definition in the DHCP push. Typically used for custom definitions, since the default set are understood by default.

Adding New Options to DHCP Product

To add new DHCP options to this option set, click on the **Show all options** checkbox at the top of the screen. This displays all DHCP options that are defined within the system.

To add a new option to this DHCP Product, click the **Enabled** checkbox next to the option that you want to add to this DHCP vendor.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Removing Options from an DHCP Option List

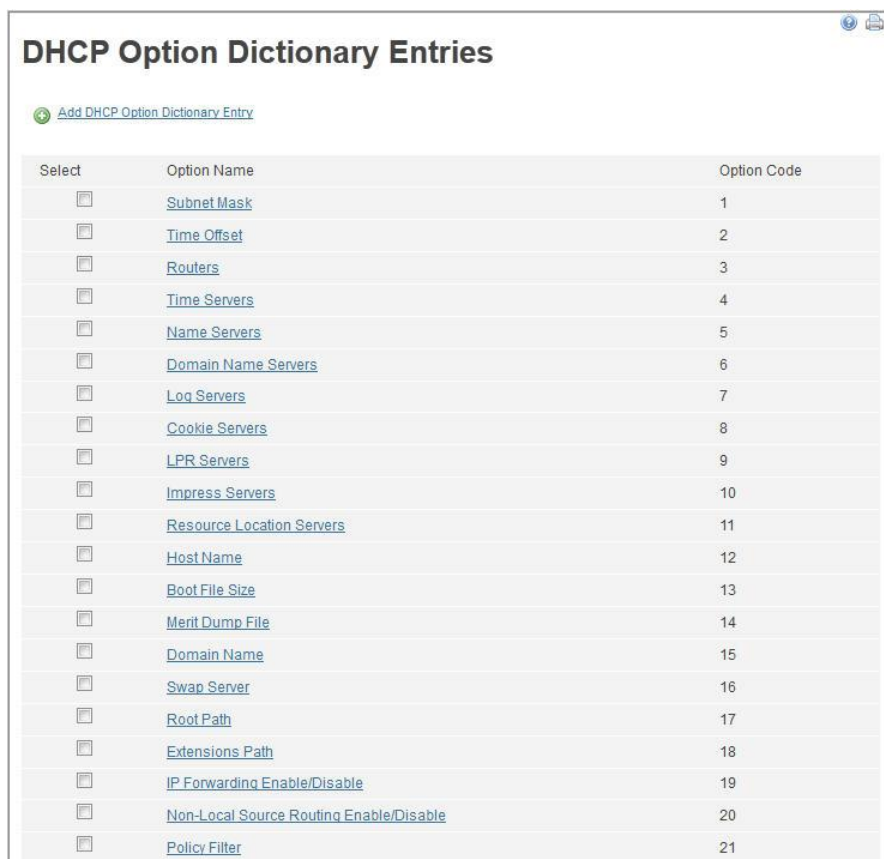
To remove options from a DHCP product, uncheck the **Enabled** checkbox next to the option that you wish to remove from this option set.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Option Master Dictionary

Use this screen to maintain DHCP Master Options within the system. Master Options are predefined with all available options that are normally configured with a DHCP server as defined by RFC2132, but may be modified for your environment.


In addition, you may add your own options if they are not already defined within the system.



Select	Option Name	Option Code
<input type="checkbox"/>	Subnet Mask	1
<input type="checkbox"/>	Time Offset	2
<input type="checkbox"/>	Routers	3
<input type="checkbox"/>	Time Servers	4
<input type="checkbox"/>	Name Servers	5
<input type="checkbox"/>	Domain Name Servers	6
<input type="checkbox"/>	Log Servers	7
<input type="checkbox"/>	Cookie Servers	8
<input type="checkbox"/>	LPR Servers	9
<input type="checkbox"/>	Impress Servers	10
<input type="checkbox"/>	Resource Location Servers	11
<input type="checkbox"/>	Host Name	12
<input type="checkbox"/>	Boot File Size	13
<input type="checkbox"/>	Merit Dump File	14
<input type="checkbox"/>	Domain Name	15
<input type="checkbox"/>	Swap Server	16
<input type="checkbox"/>	Root Path	17
<input type="checkbox"/>	Extensions Path	18
<input type="checkbox"/>	IP Forwarding Enable/Disable	19
<input type="checkbox"/>	Non-Local Source Routing Enable/Disable	20
<input type="checkbox"/>	Policy Filter	21

Figure 5-34 DHCP Option Dictionary Entries (partial)

When the DHCP Option Master Dictionary icon or link is selected, the existing DHCP Master options and associated descriptions will be shown.

To delete one or more DHCP Master options, select the checkbox beside each item you wish to clear, and click . You are prompted for confirmation. Click **OK** to delete the selected master options, or **Cancel** to return to the previous screen.

To add a DHCP Master Option, click the **Add DHCP Option Dictionary** link. The Add Master DNS Option screen appears.

Add DHCP Option Dictionary Entry

Parent Option: None

Option Name:

Short Description:

Full Description:

Option Code:

Option Value Type: --- Please Select ---

Required?: ☒

Multi-Valued?: ☒

Save Cancel

Figure 5-35 Add DHCP Option Dictionary

Table 5-16 Add DHCP Option Dictionary Parameters

Field	Description
Parent Option	Select the parent option only if this option is a suboption. None – Indicates that this is not a suboption.
Option Name	The name of the Option. This name appears in lists within the user interface.
Short Description	The short description for this option. This description appears in tooltips. Only use alphanumeric characters.
Full Description	The full description for this option. Only use alphanumeric characters.
Option Code	The numeric option code.
Option Value Type	The type of option: IP Address Numeric String Boolean IP Address Pair Hex String Composite
Minimum	Used for validation when the “Option Value Type” is Numeric. Enter the minimum allowed value for this option.
Maximum	Used for validation when the “Option Value Type” is Numeric. Enter the maximum allowed value for this option.
Required	Checked indicates that a value for this option is required.
Multi-Valued	Checked indicates that this option can have more than one value.

Once you have completed defining the DHCP option, click **Submit** to save the option, or **Cancel** to return to the previous screen. If the option was successfully added, the list shows the new option within the list.

Editing a DHCP Master Option

To modify an existing DHCP Master Option, click on the option name in the DHCP Master Option List. This takes you to the Edit DHCP Master Option screen.

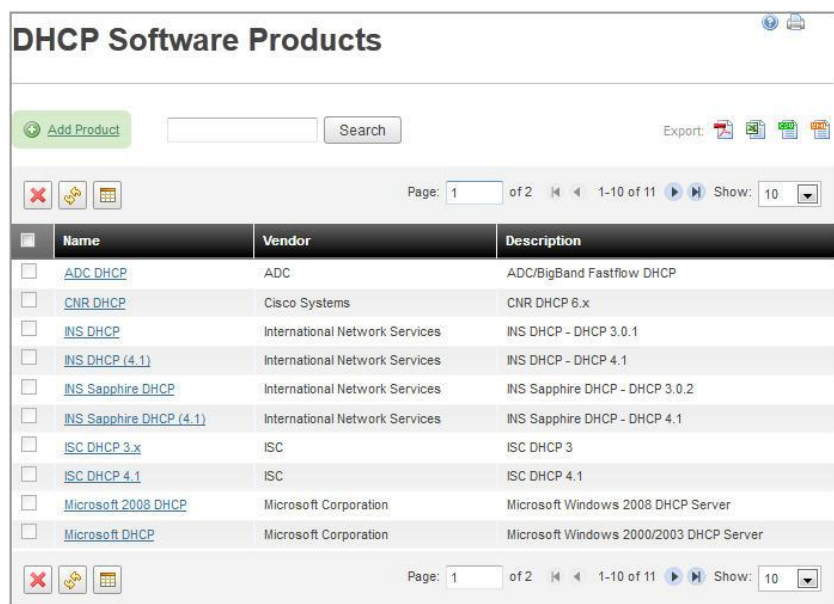
Edit the DHCP master option fields as needed. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

DHCP Software Products

Use the DHCP Software Products screen to maintain DHCP products that can be managed by IPControl. IPControl was built as a platform that can manage multiple DHCP products. This screen is used to define these products, and the attributes that are associated with them.

A set of pre-defined products are included with the system. These products include all the definitions, options, and business logic that are needed to properly manage these network services. Additional products may be added to the system, as long as these newer products are derived from existing product definitions (that is, they share the same attributes, and so on).


When you select this option, the list shown in Figure 4-56 appears:



The screenshot shows the 'DHCP Software Products' interface. At the top, there is a title bar with a search icon and a print icon. Below the title bar, there is a green 'Add Product' button, a search input field, and a 'Search' button. To the right of the search field, there are icons for 'Export', 'Print', 'PDF', 'Excel', and 'CSV'. Below the search field, there are icons for 'Delete', 'Add', and 'Edit'. The main content area is a table with the following columns: 'Name', 'Vendor', and 'Description'. The table lists several products, each with a checkbox in the first column. The products listed are: ADC DHCP (ADC), CNR DHCP (Cisco Systems), INS DHCP (International Network Services), INS DHCP (4.1) (International Network Services), INS Sapphire DHCP (International Network Services), INS Sapphire DHCP (4.1) (International Network Services), ISC DHCP 3.x (ISC), ISC DHCP 4.1 (ISC), Microsoft 2008 DHCP (Microsoft Corporation), and Microsoft DHCP (Microsoft Corporation). At the bottom of the table, there are icons for 'Delete', 'Add', and 'Edit'. Below the table, there is a pagination bar showing 'Page: 1 of 2' and '1-10 of 11'. To the right of the pagination bar, there is a 'Show:' dropdown menu set to '10'.

	Name	Vendor	Description
<input type="checkbox"/>	ADC DHCP	ADC	ADC/BigBand Fastflow DHCP
<input type="checkbox"/>	CNR DHCP	Cisco Systems	CNR DHCP 6.x
<input type="checkbox"/>	INS DHCP	International Network Services	INS DHCP - DHCP 3.0.1
<input type="checkbox"/>	INS DHCP (4.1)	International Network Services	INS DHCP - DHCP 4.1
<input type="checkbox"/>	INS Sapphire DHCP	International Network Services	INS Sapphire DHCP - DHCP 3.0.2
<input type="checkbox"/>	INS Sapphire DHCP (4.1)	International Network Services	INS Sapphire DHCP - DHCP 4.1
<input type="checkbox"/>	ISC DHCP 3.x	ISC	ISC DHCP 3
<input type="checkbox"/>	ISC DHCP 4.1	ISC	ISC DHCP 4.1
<input type="checkbox"/>	Microsoft 2008 DHCP	Microsoft Corporation	Microsoft Windows 2008 DHCP Server
<input type="checkbox"/>	Microsoft DHCP	Microsoft Corporation	Microsoft Windows 2000/2003 DHCP Server

Figure 5-36 Software Components

To delete one or more DHCP Products, select the checkbox beside each item you wish to delete, and click . You are prompted for confirmation.

Note: Make sure that this Product is not assigned to any DHCP Server (Network Service) before you delete it.

Click **OK** to delete the selected Products, or **Cancel** to return to the previous screen.

Adding a Product

To add a software product, click the **Add Product** link. The Create Product screen appears as follows:

Figure 5-37 Create Product

Table 5-17 Create Product Parameters

Field	Description
Name	The DHCP Product Name that you want to create. This is a mandatory field.
Description	A description of this product. This is an optional field.
Vendor	Select the Vendor of this product.
Type	<i>Read only.</i> DHCP is selected.
Configuration Type	Used to tell the system which type (or syntax) of configuration files should be created during a configuration/deployment task: Supported DHCP Types: <ul style="list-style-type: none"> NONE – Indicates that this product will not support the creation of DHCP configuration files. ISC – Indicates that servers that are defined as this product type utilize ISC DHCP 3.0 syntax for their configuration files.

Field	Description
Collection Type	<p>Informs the system which type of collection mechanism should be used to collect information from this service.</p> <p>Supported DNS Types:</p> <ul style="list-style-type: none"> NONE – No DNS collection will be enabled for this product. <p>Supported DHCP Types:</p> <ul style="list-style-type: none"> NONE – No DHCP collection will enabled for this product. ISC – The system will use the ISC 3.0 collection mechanism. QIP – The system will use the Alcatel-Lucent VitalQIP collection mechanism. Supported DHCP servers include the DHCP servers included with VitalQIP 5.x, and VitalQIP 6.x. CNR – The system will use the Cisco CNR collection mechanism. Supported DHCP servers include the DHCP servers included with CNR 6.x. ADC – The system will use the ADC/Bigband Fastflow collection mechanism. MSFT – The system will use the Microsoft DHCP server collection mechanism. Supported DHCP servers include Windows 2003/2008.

Fill in the appropriate fields. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Editing a Software Product

To edit the attributes of a Software product, click on the name of the product.

The Edit Product screen appears as follows.

Edit Product

Name:	INS DHCP
Description:	INS DHCP - DHCP 3.0
Vendor:	International Network Services ▼
Type:	DHCP ▼
Configuration Type:	ISC ▼
Collection Type:	ISC ▼

Edit the values for the product, as described in Table 5-17.

Once finished, click **Submit** to save all changes on this Options screen, or **Cancel** to discard all changes and return to the previous screen.

Chapter 6 Producing Reports

Reports Overview




IPControl reports are grouped into three categories:

Utilization	Audit	Other
<ul style="list-style-type: none">• Container• Subnet/Block• Low Pool	<ul style="list-style-type: none">• Container• Subnet/Block• IP/Device• Resource Record• Administrator Activity• Administrator Login	<ul style="list-style-type: none">• Tasks <i>(same as link below IPControl menu)</i>• Alerts <i>(same as link below IPControl menu)</i>• Appliance Dashboard• Logged-In Administrators• RIR Summary• SWIP/Net Name Information• About <i>(same as splash screen after initial login)</i>

Note: This chapter describes each of the reports, with the exception of About (which is previously described in “The Home Tab” on page 12).

Filters

Many reports allow you to filter the data that are displayed to suit your own requirements. When you select these reports from the **Reports** menu, the left pane displays a set of filters that allows you to select what data you want to view. Report output refreshes dynamically, based on the filter criteria you select.

You can turn filtering off and on by clicking the  icon in the report pane. Filters are also organized in a similar fashion to a folder hierarchy, so you can collapse and expand elements as required by clicking the  and  icons respectively.

Descriptions of the filter elements for each report are available throughout this chapter.

In addition to filtering the content of a report, you can change which columns appear, as well as their order sequence. Columns can be sorted and are distinguished by their black headings. For further details, refer to “Column Sorting” on page 18.

Note: Changes made to filter criteria and column selection cannot be saved for reuse at a later date. If you wish to save results of a specific criteria and column selection for analysis and review, IPControl recommends you use one of the output Export options, as described in “Exporting Output” on page 18.

Container Utilization Report

The Container Utilization Report provides summarized utilization information about specific block types within the system based on the container hierarchy. It allows you to report on the utilization within a container based on any utilization criteria that you desire.

Creating a Container Utilization Report

Note: BT Diamond IP recommends that when you create Containers, you check the **Maintain History Records** option if you want to be able to perform a Global Utilization Rollup in order to view data via the Container Utilization Report.

To create a Container Utilization Report, follow these steps.

1. Run a Global Utilization Rollup, as described in Table 3-21 on page 86.
2. Select **Container** from the UTILIZATION section of the **Reports** menu. The Filters pane and default content and layout for the Container Utilization Report open, as shown in Figure 6-1 and Figure 6-2 (page 221).

Filters

Container

Branch

Search

Total IP

IPs Available

<

% Free

<

99

Days Remaining

<

R Squared

>

Dynamic IPs Available

<

Dynamic % Free

<

Dynamic Days Remaining

<

Dynamic R Squared

>

IP Version

v4

v6

Container Type

Logical

Device

User Defined Fields

UDF Name:

-- Select UDF --

UDF Value:

Block Type

Any

Data

IPv6 Lab

Management

Video

VOIP

Figure 6-1 Container Utilization Report Filters

3. Customize the report by making selections in the Filters pane, as described in Table 6-1.

Table 6-1 Container Utilization Report Filter Elements

Filter	Description
Container	
Branch	<i>Optional.</i> Select a starting container for filtering report results. The report will be generated for this container and all of its descendants.
Total IP	
IPs Available	Select the radio button next to this option to filter the report by blocks that have less than the specified number of IP Addresses free. Enter the “Available IPs” and blocks that have the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).
% free	Select the radio button next to this option to filter the report by blocks that have less than the specified percent free space. Enter the percent free (1-100) blocks that have the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).

Container Utilization Report • 219

Filter	Description
Days Remaining and R Squared	Select the radio button next to this option to filter the report by blocks that have less than the specified days remaining before running out of address space. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>). Enter the specified days, and the correlation coefficient (r2). The correlation coefficient is between 0.0 and 1.0 and indicates the confidence in the regression. A 1.0 specifies a perfect fit. Blocks that have the specified number of days remaining with free space will be displayed in the report. This option uses the regression analysis and the forecasting algorithm that is built into IPControl.
Dynamic IPs Available	Select the radio button next to this option to filter the report by blocks that have less than the specified number of dynamic IP Addresses free. Enter the “Available IPs” and blocks that have the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).
Dynamic % Free	Select the radio button next to this option to filter the report by blocks that have less than the specified percent of dynamic free space. Enter the percent free (1-100) blocks that have the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).
Dynamic Days Remaining and Dynamic R Squared	Select the radio button next to this option to filter the report by blocks that have less than the specified days remaining before running out of dynamic address space. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>). Enter the specified days, and the correlation coefficient (r2). The correlation coefficient is between 0.0 and 1.0 and indicates the confidence in the regression. A 1.0 specifies a perfect fit. Blocks that have the specified number of days remaining with free space are displayed in the report. This option uses the regression analysis and the forecasting algorithm that is built into IPControl.
IP Version	
v6 v4	Choose whether v4 or v6 will be used as a filter.
Container Type	
Logical Device	<i>Optional.</i> Select a container type if you wish to filter report output for Logical or Device containers.
User Defined Fields	
UDF Name	Select the name of the User Defined Field to be used as a filter. Note: User defined fields are defined in the User Defined Fields tool on the Tools menu.
UDF Value	Select the value that appears in the User Defined Fields column.
Block Type	
<Site Dependent>	Select the Block Type that you want to report against. Block types are defined in the Block Types tool on the Tools menu.

Container Utilization Report Output

The default Container Utilization Report is shown in Figure 6-2.

Container	History	Interface	Total IP	In Use	Locked	IPs Available	Last Update	% Free	Dynamic % Free	R Squared	Dynamic IPs Available	Dynamic R Squared	Days Remaining	Dynamic Days Remaining	IP Version	Container Type	User Defined Fields	Block Type
InControl	History		13104	2128	2	10555	2011-12-15	80.55	74.84	0.0	6335	0.0	0	0	v4	Logical		Data
InControl	History		254	0	0	245	2011-12-15	96.46	100.0	0.0	36	0.0	0	0	v4	Logical		Video
Europe	History		254	0	0	245	2011-12-15	96.46	100.0	0.0	36	0.0	0	0	v4	Logical		Data
Americas	History		12850	2128	2	10310	2011-12-15	80.23	74.73	0.0	6299	0.0	0	0	v4	Logical		Data
Americas	History		254	0	0	245	2011-12-15	96.46	100.0	0.0	36	0.0	0	0	v4	Logical		Video
Asia	History		254	0	0	244	2011-12-15	96.06	100.0	0.0	36	0.0	0	0	v4	Logical		VOIP
U.S.	History		9040	2128	2	6755	2011-12-15	74.72	70.32	0.0	5047	0.0	0	0	v4	Logical		Data
U.S.	History		13478	4484	2	8873	2011-12-15	65.83	28.74	0.0	1809	0.0	0	0	v4	Logical		VOIP
U.S.	History		254	0	0	245	2011-12-15	96.46	100.0	0.0	36	0.0	0	0	v4	Logical		Video
Canada	History		508	0	0	460	2011-12-15	90.55	100.0	0.0	250	0.0	0	0	v4	Logical		Data

Figure 6-2 Container Utilization Report Output

Columns in the report output are described in Table 6-2.

Table 6-2 Container Utilization Report Output Elements

Field	Description
Container	The Container Name that contains the utilization criteria that you selected. Click on the link to open the Address Block Details screen for the container.
History	Click on this link to view a history graph of the utilization information for this address pool.
Interface	The interface name (if any) associated with the utilization criteria that was selected.
Total IP	The total IP addresses of this address block.
In Use	The total IP Addresses within this block that are in use.
Locked	The number of locked IP Address(es). IP Addresses that have been reported as being locked by a DHCP server during a “ping before assign” check.
IPs Available	The number of IP Addresses that are available within this block.
Last Update	The last date and time that this block was updated during a Global Utilization Rollup task.
% Free	The percent of free space available within this block.
Dynamic % Free	The percent of dynamic free space available within this block.
R Squared	Displays the correlation coefficient for predicting the number of days remaining for all IP addresses (between 0.0 and 1.0), and indicates the confidence in the regression. A 1.0 specifies a perfect fit.
Dynamic IPs Available	Indicates the number of dynamic IP addresses currently available.

Field	Description
Dynamic R Squared	Displays the correlation coefficient for predicting the number of days remaining for dynamic addresses (between 0.0 and 1.0), and indicates the confidence in the regression. A 1.0 specifies a perfect fit.
Days Remaining	Indicated the number of days remaining before running out of address space.
Dynamic Days Remaining	Indicates the number of days remaining before running out of dynamic address space. Enter the specified days, and the correlation coefficient (r2).
IP Version	Indicates whether the IP addresses are v4 or v6 format.
Container Type	Indicates whether the container is a logical or device container.
User Defined Fields	The user defined fields affiliated with this block.
Block Type	The Block type associated with this block.

Block Utilization Report

The Block Utilization Report provides utilization information about specific blocks within the system. It allows you to report on blocks based on any utilization criteria that you desire.

Creating a Block Utilization Report

Note: To run accurate Block Utilization Reports, ensure that you select **Include in Regression Analysis** and **Maintain History** in the Block Type definition, as described in Table 8-2 on page 279.

To create a Block Utilization Report, follow these steps.

1. Run a Global Utilization Rollup, as described in Table 3-21 on page 86.
2. Select **Subnet/Block** from the UTILIZATION section of the **Reports** menu. The Filters pane and default content and layout for the Block Utilization Report open, as shown in Figure 6-3 and Figure 6-4 (page 225).

Filters

☒ Block Type

☐ Any

☐ Data

☐ IPv6 Lab

☐ Management

☐ Video

☐ VOIP

☒ Total IP

☒ % Free

☐ IPs Available

☐ Days Remaining

☐ R Squared

☐ Dynamic % Free

☐ Dynamic IPs Available

☐ Dynamic Days Remaining

☐ Dynamic R Squared

Figure 6-3 Block Utilization Report Filters

3. Customize the report by making selections in the Filters pane, as described in Table 6-3.

Table 6-3 Block Utilization Report Filter Elements

Field	Description
Block Type	
<Site Dependent>	Select the Block Type that you want to report against. Block types are defined in the Block Types tool on the Tools menu.
Total IP	
% Free	Select the radio button next to this option to filter the report by blocks that have the specified percent free space. Enter the percent free (1-100) blocks that have the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).
IPs Available	Select the radio button next to this option to filter the report by blocks that have the specified number of IP Addresses free. Enter the “IPs Available” and blocks that have the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).
Days Remaining and R Squared	Select the radio button next to this option to filter the report by blocks that have the specified days remaining before running out of address space. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>). Enter the specified days, and the correlation coefficient (r2). The correlation coefficient is between 0.0 and 1.0 and indicates the confidence in the regression. A 1.0 specifies a perfect fit. Blocks that have the specified number of days remaining with free space are displayed in the report. This option uses the regression analysis and the forecasting algorithm that is built into IPControl.

Field	Description
Dynamic % free	Select the radio button next to this option to filter the report by blocks that have the specified percent free space for dynamic devices only (Manual DHCP, Automatic DHCP, and Dynamic DHCP). Enter the percent free (1-100) blocks that have the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).
Dynamic IPs Available	Select the radio button next to this option to filter the report by blocks that have the specified number of IP Addresses free for dynamic devices only (Manual DHCP, Automatic DHCP, and Dynamic DHCP). Enter the “IPs Available”, and blocks that have the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).
Dynamic Days Remaining and Correlation Coefficient	Select the radio button next to this option to filter the report by blocks that have the specified days remaining before running out of address space for dynamic devices only (Manual DHCP, Automatic DHCP, and Dynamic DHCP). You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>). Enter the specified days, and the correlation coefficient (r2). The correlation coefficient is between 0.0 and 1.0 and indicates the confidence in the regression. A 1.0 specifies a perfect fit. Blocks that have the specified number of days remaining with free space are displayed in the report. This option uses the regression analysis and the forecasting algorithm that is built into IPControl.
IP Version	
v6 v4	Choose whether v4 or v6 will be used as a filter.
User Defined Fields	
UDF Name	Select the name of the User Defined Field to be used as a filter. Note: User defined fields are defined in the User Defined Fields tool on the Tools menu.
UDF Value	Select the value that appears in the User Defined Fields column.

Block Utilization Report Output

The default Block Utilization Report is shown in Figure 6-4.

Block	History	Block Type	Total IP	In Use	Locked	IPs Available	Last Update	% Free	Dynamic % Free	R Squared	Dynamic IPs Available	Dynamic R Squared	Days Remaining	Dynamic Days Remaining	IP Version	Container	User Defined Fields
10.168.0.0/21	History	VOIP	2046	1201	0	844	2007-05-04 13:52:23.0	41	41	0.0	844	0.0	0	0	v4	ubr01.albqrg01.nm.diamondip.com	
10.168.24.0/21	History	VOIP	2046	1855	2	188	2007-05-07 15:22:53.0	9	9	0.0	188	0.0	0	0	v4	ubr02.albqrg01.nm.diamondip.com	
10.168.8.0/21	History	VOIP	2046	1428	0	617	2007-05-04 13:54:54.0	30	30	0.0	617	0.0	0	0	v4	ubr01.albqrg01.nm.diamondip.com	
10.30.1.0/24	History	VOIP	254	0	0	250	2007-05-08 14:56:27.0	98	100	0.0	0	0.0	0	0	v4	extonhub	
10.30.12.0/24	History	VOIP	254	0	0	251	2007-05-08 14:56:33.0	99	100	0.0	0	0.0	0	0	v4	extonhub	
10.30.13.0/25	History	VOIP	126	0	0	116	2011-07-12 02:14:28.0	92	100	0.0	36	0.0	-1	-1	v4	Cayman Islands	
10.30.14.0/24	History	VOIP	254	0	0	230	2011-07-13 22:43:33.0	91	100	0.0	125	0.0	-1	-1	v4	Philadelphia	
10.30.16.0/21	History	VOIP	2046	0	0	2020	2007-05-08 14:56:34.0	99	100	0.0	0	0.0	0	0	v4	extonhub	
10.30.4.0/26	History	VOIP	62	0	0	58	2007-05-08 14:56:31.0	94	100	0.0	0	0.0	0	0	v4	extonhub	
10.30.48.0/24	History	VOIP	254	0	0	243	2007-05-09 19:57:47.0	96	100	0.0	0	0.0	0	0	v4	extonhub	

Figure 6-4 Block Utilization Report Output

Columns in the report output are described in Table 6-4.

Table 6-4 Block Utilization Report Output Elements

Field	Description
Block	The Block in CIDR notation.
History	Click on this link to view a history graph of the utilization information for this address pool.
Block Type	The Block type associated with this block.
Total IP	The total IP addresses of this address block.
In Use	The total IP Addresses within this block that are in use.
Locked	The number of locked IP Address(es). IP Addresses that have been reported as being locked by a DHCP server during a “ping before assign” check.
IPs Available	The number of IP Addresses that are available within this block.
Last Update	The last date and time that this block was updated during a Global Utilization Rollup task.
% Free	The percent of free space available within this block.
Dynamic % Free	The percent of dynamic free space available within this block.

Field	Description
R Squared	Displays the correlation coefficient for predicting the number of days remaining for all IP addresses (between 0.0 and 1.0), and indicates the confidence in the regression. A 1.0 specifies a perfect fit.
Dynamic IPs Available	Indicates the number of dynamic IP addresses currently available.
Dynamic R Squared	Displays the correlation coefficient for predicting the number of days remaining for dynamic addresses (between 0.0 and 1.0), and indicates the confidence in the regression. A 1.0 specifies a perfect fit.
Days Remaining	Indicated the number of days remaining before running out of address space.
Dynamic Days Remaining	Indicates the number of days remaining before running out of dynamic address space. Enter the specified days, and the correlation coefficient (r2).
IP Version	Indicates whether the IP addresses are v4 or v6 format.
Container	Displays the containers with which a block is associated. Click on the link to open the Address Block Details screen for the container.
User Defined Fields	The User Defined Fields affiliated with this block.

Low Pool

The Low Pool Report displays the address pools or blocks that are high in utilization, and/or have a low number of IP addresses available. In order to see the most current data, you need to run a Collect DHCP Utilization task, as described in in Table 3-21 on page 86.

Creating a Low Pool Report

To create a Low Pool Report, follow these steps.

1. Run a Collect DHCP Utilization task to ensure you have the most current data.
2. Select **Low Pool** from the UTILIZATION section of the **Reports** menu. The Filters pane and default content and layout for the Low Pool Report open, as shown in Figure 6-5 and Figure 6-6 (page 228).

Filters

☒ Block Type

☐ Any

☐ Data

☐ IPv6 Lab

☐ Management

☐ Video

☐ VOIP

☒ Total IP

☐ % Free

☐ IPs Available

☐ Days Remaining

Correlation Coefficient (r2) >

☐ IP Version

☐ v4

☐ v6

Figure 6-5 Low Pool Report Filters

3. Customize the report by making selections in the Filters pane, as described in Table 6-5.

Table 6-5 Low Pool Report Filter Elements

Field	Description
Block Type	Select a specific block type to report against, or select “All Block Types”.
IP Version	Choose whether IPv4 or IPv6 is used as a filter.
Page Size	Page Size controls how many lines of the report are displayed at a time.
Percent free	Select the radio button next to this option to filter the report by blocks that have less than the specified percent free space. Enter the percent free (1-100) blocks that have less than the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).
Available IPs	Select the radio button next to this option to filter the report by blocks that have less than the specified number of IP Addresses free. Enter the “Available IPs”, and blocks that have less than the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).
Days Remaining and Correlation Coefficient	<p>Select the radio button next to this option to filter the report by blocks that have less than the specified days remaining before running out of address space. Enter the days remaining, and the correlation coefficient (r2). The correlation coefficient is between 0.0 and 1.0 and indicates the confidence in the regression. A 1.0 specifies a perfect fit. Blocks that have less than the specified number of days remaining with free space are displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).</p> <p>Note: This option uses the regression analysis and the forecasting algorithm that is built into IPControl.</p>

Low Pool Report Output

The default Low Pool Report is shown in Figure 6-6.

Pool	History	Block Type	Total IP	In Use	Locked	IPs Available	IP Version	Last Update	Container	% Free
10.168.0.0/21	History	VOIP	2046	1201	0	844	v4	2007-05-04 13:52:23.0	ubr01.albqrq01.nm.diamondip.com	41
10.168.24.0/21	History	VOIP	2046	1855	2	188	v4	2007-05-07 15:22:53.0	ubr02.albqrq01.nm.diamondip.com	9
10.168.8.0/21	History	VOIP	2046	1428	0	617	v4	2007-05-04 13:54:54.0	ubr01.albqrq01.nm.diamondip.com	30
10.30.1.0/24	History	VOIP	254	0	0	250	v4	2007-05-08 14:56:27.0	extonhub	98
10.30.12.0/24	History	VOIP	254	0	0	251	v4	2007-05-08 14:56:33.0	extonhub	99
10.30.16.0/21	History	VOIP	2046	0	0	2020	v4	2007-05-08 14:56:34.0	extonhub	99
10.30.4.0/26	History	VOIP	62	0	0	58	v4	2007-05-08 14:56:31.0	extonhub	94
10.30.48.0/24	History	VOIP	254	0	0	243	v4	2007-05-09 19:57:47.0	extonhub	96
10.30.5.0/24	History	VOIP	254	0	0	244	v4	2007-05-09 17:41:04.0	China	96
10.30.8.0/22	History	VOIP	1022	0	0	999	v4	2007-05-08 14:56:32.0	extonhub	98

Figure 6-6 Low Pool Report Output

Columns in the report output are described in Table 6-6.

Table 6-6 Low Pool Report Output Elements

Field	Description
History	Click on the link to view a history graph of the utilization information for this address pool.
Pool	The pool starting and ending IP Addresses or the shared network name.
Block Type	The Block type associated with this pool.
Total IP	The total IP addresses of this address pool.
In Use	The total IP Addresses within this pool that are in use.
Locked	The number of locked IP Addresses. IP Addresses that have been reported as being locked by a DHCP server during a “ping before assign” check.
IPs Available	The number of IP Addresses that are available within this pool.
Container	Displays the container with which a block is associated. Click on the link to open the Address Block Details screen for the container.

Field	Description
IP Version	The version of the IP (IPv4 or IPv6).
Last Update	The time the statistics were last updated.
% Free	The percent of free space available within this pool.

Container Audit Report

The Container Audit Report provides audit information about changes that have occurred within a specific container.

Creating a Container Audit Report

To create a Container Audit Report, follow these steps.

1. Select **Container** from the **AUDIT** section of the **Reports** menu. The Filters pane and default content and layout for the Container Audit Report open, as shown in Figure 6-7 and Figure 6-8 (page 230).

Figure 6-7 Container Audit Report Filters

2. Customize the report by making selections in the Filter pane, as described in Table 6-7.

Table 6-7 Container Audit Report Filters

Field	Description
Date/Time	
Start date	Select the calendar icon, and select the starting date for which to filter the audit report. The format of the start date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of start date. Select the start time using the drop-down menus.
End date	Select the calendar icon, and select the ending date for which to filter the audit report. The format of the end date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of end date. Select the end time using the drop-down menus.
Admin	

Field	Description
<Site Dependent>	Select the administrators that you want to filter the report against.

Container Audit Report Output

The default Container Audit Report is shown in Figure 6-8.

The screenshot shows the 'Container Audit Report' window. It includes a search bar, export options, and a table of audit events. The table has five columns: Date/Time, Admin, Container, Event Type, and Additional Info. The data shows various 'Add Block' events for different containers and IP ranges.

Date/Time	Admin	Container	Event Type	Additional Info
2007-05-03 13:38:44.0	incadmin	Americas	Add Block Americas Aggregate	
2007-05-03 13:39:47.0	incadmin	Americas	Add Block 4FFE:DAF0::/40	
2007-05-03 13:40:22.0	incadmin	Asia	Add Block 4FFE:DAF0:8000::/40	
2007-05-03 13:40:55.0	incadmin	Europe	Add Block 4FFE:DAF0:C000::/40	
2007-05-03 13:42:51.0	incadmin	U.S.	Add Block US Aggregate	
2007-05-03 13:47:54.0	incadmin	ubr01.albqrq01.nm.diamondip.com	Add Block 68.32.100.0/22	
2007-05-03 13:50:55.0	incadmin	ubr01.albqrq01.nm.diamondip.com	Add Block 68.35.112.0/22	
2007-05-04 07:51:45.0	incadmin	Americas	Add Block 10.168.0.0/13	
2007-05-04 07:52:25.0	incadmin	ubr01.albqrq01.nm.diamondip.com	Add Block 10.168.0.0/21	
2007-05-04 07:54:54.0	incadmin	ubr01.albqrq01.nm.diamondip.com	Add Block 10.168.8.0/21	

Figure 6-8 Container Audit Report Output

Columns in the report output are described in Table 6-8.

Table 6-8 Container Audit Report Output Elements

Field	Description
Date/Time	The date and time that the audit event took place.
Admin	The administrator that initiated the event.
Container	The container that this event occurred in.
Event Type	The event type that took place: Create Container – A container was created Modify Container – A container was changed Delete Container – A container was deleted Add Block – a block has been added to this container Delete Block – a block has been deleted from this container.
Additional Information	Displays updated information: Admin, From and To values.

Block Audit Report

The Block Audit Report provides audit information about changes that have occurred to a specific block.

Creating a Block Audit Report

To create a Block Audit Report, follow these steps.

- 1. Select **Subnet/Block** from the AUDIT section of the **Reports** menu. The Filters pane and default content and layout for the Block Audit Report open, as shown in Figure 6-9 and Figure 6-10 (page 232).

Filters

Date/Time

Start Date

01

:

00

AM

(hh:mm)

End Date

01

:

00

AM

(hh:mm)

Admin

asiaadmin

incadmin

subadmin

Block Size

Select Block Size: -- Select All --

IP Version

v4

v6

Reason Code

Select Reason Code: -- Select All --

Figure 6-9 Block Audit Report Filters

- 2. Customize the report by making selections in the Filter pane, as described in Table 6-9.

Table 6-9 Block Audit Report Filter Elements

Field	Description
Date/Time	
Start date	Select the calendar icon, and select the starting date for which to filter the audit report. The format of the start date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of start date. Select the start time using the drop-down menus.
End date	Select the calendar icon, and select the ending date for which to filter the audit report. The format of the end date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of end date. Select the end time using the drop-down menus.
Admin	
<Site Dependent>	Select the administrators that you want to filter the report against.
Block Size	
Selected Block Size	Select the size of the block in CIDR notation from the drop-down list, or leave at Select All to display all blocks.
IP Version	Choose whether v4 or v6 will be used as a filter.
Reason Code	Select one of the Allocation Reason Codes, defined in Allocation Reason Codes in the SUBNET/BLOCK section of the Tools menu.

Block Audit Report Output

The default Block Audit Report is shown in Figure 6-10.

Date/Time	Admin	Block	Block Size	Event Type	IP Version	Reason Code	Additional Info
2007-05-03 13:11:03.0	incadmin	68.32.0.0/11	11	Create	v4		
2007-05-03 13:11:47.0	incadmin	10.0.0.0/8	8	Create	v4		
2007-05-03 13:13:17.0	incadmin	69.177.0.0/16	16	Create	v4		
2007-05-03 13:13:54.0	incadmin	4ffe:dafo::/32	32	Create	v6		
2007-05-03 13:38:44.0	incadmin	68.32.0.0/13	13	Create	v4		
2007-05-03 13:39:48.0	incadmin	4ffe:dafo::/40	40	Create	v6		
2007-05-03 13:40:22.0	incadmin	4ffe:dafo:8000::/40	40	Create	v6		
2007-05-03 13:40:55.0	incadmin	4ffe:dafo:c000::/40	40	Create	v6		
2007-05-03 13:42:51.0	incadmin	68.32.0.0/14	14	Create	v4		
2007-05-03 13:47:54.0	incadmin	68.32.100.0/22	22	Create	v4		

Figure 6-10 Block Audit Report Output

Columns in the report output are described in Table 6-10.

Table 6-10 Block Audit Report Output Elements

Field	Description
Date/Time	The date and time that the audit event took place.
Admin	The administrator that initiated the event.
Block	The block on which this event occurred.
Block Size	The size of the block in CIDR notation.
Event Type	The event type that took place: Create – a block has been added Delete – a block has been deleted Update – a block has been updated
IP Version	Displays v4 or v6.
Reason Code	Displays an Allocation Reason Code.
Additional Info	Additional information related to the specific task, such as Base Allocation, and Internal Web Request.

Device Audit Report

The Device Audit Report provides audit information about changes that have occurred to a specific device. You may run this report for a specific IP Address or a specific MAC Address.

Creating a Device Audit Report

To create a Block Audit Report, follow these steps.

- 1. Select **IP/Device** from the AUDIT section of the **Reports** menu. The Filters pane and default content and layout for the Device Audit Report open, as shown in Figure 6-11 and Figure 6-12 (page 234).

Filters

Date/Time

Start Date

01

:

00

AM

(hh:mm)

End Date

01

:

00

AM

(hh:mm)

Admin

asiaadmin

incadmin

subadmin

IP Address

Enter IP Address:

Is Exactly

Hardware Address

Enter Hardware Address:

Is Exactly

Figure 6-11 Device Audit Report Filters

- 2. Customize the report by making selections in the Filter pane, as described in Table 6-11.

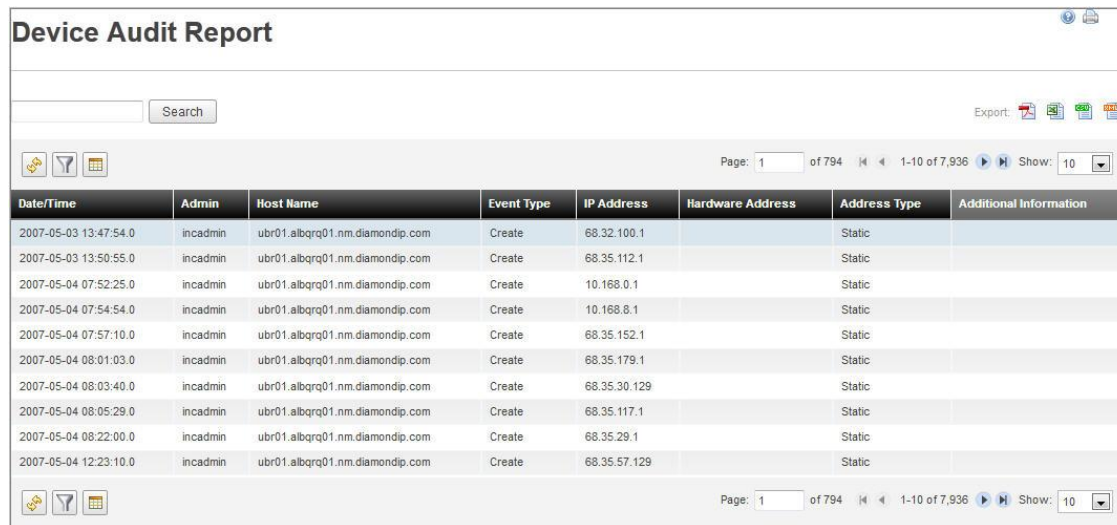
Table 6-11 Device Audit Report Filter Elements

Field	Description
Date/Time	
Start date	Select the calendar icon, and select the starting date for which to filter the audit report. The format of the start date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of start date. Select the start time using the drop-down menus.
End date	Select the calendar icon, and select the ending date for which to filter the audit report. The format of the end date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of end date. Select the end time using the drop-down menus.
Admin	
<Site Dependent>	Select the administrators that you want to filter the report against.
IP Address	
Enter IP Address	Enter the IP Address to display audit information. You can use the default criterion of an exact match (Is Exactly), or use the drop-down to select Begins with or Contains .
Hardware Address	
Enter Hardware Address	Enter the hardware address (MAC Address) to display audit information. You can use the default criterion of an exact match (Is Exactly), or use the drop-down to select Begins with or Contains .

Device Audit Report • 233

Device Audit Report Output

The default Device Audit Report is shown in Figure 6-12.



The screenshot shows the 'Device Audit Report' window. It includes a search bar, export options (PDF, CSV, XLS, HTML), and pagination controls. The main table displays audit events with the following columns: Date/Time, Admin, Host Name, Event Type, IP Address, Hardware Address, Address Type, and Additional Information. The table shows 10 events, all of type 'Create', initiated by 'incadmin' for the host 'ubr01.albqrq01.nm.diamondip.com'.

Date/Time	Admin	Host Name	Event Type	IP Address	Hardware Address	Address Type	Additional Information
2007-05-03 13:47:54.0	incadmin	ubr01.albqrq01.nm.diamondip.com	Create	68.32.100.1		Static	
2007-05-03 13:50:55.0	incadmin	ubr01.albqrq01.nm.diamondip.com	Create	68.35.112.1		Static	
2007-05-04 07:52:25.0	incadmin	ubr01.albqrq01.nm.diamondip.com	Create	10.168.0.1		Static	
2007-05-04 07:54:54.0	incadmin	ubr01.albqrq01.nm.diamondip.com	Create	10.168.8.1		Static	
2007-05-04 07:57:10.0	incadmin	ubr01.albqrq01.nm.diamondip.com	Create	68.35.152.1		Static	
2007-05-04 08:01:03.0	incadmin	ubr01.albqrq01.nm.diamondip.com	Create	68.35.179.1		Static	
2007-05-04 08:03:40.0	incadmin	ubr01.albqrq01.nm.diamondip.com	Create	68.35.30.129		Static	
2007-05-04 08:05:29.0	incadmin	ubr01.albqrq01.nm.diamondip.com	Create	68.35.117.1		Static	
2007-05-04 08:22:00.0	incadmin	ubr01.albqrq01.nm.diamondip.com	Create	68.35.29.1		Static	
2007-05-04 12:23:10.0	incadmin	ubr01.albqrq01.nm.diamondip.com	Create	68.35.57.129		Static	

Figure 6-12 Device Audit Report Output

Columns in the report output are described in Table 6-12.

Table 6-12 Device Audit Report Output Screen Elements

Field	Description
Date/Time	The date and time that the audit event took place.
Admin	The administrator that initiated the event.
Host Name	The host name for this device.
Event Type	The event type that took place: Create , Delete , or Modify
IP Address	The IP Address for this device.
Hardware Address	The MAC Address for this device.
Address Type	The Address type that was assigned to this device when the audit record was created.
Additional Information	Additional information related to the specific task.

Resource Record Audit Report

The Resource Record Audit Report provides audit information about changes that have occurred to DNS Resource Records. You may run this report for a specific FQDN, DNS Owner, and Resource Record Type.

Creating a Resource Record Audit Report

- 1. Select **Resource Record** from the AUDIT section of the **Reports** menu. The Filters pane and default content and layout for the Resource Record Audit Report open, as shown in Figure 6-13 and Figure 6-14 (page 236).

Filters

Date/Time

Start Date

01

00

AM

(hh:mm)

End Date

01

00

AM

(hh:mm)

Admin

asiaadmin

incadmin

subadmin

FQDN

Is Exactly

Owner

Is Exactly

RR Type

Data

Is Exactly

IP Address

Figure 6-13 Resource Record Audit Report Filters

- 2. Customize the report by making selections in the Filter pane, as described in Table 6-13.

Table 6-13 Resource Record Audit Report Filter Elements

Field	Description
Date/Time	
Start date	Select the calendar icon, and select the starting date for which to filter the audit report. The format of the start date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of start date. Select the start time using the drop-down menus.
End date	Select the calendar icon, and select the ending date for which to filter the audit report. The format of the end date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of end date. Select the end time using the drop-down menus.
Admin	
<Site Dependent>	Select the administrators that you want to filter the report against.
FQDN	Enter the Fully Qualified Domain Name (Host name.domain name) of the resource records for which you want to display audit information. You can use the default criterion of an exact match (Is Exactly), or use the drop-down to select Begins with or Contains .
Owner	Enter the DNS “Owner” field, as specified in DNS Resource Record definitions, that will be used to display audit information. You can use

Field	Description
	the default criterion of an exact match (Is Exactly), or use the drop-down to select Begins with or Contains .
RR Type	Enter the Resource Record Type (that is, A, PTR, CNAME, and so on) if you are trying to limit the report to a specific Resource Record Type.
Data	Enter the DNS “RData” field, as specified in DNS Resource Record definitions, that will be used to display audit information. You can use the default criterion of an exact match (Is Exactly), or use the drop-down to select Begins with or Contains .
IP Address	Enter the IP Address for which to display audit information. You should only use this filter for A and PTR records.

Resource Record Audit Report Output

The default Resource Record Audit Report is shown in Figure 6-14.

Resource Record Audit Report

Search

Export:    

Page: 1 of 451 1-10 of 4,504 Show: 10

Date/Time	Admin	FQDN	Event Type	Domain	Owner	RR Type	Data	IP Address	Additional Information Type
2007-05-08 08:45:50.0	incadmin	router-172-16-0-2.diamondip.com.	Create	diamondip.com. (Default)	router-172-16-0-2	A	172.16.0.2	172.16.0.2	
2007-05-08 08:45:50.0	incadmin	2.0.16.172.in-addr.arpa.	Create	0.16.172.in-addr.arpa. (Asia)	2	PTR	router-172-16-0-2.diamondip.com.	172.16.0.2	
2007-05-08 08:45:50.0	incadmin	router-172-16-0-3.diamondip.com.	Create	diamondip.com. (Default)	router-172-16-0-3	A	172.16.0.3	172.16.0.3	
2007-05-08 08:45:50.0	incadmin	3.0.16.172.in-addr.arpa.	Create	0.16.172.in-addr.arpa. (Asia)	3	PTR	router-172-16-0-3.diamondip.com.	172.16.0.3	
2007-05-08 08:45:51.0	incadmin	router-172-16-0-4.diamondip.com.	Create	diamondip.com. (Default)	router-172-16-0-4	A	172.16.0.4	172.16.0.4	
2007-05-08 08:45:51.0	incadmin	4.0.16.172.in-addr.arpa.	Create	0.16.172.in-addr.arpa. (Asia)	4	PTR	router-172-16-0-4.diamondip.com.	172.16.0.4	
2007-05-08 08:45:51.0	incadmin	prtr-00000.diamondip.com.	Create	diamondip.com. (Default)	prtr-00000	A	172.16.0.5	172.16.0.5	
2007-05-08 08:45:51.0	incadmin	5.0.16.172.in-addr.arpa.	Create	0.16.172.in-addr.arpa. (Asia)	5	PTR	prtr-00000.diamondip.com.	172.16.0.5	
2007-05-08 08:45:51.0	incadmin	prtr-00001.diamondip.com.	Create	diamondip.com. (Default)	prtr-00001	A	172.16.0.6	172.16.0.6	
2007-05-08 08:45:51.0	incadmin	6.0.16.172.in-addr.arpa.	Create	0.16.172.in-addr.arpa. (Asia)	6	PTR	prtr-00001.diamondip.com.	172.16.0.6	

Page: 1 of 451 1-10 of 4,504 Show: 10

Figure 6-14 Resource Record Audit Report Output

Columns in the report output are described in Table 6-14.

Table 6-14 Resource Record Audit Report Output Elements

Field	Description
Date/Time	The date and time that the audit event took place.

Field	Description
Admin	The administrator that initiated the event.
FQDN	The Fully Qualified Domain Name for this record.
Event Type	The event type that took place: Create, Delete, Update, Pending Create, Pending Delete, Pending Update, Create Approved, Update Approved, Delete Approved.
Domain	The Domain where this Resource Record is assigned.
Owner	The DNS “Owner” Information of this record.
RR Type	The DNS Resource Record Type of this device.
Data	The DNS “RData” Information of this record.
IP Address	The IP Address for this device.
Additional Information	Additional information related to the specific task.

Administrator Audit Report

The Administrator Audit Report provides a combined view of the audit activities from all the other audit reports. It allows you to see all the activities of a user from login to logoff or all the changes made to the system for a particular time.

Creating an Administrator Audit Report

1. Select **Administrator Activity** from the AUDIT section of the **Reports** menu. The Filters pane and default content and layout for the Administrator Audit Report open, as shown in Figure 6-15 and Figure 6-16 (page 238).

Figure 6-15 Administrator Audit Report Filters

2. Customize the report by making selections in the Filter pane, as described in Table 6-15

Table 6-15 Administrator Audit Report Filter Elements

Field	Description
Date/Time	

Start date	Select the calendar icon, and select the starting date for which to filter the audit report. The format of the start date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of start date. Select the start time using the drop-down menus.
End date	Select the calendar icon, and select the ending date for which to filter the audit report. The format of the end date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of end date. Select the end time using the drop-down menus.
Admin	
<Site Dependent>	Select the administrators that you want to filter the report against.

Administrator Audit Report Output

The default Administrator Audit Report is shown in Figure 6-16.

Date/Time	Admin	Scope	Event Type	Details
2007-05-03 12:58:29.0	incadmin	Container	Create	Container Additional Info Europe
2007-05-03 12:58:41.0	incadmin	Container	Create	Container Additional Info Americas
2007-05-03 12:58:51.0	incadmin	Container	Create	Container Additional Info Asia
2007-05-03 12:59:21.0	incadmin	Container	Create	Container Additional Info U.S.
2007-05-03 12:59:32.0	incadmin	Container	Create	Container Additional Info Canada
2007-05-03 13:00:11.0	incadmin	Container	Create	Container Additional Info Caribbean
2007-05-03 13:00:32.0	incadmin	Container	Create	Container Additional Info China
2007-05-03 13:00:48.0	incadmin	Container	Create	Container Additional Info Japan
2007-05-03 13:00:58.0	incadmin	Container	Create	Container Additional Info Australia
2007-05-03 13:01:06.0	incadmin	Container	Create	Container Additional Info UK

Figure 6-16 Administrator Audit Report Output

Columns in the report output are described in Table 6-16.

Table 6-16 Administrator Audit Report Output Screen Elements

Field	Description
Date/Time	The date and time that the audit event took place.

Field	Description
Admin	The administrator that initiated the event.
Scope	Categorization based on the area of activity. For example: Changes to container have the scope container Changes to device are under device scope. The sub-columns under Details change based on the scope.
Event Type	The event type that took place: Login, Logoff, Create, Add Block, Update and so on.
Details	Details column has sub-columns based on the scope and provides additional information related to the activity. For example: Login scope has Session ID and Client IP Address sub-columns under Details. Container scope has Container Name and Additional Info sub-columns.

Login Audit Report

The Login Audit Report provides audit information about system access activities like login, logout, session timeout, and so on.

Creating a Login Audit Report

1. Select **Administrator Login** from the AUDIT section of the **Reports** menu. The Filters pane and default content and layout for the Login Audit Report open, as shown in Figure 6-17 and Figure 6-18 (page 240).

Filters

☒ Date/Time

Start Date: 01 : 00 AM (hh:mm)

End Date: 01 : 00 AM (hh:mm)

☒ Admin

☐ asiaadmin

☐ incadmin

☐ subadmin

Figure 6-17 Login Audit Report Filters

2. Customize the report by making selections in the Filter pane, as described in Table 6-17.

Table 6-17 Login Audit Report Filter Elements

Field	Description
Date/Time	
Start date	Select the calendar icon, and select the starting date for which to filter the audit report. The format of the start date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of start date. Select the start time using the drop-down menus.
End date	Select the calendar icon, and select the ending date for which to filter the audit report. The format of the end date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of end date. Select the end time using the drop-down menus.
Admin	
<Site Dependent>	Select the administrators that you want to filter the report against.

Login Audit Report Output

The default Login Audit Report is shown in Figure 6-18.

Login Audit Report

Search [] Export [PDF] [Excel] [CSV] [HTML]

Page: 1 of 35 1-10 of 342 Show: 10

Date/Time	Admin	Event Type	Session ID	Client IP Address
2011-05-20 12:51:03.0	incadmin	Logoff	6081EC80F4D469EF56B3F81A83FC231E	
2011-05-20 12:51:12.0	incadmin	Authentication failed	3E9CD4138D2DE11B87E21205F173D981	127.0.0.1
2011-05-20 12:51:19.0	incadmin	License key expired	3E9CD4138D2DE11B87E21205F173D981	127.0.0.1
2011-05-20 12:51:32.0	incadmin	Logoff	3E9CD4138D2DE11B87E21205F173D981	
2011-05-20 12:51:37.0	incadmin	Login	FFA99250EF5A3D7D38DFF09E7D36D2A	127.0.0.1
2011-05-20 13:57:08.0	incadmin	Logoff	FFA99250EF5A3D7D38DFF09E7D36D2A	
2011-05-20 13:57:21.0	incadmin	Login	C84A3F7F78BC2B503CA6A36916691901	127.0.0.1
2011-05-20 14:41:39.0	incadmin	Session timed out	C84A3F7F78BC2B503CA6A36916691901	
2011-05-20 14:42:57.0	incadmin	Login	ED118FB299224383C9017178BE14C24A	127.0.0.1
2011-05-22 07:09:17.0	incadmin	Session timed out	ED118FB299224383C9017178BE14C24A	

Page: 1 of 35 1-10 of 342 Show: 10

Figure 6-18 Login Audit Report Output

Columns in the report output are described in Table 6-18.

Table 6-18 Login Audit Report Output Elements

Field	Description
Date/Time	The date and time that the audit event took place.
Admin	The administrator that initiated the event.
Event Type	The event type that took place: Login, Logoff, Session timed out
Session ID	Session ID associated with this particular session. This is useful when

Field	Description
	an admin has multiple application sessions open.
Client IP Address	IP address of the client or last proxy that the Admin logged in from.

Tasks

The **Tasks** option allows you to view and manage tasks that have been created in the system. You may use this option to view the status of the tasks, as well as view specific results from the task itself.

The reports that are created in the task display provide you with planned vs. actual views of the configuration (IP Address space allocations) to your network services and network elements.

Tasks Screen Layout

When you select **Tasks** from the OTHER section of the **Reports** menu, a Filters pane appears in the left pane, as shown in Figure 6-19, and a view of your tasks is displayed within the main browser window, as shown in Figure 6-20 (page 243).

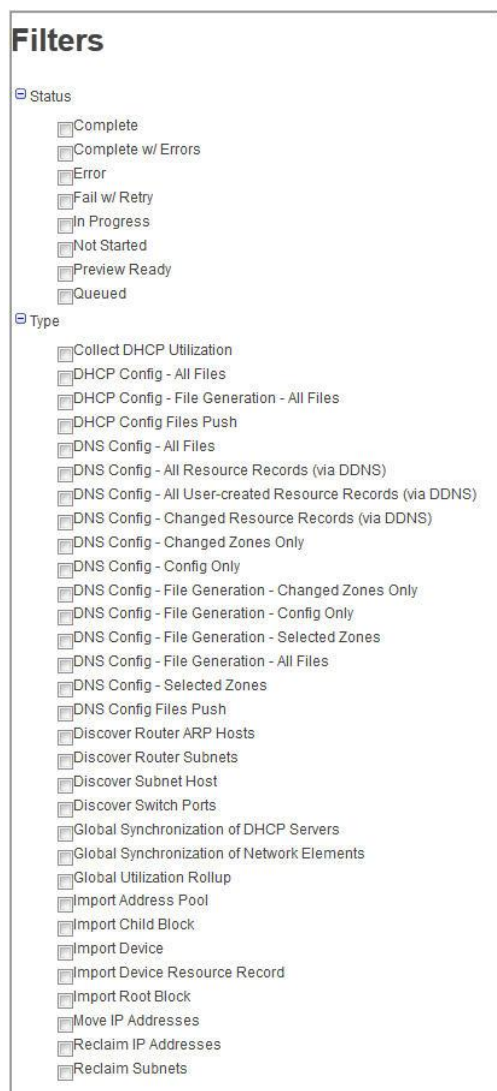










Figure 6-19 Tasks Filter

Tasks




















Search





Refresh: Off

Export:    


Page: 1 of 2 1-10 of 17 Show: 10

ID	Status	Start Time	Completed Time	Scheduled	Scope	Type	Admin
 Task 39	Not Started	2011-12-04 16:50:00.0		Sched		Import Root Block	InControl Administrator
 Task 40	 Queued	2011-12-04 15:35:07.0		Immed		Import Root Block	InControl Administrator
 Task 38	 Complete	2008-10-08 14:21:08.0	2008-10-08 14:21:30.0	Immed		Global Utilization Rollup	InControl Administrator
 Task 36	 Preview Ready	2007-05-11 08:42:28.0	2007-05-11 08:42:49.0	Immed	sapphire1.diamondip.com	DNS Config - All Files	InControl Administrator
 Task 35	 In Progress	2007-05-09 14:14:24.0		Immed		Global Utilization Rollup	InControl Administrator
 Task 34	 Complete	2007-05-09 14:00:56.0	2007-05-09 14:01:09.0	Immed	exton-sw01.diamondip.com	Discover Switch Ports	InControl Administrator
 Task 32	 Preview Ready	2007-05-09 13:18:21.0	2007-05-09 13:18:39.0	Immed	ns1-jp.diamondip.com	DNS Config - All Files	InControl Administrator
 Task 30	 Preview Ready	2007-05-09 13:17:50.0	2007-05-09 13:18:08.0	Immed	dhcp1.sw.diamondip.com	DHCP Config - All Files	InControl Administrator
 Task 29	 Fail w/ Retry	2007-05-09 13:17:05.0	2007-05-09 13:17:08.0	Immed	wayne-sw01.diamondip.com	Discover Switch Ports	InControl Administrator
 Task 27	 Preview Ready	2007-05-09 13:13:16.0	2007-05-09 13:13:33.0	Immed	sapphire1.diamondip.com	DNS Config - Config Only	InControl Administrator


   

Page: 1 of 2 1-10 of 17 Show: 10

Figure 6-20 Task List

To delete tasks, select the checkbox next to the task ID you want to delete and click .

To refresh, choose from the following actions.

- To refresh immediately, click .
- To select other refresh intervals, select an interval from the **Refresh** drop-down list:

Refresh:

Off

Off30 seconds60 seconds90 seconds2 minutes5 minutes10 minutes

Figure 6-21 Refresh Intervals

You can also sort most columns by clicking on the column header. Columns in the report output are described in Table 6-19.

Table 6-19 Task List Screen Elements

Field	Description
ID	A unique task id that is assigned by the system.

Field	Description
Status	Graphical representation of the status of the task. White –Task has not yet started. Black –Task is complete. Red – An error has occurred. Yellow – Task has been queued. Green – Task is in progress. Flag – Task is complete with errors Magnifier – Configuration files can be viewed.
Select	Check this box to select this task for deletion.
Start Time	The date and time that the task started.
Completed Time	The date and time that the task completed.
Scheduled	The scheduled interval for the task to run (Immediate, Scheduled, or recurring).
Scope	Task type specific; the specific scope for this task. Depending upon which type of task this is, this could be the network service or network element.
Type	The type of task.
Admin	Identifies the administrator who initiated the task.

Task Details

When you click on the **Task ID** link on a specific task in the task list, the task details are displayed as shown below. This display shows you summary information about the task, such as how long the task took to run.

Task 38 Summary

ID	38
Type	Global Utilization Rollup
Scope	
Status	Complete
Hold files for preview:	<input type="checkbox"/>
Administrator	incadmin
Start Time	10/08/08 2:21 PM
Completed Time	10/08/08 2:21 PM
Duration	00:00:22

Results:

Time	Result Level	Text
10/08/08 2:21 PM	INFO	Block Utilization Totals: NumAllocated=24646, NumAssigned=11028, SubnetLoss=88
10/08/08 2:21 PM	INFO	Container Utilization: 18 Containers Processed
10/08/08 2:21 PM	INFO	Total Homes Passed: 0
10/08/08 2:21 PM	INFO	Address Pool History: 39 Pool History records created.
10/08/08 2:21 PM	INFO	Block History: 308 Block History records created.
10/08/08 2:21 PM	INFO	Container History: 64 Container History records created.
10/08/08 2:21 PM	INFO	GlobalRollup completed successfully.
10/08/08 2:21 PM	INFO	Block Utilization Totals: NumAllocated=24646, NumAssigned=11028, SubnetLoss=88
10/08/08 2:21 PM	INFO	Container Utilization: 18 Containers Processed
10/08/08 2:21 PM	INFO	Total Homes Passed: 0

14 items found, displaying 1 to 10. [First/Prev] 1, 2 [Next/Last]

[Back to Task List](#) Page Size 10

Figure 6-22 Task Summary

Click **Back to Task List** to return to the task list display.

Locate Queued/In-Progress Task Messages

For tasks with a status of Queued or In Progress, the Task Details page provides a troubleshooting button for locating task messages within the IPControl task and result queues.

The status of each message located within the task and result queues is displayed in the corresponding read-only text area. If multiple lines are displayed, then more than one message was found. The following is a list of the message statuses that can appear.

- Task has not started.
No queued messages exist for tasks that have not started.
- Task has completed.
No queued messages exist for tasks that have completed.
- No task messages found for ID=###
If this is a parent task, check the child tasks. If this is a child task, the Agent is working on it. No queued messages exist for parent tasks.

- Queued(ActiveMQ) for 3.x Agent: x.x.x.x
A task message has been posted to the ActiveMQ task queue, and the message is waiting for the IPControl 3.x Agent identified by IP address ‘x.x.x.x’ to process the message.
- Queued(ActiveMQ) for 3.x Result Manager
A result message has been posted by the IPControl 3.x Agent that was responsible for the task, and the message is waiting for the IPControl 3.x Result Manager to process the message.

Previewing Configuration Files

When you click on the **Details** link for a task with status “Preview Ready”, the child task details are displayed. When you click on the **Details** link for that child task, the task summary results section includes a list of configuration and zone files that were created.

To view a file, select either the **PDF** or **Text** link for that file. A new window displays the file contents in the format you selected. The **Deploy** button enables you to continue the deploy process using the files held for preview.

Alert Log

The Alert Log informs the administrator of thresholds that have been crossed in the system. Use this screen to view, search, or delete outstanding alerts.

Working with the Alert Log

1. To work with the Alert Log, select **Alerts** from the OTHER sections of the **Reports** menu, or simply click the **Alerts** link below the IPControl logo. The Filters pane and default content and layout for the Alert Log open, as shown in Figure 6-1 and Figure 6-2 (page 221).

Filters

Date/Time

Start Date

01

:

00

AM

(hh:mm)

End Date

01

:

00

AM

(hh:mm)

Severity

☐Critical

☐Warning

☐Info

Figure 6-23 Alert Log Filter





Table 6-20 Alert Log Filter Elements





Field	Description
Date/Time	
Start Date	Fill in this field to limit the output to alerts raised after this date and

Field	Description
	time.
End Date	Fill in this field to limit the output to alerts raised before this date and time.
Severity	Select from the following choices: <ul style="list-style-type: none">CriticalWarningInfo











Alert Log





Search

Export:    

Page: 1 of 512 1-10 of 5,116 Show: 10

	Date/Time	Severity	Object	Criteria	Observed Value	Confidence
<input type="checkbox"/>	2008-10-08 16:21:18.0		dhcp1.sw.diamondip.com: 10.168.24.2-10.168.31.254	assigned is greater than 70%	91	0.0
<input type="checkbox"/>	2008-10-08 16:21:19.0		dhcp1.sw.diamondip.com: 10.168.24.2-10.168.31.254	assigned is greater than 85%	91	0.0
<input type="checkbox"/>	2008-10-08 16:21:21.0		dhcp1.sw.diamondip.com: ubr01-a.albqrq01-shared	assigned is greater than 70%	96	0.0
<input type="checkbox"/>	2008-10-08 16:21:21.0		dhcp1.sw.diamondip.com: ubr01-a.albqrq01-shared	assigned is greater than 85%	96	0.0
<input type="checkbox"/>	2008-10-08 16:21:21.0		dhcp1.sw.diamondip.com: ubr01-a.albqrq01-shared	assigned is greater than 95%	96	0.0
<input type="checkbox"/>	2008-10-08 16:21:21.0		dhcp1.sw.diamondip.com: ubr01-b.albqrq01-shared	assigned is greater than 70%	94	0.0
<input type="checkbox"/>	2008-10-08 16:21:21.0		dhcp1.sw.diamondip.com: ubr01-b.albqrq01-shared	assigned is greater than 85%	94	0.0
<input type="checkbox"/>	2008-10-08 16:21:22.0		dhcp1.sw.diamondip.com: ubr02-a.albqrq01-shared	assigned is greater than 70%	95	0.0
<input type="checkbox"/>	2008-10-08 16:21:22.0		dhcp1.sw.diamondip.com: ubr02-a.albqrq01-shared	assigned is greater than 85%	95	0.0
<input type="checkbox"/>	2008-10-08 16:21:22.0		dhcp1.sw.diamondip.com: ubr02-b.albqrq01-shared	assigned is greater than 70%	73	0.0




   

Page: 1 of 512 1-10 of 5,116 Show: 10

Figure 6-24 Alerts Output

Columns in the report output are described in Table 6-21.

Table 6-21 Output Fields

Field	Description
(Untitled First Column)	Indicates the severity of the Alert.
Selected	Check the box in this column for delete operations.
Date/Time	The Date and Time the alert was raised.
Severity	Displays icons that indicate the severity of the alert: <ul style="list-style-type: none"> Information Warning Error
Object	Displays the Object that raised the Alert. A Container alert shows the container name, followed by the Block

Field	Description
	Type specified on the Threshold. The container name displayed as a fully qualified path from the root of the container true. An Interface Alert shows the Device container name, followed by the Interface name, followed by the block type configured on the Threshold. A Block Alert shows the name of the Block in CIDR notation. A Network Service alert shows the name of the Network Service, followed by Address Pool or Address Pool share name that raised the alert.
Criteria	The Criteria that caused the alert.
Observed Value	The Value that caused the alert.
Confidence	The Confidence value if Criteria tested “Days Left”

Appliance Dashboard

The Appliance Dashboard allows the administrator to view the status of all Sapphire Appliances. The dashboard provides different icons to indicate the status of the appliance and the services hosted by the appliance. In addition, the dashboard includes links to manage the appliance and its services and to view all detailed event messages related to each appliance.

Name	IP	System	IP Control	DNS	DHCP	Status Check	Actions
sapphire1.diamondip.com	10.30.8.200						Details Manage
sapphire2.diamondip.com	10.30.4.199						Details Manage
sapphire3.diamondip.com	10.92.172.36						Details Manage
sapphire4.diamondip.com	192.168.196.20					2011-10-21 09:47:02.0	Details Manage

- Connected / running
 - Disconnected or down
 - Hot / In stand by
 - Unknown / Unreachable
 - Found unconfigured service running
 - Hardware problem (cursor over for details)

Figure 6-25 Appliance Dashboard







Columns in the dashboard are described in Table 6-22. Further explanation of the system icons is available in Table 6-23.

Table 6-22 Appliance Dashboard Columns

Field	Description
Name	The name of the appliance.

Field	Description
IP	IP of the appliance. In the case of Twin Mirror this would be the virtual IP.
System	<p>System status is reported with a single icon in x10 configurations and two icons in TwinMirror configurations. All appliances start out as <i>Disconnected</i>.</p> <p>After an Executive has established communication with an appliance, the status <i>Connected</i> status should display.</p> <p>For Twin Mirror Appliances, the icons should switch from <i>Connected</i> to a more detailed status, indicating the status of each node. In typical operation this would be <i>Primary Running/ Secondary Hot</i>.</p>
IP Control	The state of IP Control on the appliance.
DNS	The state of the DNS service on the appliance
DHCP	The state of the DHCP service on the appliance
Status Check	Timestamp of last status message polled/received.
Details	A detailed view of a given appliance status and a paged history of statuses and events.
Manage	Provides a web based management console similar to the console available on an appliance with a terminal login.

Table 6-23 Agent Dashboard Status Explanations

Field	Description
 Connected/running	System is up or service is running.
 Disconnected or down	System is unreachable or service is down.
 Hot/In stand by	Typically used in TwinMirror representation to indicate that a node is ready for failover, but is not currently the node responsible for operation.
 Unknown/Unreachable	The current status is unable to be determined. One common reason for reporting an unknown System status for a node in a Twin Mirror configuration, would be if the primary server cannot talk to the secondary via the Twin Mirror cable.
 Found unconfigured service running	If an appliance is defined in the Executive without DNS or DHCP configured (checked), but the Executive receives a message from an appliance that the service is up and running. The message <i>Running but unconfigured</i> is displayed.
 Hardware problem	A hardware problem has been detected. Hover the cursor over the entry for further details.

Appliance Details

When you click on the **Details** link on a specific appliance on the dashboard, the event message details are displayed, as shown in Figure 6-26.

Appliance Details - sapphire4.diamondip.com

Name	IP	System	IPControl	DNS	DHCP	Status Check
sapphire4.diamondip.com	192.168.196.20					2011-10-21 09:47:02.0

Export:

Page: 1 of 16 1-10 of 158 Show: 10

Time	Source	Category	Details
2011-07-25 14:27:09.0	sapphire4.diamondip.com - appliance	status	Disconnected
2011-07-25 14:27:12.0	sapphire4.diamondip.com - appliance	status	Connected
2011-07-25 14:27:12.0	sapphire4.diamondip.com - agent	status	Running
2011-07-25 14:27:12.0	sapphire4.diamondip.com - msgrouter	status	Running
2011-07-25 14:27:12.0	sapphire4.diamondip.com - dnsserver	status	Running
2011-07-25 14:27:13.0	sapphire4.diamondip.com - dhcpserver	status	Down
2011-07-25 14:27:13.0	sapphire4.diamondip.com - appliance	status	Primary Running / Secondary Down
2011-07-25 14:27:13.0	sapphire4.diamondip.com - raiddisk	status	No RAID subsystem installed
2011-07-25 14:27:13.0	sapphire4.diamondip.com - powersupply	status	No redundant power supply installed
2011-07-25 16:36:42.0	sapphire4.diamondip.com - appliance	status	Disconnected

Page: 1 of 16 1-10 of 158 Show: 10

Figure 6-26 Appliance Details

To return to the Appliance Dashboard, click

All event messages include the date/time of the event, and the source, category, and message details. The complete list of events generated by the Sapphire Appliances is included in Table 6-24.

Table 6-24 Appliance Events

Source	Category	Message	Details
appliance	action	boot	Standalone appliance boot
appliance	action	reboot	Standalone appliance reboot
appliance	action	shutdown	Standalone appliance shutdown
appliance	action	boot.twinmirror	TwinMirror pair boot
appliance	action	reboot.twinmirror	TwinMirror pair reboot
appliance	action	shutdown.twinmirror	TwinMirror pair shutdown
appliance	action	boot.primary	TwinMirror primary boot
appliance	action	reboot.primary	TwinMirror primary reboot
appliance	action	shutdown.primary	TwinMirror primary shutdown
appliance	action	boot.secondary	TwinMirror secondary boot
appliance	action	reboot.secondary	TwinMirror secondary reboot
appliance	action	shutdown.secondary	TwinMirror secondary shutdown
appliance	action	runon.primary	Run IPControl on primary node
appliance	action	runon.secondary	Run IPControl on secondary node
appliance	status	connected	Connected to management service
appliance	status	disconnected	Disconnected from management service
appliance	status	prsh	Primary running / Secondary hot
appliance	status	phsr	Primary hot / Secondary running

Source	Category	Message	Details
appliance	status	prsd	Primary running / Secondary down
appliance	status	pdsr	Primary down / Secondary run
appliance	status	prsu	Primary running / Secondary unknown
appliance	status	pusr	Primary unknown / Secondary running
appliance	status	pusu	Primary unknown / Secondary unknown
appliance	status	pdsd	Primary down / Secondary down
agent	action	started	The IPControl Agent was started
agent	action	stopped	The IPControl Agent was stopped
agent	status	running	The IPControl Agent is running
agent	status	down	The IPControl Agent is down
msgrouter	action	started	The IPControl Message Router was started
msgrouter	action	stopped	The IPControl Message Router was stopped
msgrouter	status	running	The IPControl Message Router is running
msgrouter	status	down	The IPControl Message Router is down
dhcpserver	action	started	The DHCP Server was started
dhcpserver	action	stopped	The DHCP Server was stopped
dhcpserver	status	running	The DHCP Server is running
dhcpserver	status	down	The DHCP Server is down
dnsserver	action	started	The DNS Server was started
dnsserver	action	stopped	The DNS Server was stopped
dnsserver	status	running	The DNS Server is running
dnsserver	status	down	The DNS Server is down

Appliance Management

When you click on the **Manage** link on a specific appliance on the dashboard, the management console is displayed as shown in Figure 6-27. All management and configuration operations correspond to those available from the console on the Sapphire Appliance. Each operation is performed remotely on the appliance by sending a secure message to the management server running on the Sapphire Appliance. The management server then invokes the corresponding script to carry out the operation.

Please refer to the *Sapphire Install Guide* for a detailed explanation of each available operation.



Figure 6-27 Appliance Management Operations

A sample Network Configuration screen is shown in Figure 6-28.

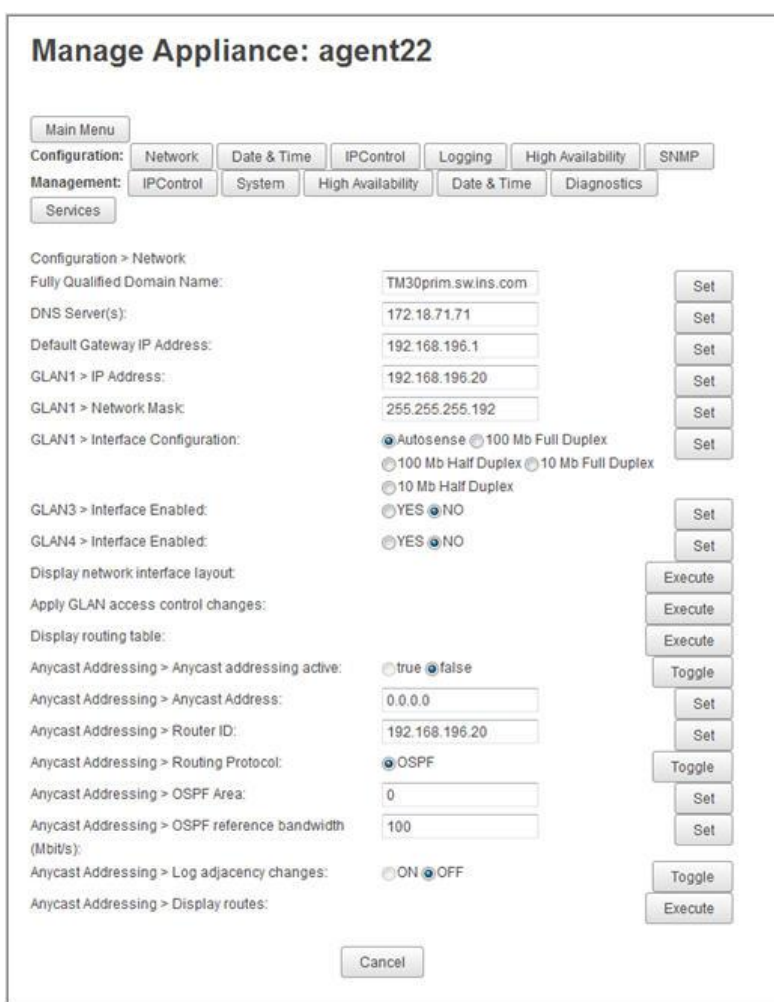


Figure 6-28 Appliance Configuration - Network

A sample Management IPControl screen is shown in Figure 6-29.

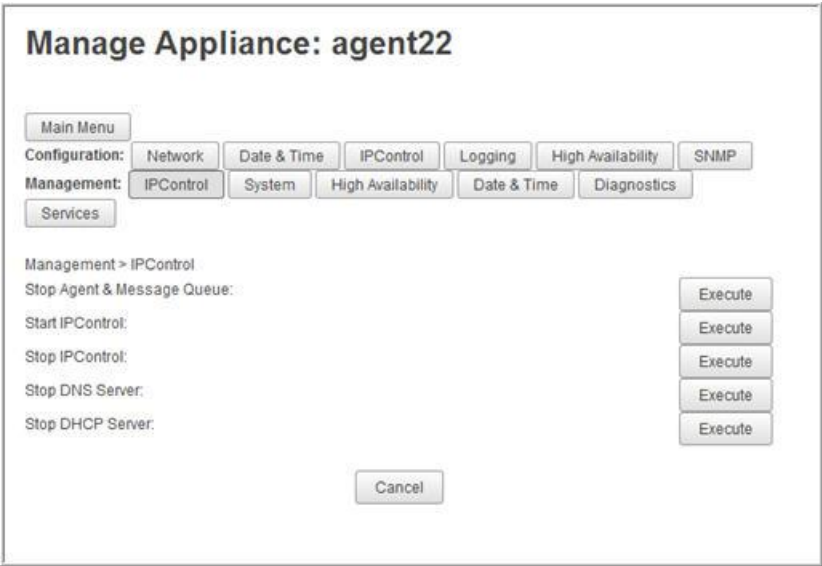


Figure 6-29 Appliance Management - IPControl

Logged-In Administrators Report

The Logged-In Administrator Report provides information on the administrators that are currently logged-in to the system.

Accessing the Logged-In Administrators Report

To access the report, select **Logged-In Administrators** from the OTHER section of the **Reports** menu. The report shown in Figure 6-30 opens.

Logged-In Administrators Report Output

The default Logged-In Administrator report is shown in Figure 6-30.

The screenshot displays the 'Logged In Administrators' report interface. At the top, there is a search bar and a 'Search' button. To the right, there are 'Export' options with icons for PDF, CSV, and XLS. Below this, a pagination bar shows 'Page: 1 of 1' and 'Show: 10'. The main table has four columns: 'Login Time', 'Admin', 'Session ID', and 'Client IP Address'. The table contains one row of data: 'Thu Dec 15 18:09:19 CST 2011', 'incadmin', 'FCDB024EB0F4C8998091CDA8E029E93E', and '173.62.178.23'. At the bottom, there is another pagination bar showing 'Page: 1 of 1' and 'Show: 10'.

Login Time	Admin	Session ID	Client IP Address
Thu Dec 15 18:09:19 CST 2011	incadmin	FCDB024EB0F4C8998091CDA8E029E93E	173.62.178.23

Figure 6-30 Logged-In Administrators Report

Columns in the report output are described in Table 6-25.

Table 6-25 Logged-In Administrators Report Output Elements

Field	Description
Login Time	The date and time that the user logged in.
Admin	The administrator that logged in.
Session ID	Session ID associated with this particular session. This is useful when an admin has multiple application sessions open.
Client IP Address	IP address of the client or last proxy that the Admin logged in from.

RIR Summary Report

The RIR Summary Report creates a report that can be used to provide utilization information to a Regional Internet Registry such as ARIN or APNIC.

Accessing the RIR Summary Report

To access the report, follow these steps.

1. Run a Global Utilization Rollup task to ensure you have the most accurate data.
2. Select **RIR Summary** from the OTHER section of the **Reports** menu. A Filters pane appears in the left pane, as shown in Figure 6-31, and a view of your block allocation is displayed within the main browser window, as shown in Figure 6-20 (page 243).



Filters

☐ Internet Registry
Select Internet Registry: ARIN

☐ Organization Id
Select Organization Id: --- All ---

☐ IP Version
☐ v4
☐ v6

Figure 6-31 Regional Internet Registry Report Filter

RIR Summary Report Output

The default Regional Internet Registry Report is shown in Figure 6-32.

Block	Internet Registry	Usables	Allocated	UnAllocated	Reserved	Assigned	Locked	IP Version	Alloc %	Util %
2.2.2.0/30	ARIN	4	0	4	0	0	0	v4	0	0
2.2.2.100/30	ARIN	4	0	4	0	0	0	v4	0	0
2.2.2.104/30	ARIN	4	0	4	0	0	0	v4	0	0
2.2.2.108/30	ARIN	4	0	4	0	0	0	v4	0	0
2.2.2.112/30	ARIN	4	0	4	0	0	0	v4	0	0
2.2.2.116/30	ARIN	4	0	4	0	0	0	v4	0	0
2.2.2.12/30	ARIN	4	0	4	0	0	0	v4	0	0
2.2.2.120/30	ARIN	4	0	4	0	0	0	v4	0	0
2.2.2.124/30	ARIN	4	0	4	0	0	0	v4	0	0
2.2.2.128/30	ARIN	4	0	4	0	0	0	v4	0	0

Figure 6-32 Regional Internet Registry Report

Columns in the report output are described in Table 6-26.

Table 6-26 RIR Report Screen Elements

Field	Description
Block	The root block and CIDR size.
Internet Registry	The name of the Internet Registry.
Usables	The total number of addresses in this block.
Allocated	The number of IP Addresses in sub-blocks (of this block) that have a status of InUse/Deployed or InUse/Fully Assigned.
Unallocated	The number of IP Addresses that are still available for allocation from this block.
Reserved	The number of IP Addresses from this block that have a reserved status.
Assigned	The number of IP Addresses from this block that has been assigned either dynamically, statically, or is in a locked state.
Locked	The number of IP Addresses that are locked.
Alloc %	The percent of this block that is allocated. This is equal to the (number allocated / blocksize hosts) * 100.
IP Version	Displays v4 or v6.
Util %	The percent of this block that is utilized. This is calculated by taking the (number assigned / number of addressable hosts) * 100. Number of addressable hosts is determined by taking the total blocksize and subtracting all addresses lost due to subnet assignment, such as the subnet and broadcast address.

SWIP/Net Name Report

The SWIP Report provides a report that shows the SWIP ([Shared WHOIS Project](#)) information that is needed to assist in reporting to the ARIN internet registry. Internet Service Providers (ISPs) that receive IP address space from ARIN directly or indirectly (as a downstream customer of another ISP) MUST use either Shared WHOIS Project known as SWIP or a Referral WHOIS server known as RWhois to provide reassignment information for /29 and larger blocks to ARIN.

SWIP is a process used by ISPs to submit customer IP reassignment information to ARIN’s WHOIS database. It ensures the effective and efficient maintenance of records for IP address space. All utilization templates must be submitted in ASCII format via e-mail. [RFC 2050](#) Section 2.2 provides a brief description on the submission of Reassignment information.

SWIP is intended to:

- Provide information to identify the organizations utilizing each sub-delegated IP address block.
- Provide registration information for each IP address block.
- Track utilization of allocated IP address blocks to determine if additional allocations may be justified.

Creating a SWIP/Net Name Information Report

To create a SWIP/Net Name Information Report, follow these steps.

1. Run a Global Utilization Rollup task to ensure you have the most accurate data.
2. Select SWIP/Net Name Information from the OTHER section of the Reports menu. A Filters pane appears in the left pane, as shown in Figure 6-33, and a view of your block allocation is displayed within the main browser window, as shown in Figure 6-34 (page 257).

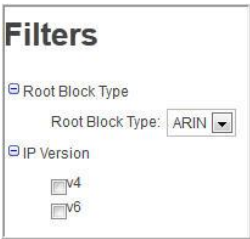


Figure 6-33 SWIP/Net Name Report Selection

3. Customize the report by making selections in the Filter pane, as described in Table 6-27.

Table 6-27 SWIP/Net Name Report Filter Elements

Field	Description
Root Block Type	
Root Block Type	Select the Regional Internet Registry block type you want to report against. Choices are ARIN or RIPE.
IP Version	

Field	Description
	Select from the following choices:
	<ul style="list-style-type: none"> v4 v6

SWIP/Net Name Information Report Output

The default SWIP Report is shown in Figure 6-34.

Block Name	SWIP/Net Name	Addressable Hosts	Allocated	UnAllocated	Reserved	Assigned	Locked	Alloc %	Util %	Root Block Type	IP Version
57.0.0.0/27	SwipName	30	32	0	0	15	0	100	50	ARIN	v4

Figure 6-34 IPv4 SWIP/Net Name Report Output

Columns in the report output are described in Table 6-28.

Table 6-28 SWIP/Net Name Information Report Output Elements

Field	Description
SWIP Name	The SWIP name that has been assigned to this block.
Block Name	The block name consisting of the starting point of the block and the CIDR size.
Addressable Hosts	The number of hosts that are addressable within this block.
Allocated	The number of IP Addresses that are allocated from this block.
Unallocated	The number of IP Addresses that have not been allocated from this block and are free.
Reserved	The number of hosts that are reserved within this block.
Assigned	The number of hosts that are in use in this block.
Locked	The number of IP Addresses that are locked.
Alloc %	The percent of this block that is allocated.
Util %	The percent of this block that is utilized.
Root Block Type	The Regional Internet Registry block type.
IP Version	Displays v4 or v6.

Chapter 7 Setting Up System Policies, Agents, and Importing Data

System Policies/Options

System Policies are policies that affect your interaction with IPControl system-wide. There are several configurable system policies. To work with System Policies, select **Policies and Options** from the **Tools** menu. The policies are described in Table 7-1 on page 260.

System Policies/Options

System Policies/Options:

License Key:	F2b35T20oY0FzaJQPt+QncNp32XWQ9ZfsTJMccFGn28k pDjsQyKQLBdc1ZY3555F	
Default Dynamic Address Pool Alert Threshold:	90	
Default Period Type for Pool Regressions:	Day	
Default Number of Periods for Pool Regressions:	90	
Task Manager Address:	127.0.0.1	
Executive IP Address:	127.0.0.1	
Executive Copy Port:	8021	
Executive Copy Username:	ftpuser	
Executive Copy Password:	Verify Password:
Executive Copy Method:	FTP	
File Manager FTP Port:	8021	
File Manager User ID:	ftpuser	
File Manager Password:	Verify Password:
Default Path for File Manager:	/	
SOA Serial Number Format:	Numerical	
Classless in-addr.arpa Notation:	CIDR Usable Range	
Enterprise or Service-Provider Constructs:	Enterprise	
Polling Interval of Task Manager (seconds):	15	
External Authentication Script:	<input type="text"/> <input type="button" value="Test"/>	
Allow Duplicate CNAME Owners:	No	

Figure 7-1 System Policies/Options (partial)

Table 7-1 System Policies/Options Parameters

Field	Description
License Key	The license key you received from INS for InControl.
Default Dynamic Address Pool Alert Threshold	The value, in percent, at which administrators will be alerted that a dynamic address pool (DHCP) is filling up.
Default Period Type for Pool Regressions	The Period type that will be used to calculate the pool regression. Days, Weeks, Months, or Years.
Default Number of Periods for Pool Regression	The default number of periods (based on Period Type – i.e., “90” Days) that will be used when calculating the pool regression. The number of periods entered will be used for creating the forecasting values for utilization information.
Task Manager Address	The IP address of the Task Manager module; usually this is the same IP address as that of the InControl Executive.

Executive IP Address	The IP Address of the Executive, used by InControl Agents when moving files.
Executive Copy Port	The port number used by InControl Agents to move files back to the Executive. Typically, 21 for FTP, 22 for SCP.
Executive Copy Username	The user name used by InControl Agents when moving files back to the Executive.
Executive Copy Password	The password used by InControl Agents when moving files back to the Executive.
Executive Copy Method	<p>The protocol used by InControl Agents to move files back to the Executive. SCP and FTP are the choices.</p> <p>Note: incadmin's \$HOME environment variable must be set to <code>/opt/incontrol/fiproot</code> if the Executive resides on a UNIX platform, when using the SCP copy method. Check <code>/etc/passwd</code> on the Executive to confirm this setting.</p>
File Manager FTP Port	The port number used by the File Manager to listen for incoming FTP connections from Agents. The File Manager is not used if the Executive Copy Method is SCP.
File Manager User ID	The User ID used by remote Agents to log in to the File Manager. Generally you do not need to change this setting.
File Manager Password	The Password used by remote Agents to log in to the File Manager. Generally you do not need to change this setting.
Default Path for File Manager	The default path for files uploaded to the File Manager.
SOA Serial Number Format	<p>Default format for DNS SOA Serial numbers. Numerical format is recommended for dynamic zones.</p> <p>Numerical – Instructs the system to use numeric SOA serial numbers when writing zone files.</p> <p>Date (YYYYMMDDxx) – Uses the date format of YYYYMMDDxx for the SOA number. Note the xx is a numeric sequence number, so if you plan on having more than 99 updates in a single day (or more than 99 dynamic DNS updates), you must use the “Numerical” SOA serial number format.</p>
Classless in-addr.arpa Notation	Style used when creating classless in-addr.arpa (RFC 2317) domains. Currently only CIDR Usable Range is supported.
Enterprise or Service Provider Constructs	Determines how certain components of the user interface are rendered. Select Enterprise if you are an Enterprise customer, select Service Provider if you are an ISP, Service Provider, or broadband operator.
Polling Interval of Task Manager	The number of seconds the task manager will wait between polls to check if any tasks need to be processed. Typically this is set to 15 seconds.
External Authentication Script	<p>The full path and name of the external authentication script that is used for authentication of users during login. Refer to “Configuring IPControl to use External Authentication” on page 351. You can override the standard user authentication using this option. For example:</p> <pre>C:\perl\bin\perl.exe "c:\program files\diamondip\test.pl"</pre>
Allow Duplicate CNAME Owners	Specifies if you wish to include duplicate CNAME owners. Typically, you should set this option to NO since BIND 9.x does not allow duplicate CNAME owners by default, and discards the zone if you attempt to add duplicates to it.

Field	Description
Enable Device Callout Policy	This policy governs whether changes to a device are sent to the Callout Manager. The policy defaults to False to minimize the amount of traffic that is sent to the Callout Manager. Set this policy to True if you want changes (add, delete, and modify) to be sent to the Callout Manager.
Allow Underscores in Host Names	Allows for system-wide permit or deny of underscores in hostnames.
Allow Dots in Host Names	Allows for system-wide permit or deny of dots (.) in hostnames.
Allow block allocation from non-writable containers	Determines whether users can allocate space from an aggregate block in a container to which the user does not have Write permission.
Enable Block Callout Policy	Governs whether changes to a block are sent to the Callout Manager. The policy is set to False to minimize the amount of unneeded traffic that is sent to the Callout Manager. Set this policy to True if you want changes (add, delete, and modify) to be sent to the Callout Manager.
Use View Name with Galaxy Zone Filenames	Set to Yes to append the View name to the end of the Galaxy zone's filename when it is written to the DNS server, for example: LocationNamedb.domain.com.ViewName
Audit Container Changes	Set to Yes to track changes (add, delete, and modify) to a Container.
Audit Block Changes	Set to Yes to track changes (add, delete, and modify) to a Block.
Audit Device/IpAddress Changes	Set to Yes to track changes (add, delete, and modify) to a Device.
Audit DNS Resource Record Changes	Set to Yes to track changes (add, delete, and modify) to Domain level Resource Records.
Force Change Password Value	Allows the administrator to set a password that <i>must</i> be changed by the user when they next logon. For example, if this policy is set to changeme, then any user whose password is changeme is required to change it at their next logon. If the policy is blank, users are not affected.
Block Folding Threshold	Sets the number of blocks in a container that triggers the folded display instead of the standard list for easier navigation. For example, if there are more than 500 blocks in a container, the folded display is used.
Default Host Discovery Ping type	The default 'Ping Host' type initialized when defining a Subnet Hosts Discovery task in the Discover Subnet Hosts screen. <ul style="list-style-type: none"> Select Ping Only to set as default the option which sends ICMP packet, then only does portscan if reply is received. Select Ping with TCP port 80 packet to set as default the option that sends ICMP and TCP packet on port 80, then waits for reply.
About Page Custom Link "#" Label	Use these numbered fields to add customized hyperlinks to the Home tab. The Label is the value displayed in the Home tab.
About Page Custom Link "#" URL	Use these numbered fields to add customized hyperlinks to the Home tab. The URL is the site (e.g., http://www.companyhelpdesk.com) to be directed to.

Field	Description
Limit Container Tree Display	<p>Governs the display of containers in the tree display within the Management > Container and Container Maintenance displays, as well as in various Search popup windows.</p> <ul style="list-style-type: none"> Select Admin Readable to limit the container tree to display only those containers (and its ancestors) to which the current Administrator has at least Read privileges. This is the default behavior. Select All Containers to allow all Administrators to see all containers in the tree regardless of privileges. However, if an administrator clicks on a container in the tree to which he/she does not have at least Read privilege, an Access Denied message is displayed.
Case Sensitive Password Check	When set to Yes, the login password validation is case sensitive.
Allow Block Allocation from the Same Container	When set to Yes, allows a child block to be allocated in the same container as its root block. Wait at least 60 seconds for this change to take effect.
Limit Display of Blocks by Blocktype Access	<p>Governs the display of blocks in various lists based on Blocktype Access Control settings. When set to Yes (the default), blocks of the selected type do not appear in lists when access for an administrator in the Blocktype Access Control tab is turned off.</p> <p>When set to No, blocks of the selected type appear in lists but an administrator may not have Write access.</p> <p>Examples of these block lists are Management > Container View, Management > Subnet/Block View, and various Search lists where only Read access is required.</p>
Default Domain Contact	<p>Specifies the policy for forming the domain contact. Select from the following:</p> <ul style="list-style-type: none"> Use Admin's Email Address to use the administrator's email address. Use Explicit Email Address to use the email address specified in the Domain Contact Email system property Use Explicit Email Address in Current Domain to use the user entered DNS Domain Name appended to the email address specified in the Domain Contact Email system property.
Domain Contact Email	The Domain contact email address used in the Default Domain Contact system policy.
Default Allocation Algorithm	<p>The default allocation algorithm to use for automatic block allocation.</p> <ul style="list-style-type: none"> Select Use Best fit Allocation to set as default the best fit algorithm. Select Use Random Allocation to set as default the random algorithm (IPv6 only). Select Use Sparse Allocation to set as default the sparse algorithm (IPv6 only)
CNR DHCP Collection Sharename	When used in conjunction with Enable Primary Subnet Handling, handles how the automatic generation of Address Pool sharenames are created. Select Primary Subnet Address or Primary Scope Name to decide where the unique sharename comes from during the Address pool creation.

Field	Description
Enable Primary Subnet Handling	When set to True, enables automatic generation of Address Pool sharenames. When set to False, the Address Pool sharenames must be specified manually and accurately. When enabled, this policy is used in conjunction with CNR DHCP Collection Sharename.
IPControl Executive FTP Copy Passive Mode	If the Executive Copy Method is FTP, then this policy can be used to control whether or not the FTP connection from the Agent to the Executive is established using passive mode.
Limit DHCP Servers by Container Tree	Important! Do not set this policy to true unless instructed by BT Diamond IP. When set to True, governs the display of DHCP Servers in certain drop-down lists by limiting the list to only those servers that are attached to the current branch of the container tree. The lists are those involved in the assigning of a DHCP server to an IP address, IP range, address pool, or block.
Container Folding Threshold	Sets the number of containers that can appear in a tree before the list of containers is folded into ranges for easier navigation. For example, the default value of 500 indicates that the folded display is used if there are more than 500 children under a given container.
Enable Task Callout Policy	When set to True, the Callout Manager is notified upon completion of a task (Configuration/Deployment or Discovery/Collectors). The default value is False due to the large overhead that can occur, particularly with DDNS Update tasks.
Perform Regression During Global Rollup	Controls whether regression analysis is performed during the global rollup task. The regression analysis includes: 1) Address Pool utilization, 2) Block Utilization (Overall), 3) Dynamic Address Block Utilization, 4) Container Utilization (Overall), 5) Dynamic Address Container Utilization. History records collected during the rollup are used as the input to the regression analysis. The result is a “days left” metric, which indicates how many days the remaining space will last. Since this analysis can slow down the system, you can set this option to False and disable computed metrics, and thereby improve performance.
Allow Overlapping Public Blocks	When set to Yes, allows the creation of overlapping non-RFC1918 root blocks. The default is No since this is typically not necessary, except in some specialized cases.
Count “Other Available” leases for CNR DHCP collections	<i>For CNR Summary Collections Only.</i> If this policy is True, leases marked as “Other Available” are counted as unavailable or locked in the utilization.
Maximum records to export from User Interface	Determines the maximum number of records that can be exported through the UIs, such as Audit reports. Care should be taken when changing this setting since the export of records consumes considerable system resource. Export of a very large number of records can result in an out of memory error that requires the web server to be restarted. The threshold at which the error may occur varies by systems but is dependent on the total memory and the system load when the report is run.

Field	Description
Enforce CNR DHCP Infrastructure Mappings	<p><i>WARNING! This policy should be used with extreme caution:</i> It requires expert knowledge and is intended for use by certain MSOs only. If you are unclear about the implications of this policy, please contact BT Diamond IP support.</p> <p>Applies the DHCP Collection tasks for CNR DHCP servers. It causes the collection task to further match the shared-network configuration found on the CNR DHCP server (via the primary-subnet attribute) to a corresponding shared-network configuration in IPControl. Shared networks are configured in IPControl by setting the Primary Subnet flag on subnets attached to the same interface of a device container. See the “Primary Subnet Handling” system policy for more information. In order for this policy to be effective, manual modifications to the IPControl Result Manager property file must be made as well. Please contact BT Diamond IP support for assistance in these manual modifications.</p>
Workflow Type	<p><i>Master Administrators only.</i> Determines the workflow type. Settings are as follows:</p> <p>None – Workflow is disabled and IPControl does not require approvals on device or resource records.</p> <p>Resource Records – Enables users to control resource record approvals at the domain level. The Resource Record Approval Access check box is enabled for all administrators on the Domain Access Control tab in Administrator Policies. You can then control access by disabling for specific administrators or by assigning a role in which the right is disabled.</p> <p>Device – Enables users to control device/IP address approvals at the container or block level. The Device Approve Access check box is enabled for all administrators on the Access Control List tab in Administrator Policies. You can then control access by disabling for specific administrators or by assigning a role in which the right is disabled.</p>

Agents

Use the Agents screen to manage the Agents used by IPControl. Agents are used to perform various tasks such as gathering subnet information or statistics, transporting network service configuration, or communicating to network devices to capture configuration information. Agents have direct interaction with DNS servers, DHCP servers, routers, and/or switches.

When you select **Agents** from the SYSTEM section of the **Tools** menu, a list of existing agents, if any, is shown in the Agents screen.

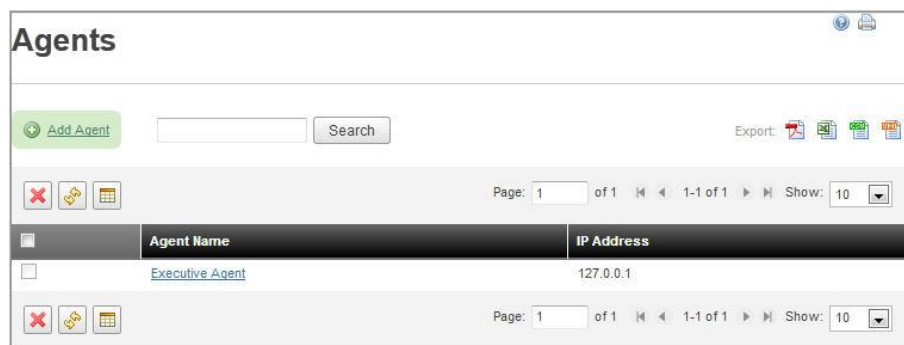



Figure 7-2 Agents List

To search for a particular agent, enter a search string into the text block and click **Search**.

To delete one or more agents, click the checkbox next to each item you want to delete, and click . At the confirmation prompt, click **OK** to delete the selected agents, or **Cancel** to undo your selections.

To add a new agent, click the **Add Agent** link. The Add Agent screen appears.

Figure 7-3 Add InControl Agent

Table 7-2 Agent Parameters

Field	Description
InControl Agent Name	The name of the agent, in either simple or fully-qualified form.
IP Address	The IP address of the agent. This is used by the InControl Executive to connect to the Agent.

Click **Submit** to add the agent, or **Cancel** to return to the previous screen.

Import Wizard

The Import Wizard allows you to import the following data types into your IPControl database in a four-step process:

- Device
- Child Block
- Root Block
- Device Resource Record
- Address Pool

Note: The size of the import file cannot exceed 2MB.

The four steps are:

1. Select the type of file to import.
2. Select the Comma Separated Value (CSV) file from your local machine and upload it to the IPControl server.
3. Validate the data in the import file.
4. Import the import file data.

To access the Import Wizard, select **Import Wizard** from the SYSTEM section of the **Tools** menu. The IPControl Import Wizard Step 1 screen opens, as shown in Figure 7-4.

Figure 7-4 Import Wizard Step 1

Step 1: Select Import Type

In Step 1, you define the type of data import that you want to perform, as described in Table 7-3. Refer to the *IPControl CLI and API Guide* for more details about each import type. When you have selected an **Import Type**, click **Next**.

Table 7-3 Import Types

Import Type	Description
Import Device	Enables importing of IP devices into IPControl. Attributes for each device including user-defined fields may be specified for each device. Each IP address associated with imported devices must exist within In-Use/Deployed subnet(s) within IPControl. For more information, refer to the ImportDevice CLI.

Import Type	Description
Import Child Block	Allows import of child blocks into IPControl. Attributes for each child block including user defined fields may be specified for each block. Each child block to be imported must reside within an existing root block defined within IPControl. For more information, refer to the ImportChildBlock CLI.
Import Root Block	Allows import of root blocks into IPControl. Attributes for each root block including user defined fields may be specified for each block. For more information, refer to the ImportRootBlock CLI.
Import Device Resource Record	Allows import of resource records associated with devices into IPControl. Each record must be associated with an existing device in IPControl. For more information, refer to the ImportDeviceResourceRecord CLI.
Import Address Pool	Allows import of address pools into IPControl. Option and policy sets for each pool may be defined, as well as allow and deny client classes. Address ranges comprising each pool must exist with In-Use/Deployed subnet(s) within IPControl. For more information, refer to the ImportAddrpool CLI.

Step 2: Select Import File

In Step 2, you specify which CSV file to use for the import type you selected in Step 1, as shown in Figure 7-5.

Note: The required CSV file format for the selected import type is shown, displaying **Column**, **Field**, **Accepted Value** and **Required** information in a scrollable section.

IPControl Import Wizard

Step 1 Select Import Type | **Step 2 Select Import File** | Step 3 Validate Import File Data | Step 4 Import Data

Please select the file on your system to import, and then select Upload:

Import File

Accepted Values Required

ColField
A Container

The name of the Yes container that will hold the block. Names can be in either short or long format. Short format example: Dallas. Long format example: IPControl/Texas. /Dallas. Long format

< Back

Figure 7-5 Import Wizard Step 2

To select a file, follow these steps:

1. Type the full path to the CSV file you want to upload, or click **Browse** to locate the file in the file selection window.
2. Click **Upload** to copy your file to the central server.

3. Click **Next** to continue. To return to the previous step, click **Back**.

The file format is validated as it is copied to the server, and the result of the validation is shown in Step 3.

Step 3: Validate Import File Data

Step 3 displays the results of a spot check of the first record in the selected file to verify that the required fields and data types are present for the selected import type. The field labels correspond to the column definitions for the selected import type, and the field values correspond to each column of the first row of the file, as shown in Figure 7-6.

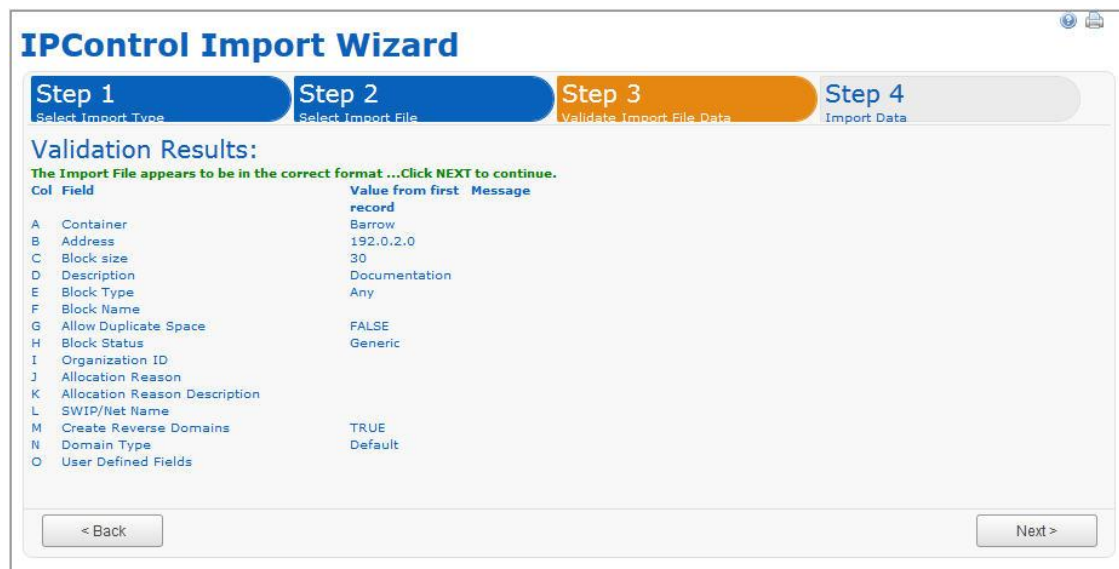


Figure 7-6 Import Wizard Step 3

If validation is successful, the Step 3 screen indicates that there were no detected errors:

The Import File appears to be in the correct format ...
Click NEXT to continue

If validation is not successful, the Step 3 screen indicates that the file contains errors and indicates where the error occurred:

The Import File is not valid and contains errors. See
below for details. Click BACK and Upload a new file.

A sample validation error is shown in Figure 7-7.

Col	Field	Value from first record	Message
A	Container	Barrow	
B	Address	192.0.2.0	
C	Block size		Block Size required
D	Description	Documentation	
E	Block Type	Any	
F	Block Name		
G	Allow Duplicate Space	FALSE	
H	Block Status	Generic	
I	Organization ID		
J	Allocation Reason		
K	Allocation Reason Description		
L	SWIP/Net Name		
M	Create Reverse Domains	TRUE	
N	Domain Type	Default	
O	User Defined Fields		

Figure 7-7 Import Wizard Step 3 Validation Error

If validation is successful, click **Next** to continue to Step 4. Otherwise, click **Back** so you can open the CSV file and fix errors before you upload the file another time.

Step 4: Import Data

Step 4 of the Import Wizard appears after successful validation of the selected import type data file has occurred, as shown in Figure 7-8.

Figure 7-8 Import Wizard Step 4

You can now decide whether to import the data file immediately, or schedule it to run later.

To select a future date to import the data file, select the Scheduled option button. The screen refreshes to show scheduling fields:

Import Data:
 When would you like to import this data? ☐ Immediate ☒ Scheduled
 Select the date and time that this import is to begin:
 : : AM (hh:mm)

Figure 7-9 Import Data Scheduled Option

Click the calendar icon to select a date. A calendar is displayed, as shown in Figure 4-19, with today's date selected by default.



Figure 7-10 Calendar Utility

You can use the following navigation links to change to another month and/or year and then select a date in the month to close the utility:



Previous Year



Previous Month



Next Year



Next Month

Select the hours, minutes, and AM or PM to schedule a specific time for the task.

Once all scheduling parameters have been entered, click **Done**. A new task is created, and submitted to the system. Once tasks have been created, they can be managed using the **Tasks** option. To view Import Tasks, select from the tasks shown in Figure 7-11 in the **Type** Filters hierarchy:

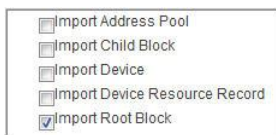


Figure 7-11 Import Task Types

The results are displayed in the Tasks List, as shown in Figure 7-12.

ID	Status	Start Time	Completed Time	Scheduled	Scope	Type	Admin
Task 39	Not Started	2011-12-04 16:50:00.0		Sched		Import Root Block	InControl Administrator
Task 40	Queued	2011-12-04 15:35:07.0		Immed		Import Root Block	InControl Administrator

Figure 7-12 Import Tasks

To review the results of a completed import task, select the **Task ID**. The Task Summary screen opens, as shown in Figure 7-13.

ID	47
Type	Import Root Block
Scope	
Status	Complete
Hold files for preview:	<input type="checkbox"/>
Administrator	rpnormal1
Start Time	2/06/12 6:42 AM
Completed Time	2/06/12 6:42 AM
Duration	00:00:01

Time	Result Level	Text
2/06/12 6:42 AM	INFO	Created reject file: rejects.csv Rejects
2/06/12 6:42 AM	INFO	Created error file: errors.txt Errors
2/06/12 6:42 AM	INFO	Successful import line: 1 - RPContainer1,11.0.0.20,24

3 items found, displaying all items.

Figure 7-13 Import Task Summary

For records that show a rejected and errored status in the **Text** column, access to the respective reject and error files is provided in CSV format. You can select the **CSV** link to view the file and then save it locally for subsequent editing to correct errors.

As with CLI/API transactions, you can review relevant audit records on import wizard activity by reviewing Audit reports for the IP infrastructure type that corresponds to the Import Type. For example, if you are importing Device Resource Records, then run a Resource Record Audit Report and check for entries that correspond to the date you scheduled the import.

Search

The **Search** option allows you to search for the following objects in the IPControl database:

- Specific IP Addresses
- Subnets
- DNS Resource Records
- Containers

When you select one of these options in the **Search For** field, the screen is updated with the respective search criteria for that selection.



Figure 7-14 Search

To perform a search, follow these steps.

1. In the **Search For** drop-down list, choose one of the following search types:
 - ▶ **Individual Objects**
 - ▶ **Subnet/Blocks**
 - ▶ **DNS Resource Records**
 - ▶ **Containers**
2. Choose one of the following actions.

If you are searching for ...	Then ...
Individual Object	<ol style="list-style-type: none"> 1. Choose one of the following search criteria: <ul style="list-style-type: none"> ▶ IP Address ▶ Host Name ▶ Hardware Address ▶ User Defined Fields ▶ Specific text in the Description 2. Select Search ALL Device Types, or refine your search further by choosing a specific Device Type from the drop-down list. 3. <i>UDF only</i>. If you selected User Defined Fields in Step 1, select a UDF from the UDF drop-down list. 4. Enter a string in the Search Value field. 5. For search criteria other than IP Address, choose from the following options: <ul style="list-style-type: none"> ▶ Begins With ▶ Contains ▶ Exact Match

If you are searching for ...	Then ...
Subnet/Block	<ol style="list-style-type: none"> 1. Choose one of the following search criteria: <ul style="list-style-type: none"> ▶ CIDR Address ▶ Specific text in the Name ▶ Specific text in the Description ▶ User Defined Fields ▶ IP Address contained within block 2. Select Search ALL Block Types, or refine your search further by choosing a specific Block Type from the drop-down list. 3. Select Search ALL Block Statuses, or refine your search further by choosing a specific Block Status from the drop-down list. 4. <i>UDF only</i>. If you selected User Defined Fields in Step 1, select a UDF from the UDF drop-down list. 5. Choose one of the following actions: <ul style="list-style-type: none"> ▶ <i>CIDR Address only</i>. Enter a CIDR format address in the Address/Size field. ▶ Enter a string in the Search Value field. 6. For search criteria other than IP Address, choose from the following options: <ul style="list-style-type: none"> ▶ Begins With ▶ Contains ▶ Exact Match
DNS Resource Record	<ol style="list-style-type: none"> 1. Select Search ALL Resource Record Types, or refine your search further by choosing a specific Resource Record Type from the drop-down list. 2. Limit the search by searching: <ul style="list-style-type: none"> ▶ OWNER field only ▶ RDATA field only, the Comment field only ▶ OWNER, RDATA and Comment fields 3. Enter a string in the Search Value field. 4. Choose from the following options: <ul style="list-style-type: none"> ▶ Begins With ▶ Contains ▶ Exact Match

If you are searching for ...	Then ...
Container	<ol style="list-style-type: none">Choose one of the following search criteria:<ul style="list-style-type: none">Specific text in the NameSpecific text in the DescriptionUser Defined FieldsSelect Search ALL Container Types, or refine your search further by choosing Logical or Device container types from the drop-down listChoose one of the following search options:<ul style="list-style-type: none">Begins withContainsExact Match

6. Click **Search**. The system is searched for the specified criteria, and records that match the query are displayed.

Search For:

Containers

Search Criteria for Containers

Specific text in the Name

-- Search ALL Container Types --





Search Value:
Phil



☒ Begins With ☐ Contains ☐ Exact Match

Search


Reset



Search Result: Containers

Export:    

Page: 1 of 1 1-1 of 1 Show: 10

Container	Type	Description	Created	Created By	User Defined Fields
InControl/Americas/U.S./Philadelphia 	Logical		2011-05-22 15:25:58.0	incadmin	

Page: 1 of 1 1-1 of 1 Show: 10

Figure 7-15 Container Search Results

Chapter 8 Working with Blocks and Subnets

Allocation Reason Codes

The Allocation Reason Codes screen allows you to maintain the reason why IP Address allocations are made. **Allocation reasons** enable IPControl administrators to record a reason why additional address space was allocated. Examples might include “Site Growth”, if your company has a site that has outgrown their current address allocation or “Customer Growth” if you are a service provider with clients that periodically request more addresses. Allocation reasons can be tailored to your organization’s particular needs.

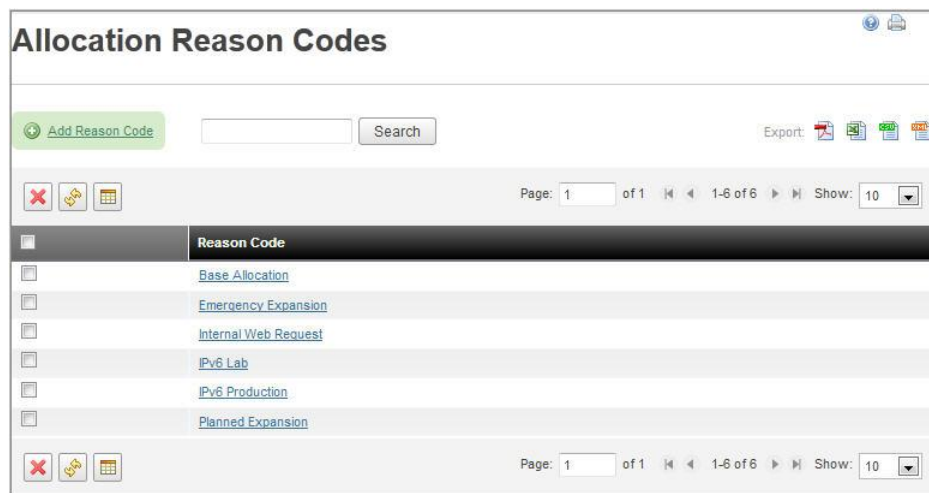



Figure 8-1 Allocation Reason Code List

Choose from the following actions:

- To search for an allocation reason code, enter a search string into the text block and hit Search.
- To delete one or more allocation reason code, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected reasons, or **Cancel** to undo your selections.
- To add a reason code, click the **Add Reason Code** link. The Add Reason screen appears.

Add Allocation Reason Code

Reason Code:

Submit

Cancel

Figure 8-2 Add Allocation Reason Code

Table 8-1 Allocation Reason Code Parameters

Field	Description
Reason Code	The text of the allocation reason you wish to add.

Click **Submit** to add the allocation reason, or **Cancel** to return to the previous screen.





Block Types




Use the Block Types screen to maintain block types. Block types enable you to differentiate your IP address space by function or role. For example, you may want to distinguish between blocks based on how they will be used (customer space, internal topology, loopback space, gold level of service space, and so on). This powerful feature enables the IPControl allocation engine to distinguish between different types of space when automatically allocating IP Address space. In addition, the use of block types allows administrators to tightly control how the IP Address space is allocated, and where that type of address space can be deployed.

Block Types


Add Block Type




Search

Export:    

Page: 1 of 1 1-6 of 6 Show: 10

	Block Type Name	Parent Block Type Name	# of Child Block types
<input type="checkbox"/>	Any		3
<input type="checkbox"/>	Data	Any	0
<input type="checkbox"/>	IPv6 Lab		0
<input type="checkbox"/>	Management		0
<input type="checkbox"/>	Video	Any	0
<input type="checkbox"/>	VOIP	Any	0


Page: 1 of 1 1-6 of 6 Show: 10

Figure 8-3 Block Types

Note: By default, the **Any** block type cannot be deleted.

Choose from the following actions

- To search for a particular block type, enter a search string into the text block and click **Search**.

- To delete one or more block types, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected block types, or **Cancel** to undo your selections. Note that the **Any** block type cannot be deleted.
- To add a block type, click the **Add Block Type** link. The Add Block Type screen appears. Fill in the fields, as described in Table 8-2.

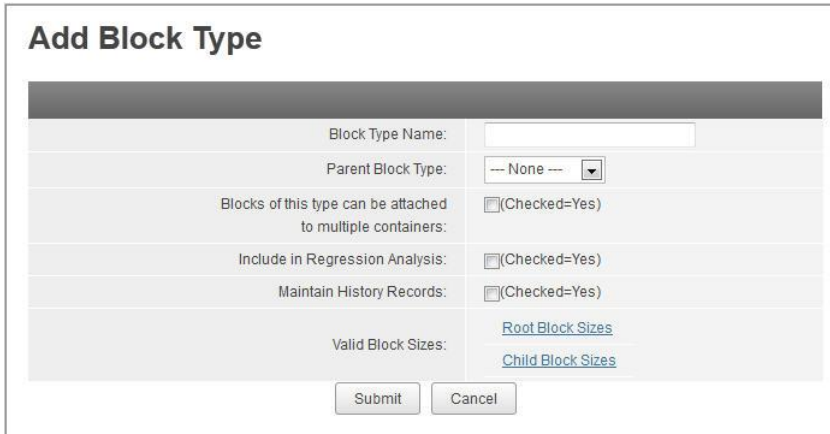


Figure 8-4 Add Block Type

Table 8-2 Add Block Type Parameters

Field	Description
Block Type Name	The name of the block type.
Parent Block Type	A block type can be a child of other block types, including Any . A block type with a parent block type None , however, is not a child to any other block type. During auto allocation, if a block type has a parent, blocks of its own type, as well as of its parent type are included in the result list.
Blocks of this type can be attached to multiple containers	If this box is checked, this block type can be associated with more than one container. This feature allows blocks that are assigned this specific block type to belong to multiple containers. This feature is useful for modeling blocks assigned to multiple physical network devices (that is, routers), such as loopback or point-to-point space.
Include in Regression Analysis	If this box is checked, blocks assigned this block type are included in the regression analysis. For many block types (such as point to point, or loopback), it does not make sense to calculate regression analysis for trending purposes. Because the regression analysis is CPU intensive, in a large deployment it is important to calculate the regression analysis only against blocks that need the trending.
Maintain History Records	If checked, Container History and Block History records are kept for this block type. The history records are created each time the Global Utilization Rollup task is run.

Field	Description
Valid Block Sizes	<p>A block type can be constrained to discrete sizes of an address block for block allocation.</p> <ul style="list-style-type: none"> Select the Root Block Sizes link to constrain block sizes for root block allocation for the block type. Select the Child Block Sizes link to constrain block sizes for child block allocation for the block type.

Constraining Block Sizes

To constrain block allocation for the block type to discrete sizes of an address block, select either the **Root Block Sizes** link for root block allocation or **Child Block Size** link for child block allocation. Selecting either link opens the Edit Block Sizes screen.

Edit Block Sizes: Root

IPv4 IPv6

☒ Check All/Uncheck All

Select	CIDR Block Size
<input checked="" type="checkbox"/>	/32 - 1 Host
<input checked="" type="checkbox"/>	/31 - 2 Hosts (RFC 3021)
<input checked="" type="checkbox"/>	/30 - 2 Hosts
<input checked="" type="checkbox"/>	/29 - 6 Hosts
<input checked="" type="checkbox"/>	/28 - 14 Hosts
<input checked="" type="checkbox"/>	/27 - 30 Hosts
<input checked="" type="checkbox"/>	/26 - 62 Hosts
<input checked="" type="checkbox"/>	/25 - 126 Hosts
<input checked="" type="checkbox"/>	/24 - 254 Hosts (1 Class C)
<input checked="" type="checkbox"/>	/23 - 510 Hosts (2 Class Cs)
<input checked="" type="checkbox"/>	/22 - 1022 Hosts (4 Class Cs)
<input checked="" type="checkbox"/>	/21 - 2046 Hosts (8 Class Cs)
<input checked="" type="checkbox"/>	/20 - 4094 Hosts (16 Class Cs)
<input checked="" type="checkbox"/>	/19 - 8190 Hosts (32 Class Cs)
<input checked="" type="checkbox"/>	/18 - 16382 Hosts (64 Class Cs)
<input checked="" type="checkbox"/>	/17 - 32766 Hosts (128 Class Cs)
<input checked="" type="checkbox"/>	/16 - 65534 Hosts (1 Class B)
<input checked="" type="checkbox"/>	/15 - 131070 Hosts (2 Class Bs)
<input checked="" type="checkbox"/>	/14 - 262142 Hosts (4 Class Bs)

Figure 8-5 Edit Block Sizes

Select all block sizes allowable for allocation for the block type. All unchecked block sizes will not be allowed for allocation. Use the **IPv4** tab to edit settings for IPv4 block size addressing. Use the **IPv6** tab to edit settings for IPv6 block size addressing.

Whether or not a block type is allowed block allocation for a specific size is determined by examining the block size constraint rules defined at the block type definition and rules defined at the administrator for all roles owned by the user seeking to allocate blocks. See the block type policies **Block Type Size Allocation Rules** for further details on this. Note that if a block type is constrained by a block size at the block type definition, it may not be unconstrained at the administrator role block type policy. Block types may only be further constrained by block size at the administrator role policy level, not the other way around.

Click **Submit** to add the block type, or **Cancel** to return to the previous screen.

Address Pool Allocation Templates

Use the Address Allocation Template List screen to maintain address allocation templates. Address allocation templates enable you to define standard policies that govern the allocation of address space or address pools within a subnet. For example, you may want to create a template that reserves the first address within the subnet for a static router assignment, and then all the rest of the space for dynamic assignment. When you add an “Address Block” (subnet) to a container, you can optionally assign that block an “Address Pool Allocation Template”. When you do this, address pools and/or individual IP Addresses will be created within the specific subnet. This capability allows you to automatically configure subnets using established policies.

Select	Template Name
<input type="checkbox"/>	AllDynamic
<input type="checkbox"/>	Branch
<input type="checkbox"/>	IPv6 Subnet
<input type="checkbox"/>	PointToPoint
<input type="checkbox"/>	Retail

Figure 8-6 Address Allocation Template List

The Address Allocation Template List supports the following actions:

- Search for an existing template
- Delete one or more existing templates
- Add a new template


Searching for an address allocation template

To search for a particular address allocation template, follow these steps:

1. Enter a search string into the text block
2. Click **Search**.

Deleting an existing address allocation template

To delete one or more address allocation templates, follow these steps:

1. Select the checkbox in the Select column beside each template you wish to delete.
2. Click . A dialog opens with the message **Are you sure?**
3. Choose one of the following actions:
 - ▶ Click **OK** to delete the selected device templates.
 - ▶ Click **Cancel** to return to the previous screen.
4. The templates you selected are removed and the message Address Pool Template *<template name>* deleted appears.

Adding a new address allocation template

To add an address allocation template, follow these steps:

1. Click the **Add Address Allocation Template** link. The Add Address Allocation Template screen appears, as shown in Figure 8-7.

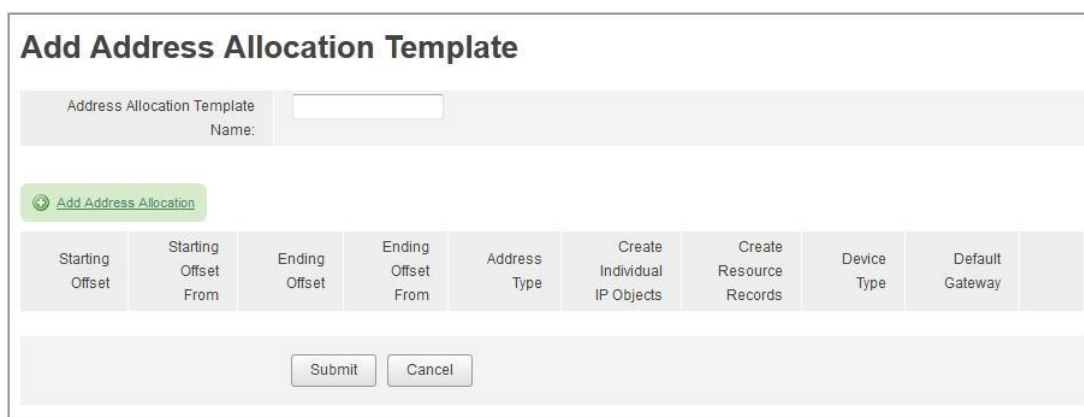


Figure 8-7 Add Address Allocation Template

2. Enter a name of up to 255 alphanumeric characters in the **Address Allocation Template Name** field.
3. Select the **Add Address Allocation** link. The Address Allocation screen shown in Figure 8-8 appears.

Add Address Allocation

Starting Offset:

Starting Offset From:

Ending Offset:

Ending Offset From:

Address Type:

Create Individual IP Objects: ☐

Create Resource Record: ☐

Device Type:

Default Gateway(s): ☐

Figure 8-8 Add Address Allocation

4. Refer to Table 8-3 as you define the allocation parameters for the template you are designing.

Table 8-3 Address Allocation Parameters

Field	Description
Starting Offset	Specify the number of IP addresses you want to offset from beginning or end of the subnet. 0 is not valid.
Starting Offset From	Choose whether you want this offset to start from the beginning or the end of the subnet. Examples: 1) For a /24, 1 from the beginning is x.x.x.1 2) For a /24, 1 from the end is x.x.x.254 3) For a /24, if you create a template using the end of the subnet, Starting Offset=>3 from the end, and Ending Offset=>1 from the end, the expected pool is 252-254.
Ending Offset	Specify the number of IP addresses you want to offset from the beginning or end of the subnet. 0 is not valid.
Ending Offset From	Choose whether you want this offset to start from the beginning or the end of the subnet. Examples: 1) For a /24, 1 from the beginning is x.x.x.1 2) For a /24, 1 from the end is x.x.x.254 3) For a /24, if you create a template using the end of the subnet, Starting Offset=>3 from the end, and Ending Offset=>1 from the end, the expected pool is 252-254.
Address Type	Specify the address type that will be created; Dynamic DHCP, Automatic DHCP, Static Address, or Reserved Address.
Create Individual IP Objects	Unchecked indicates that these IP Addresses will be created as an IP Address Pool. Check indicates that that these IP Address(es) will be created as individual IP Address(es). Refer the IP Management Section for more details regarding IP Addresses versus IP Address Pools.
Create Resource Record	Checked indicates that the system will create default DNS Resource Records for this IP Address(es) when it is created.

Field	Description
Device Type	Enabled only when Create Individual IP Objects is checked. Select the default device type for this IP Address(es).
Default Gateway(s)	Enabled when the Address Type is Static and Create Individual IP Objects is selected. When checked, indicates that default gateway address(es) are available on the block. If selected, the Starting Offset From value and Ending Offset From value must be the same. For more information on specifying the default gateway, refer to “Defining a Default Gateway” on page 46.

- Once the fields are completed, click **Submit**. The Add Allocation Template screen is updated to display the allocation you just defined and the **Edit** and **Delete** buttons appear, as shown in Figure 8-9.

Figure 8-9 Address Allocation Template Defined

- Choose from the following actions.
 - ▶ To make additional allocations within the same template, click the **Add Address Allocation** link and repeat steps 4 and 5.
 - ▶ To delete an allocation, click its **Delete** button. The entry is removed from the template.
 - ▶ To edit an allocation, click its **Edit** button. The Address Allocation screen opens for you to make your changes.
 - ▶ To discard your address allocations and return to the Address Pool Allocation Template List, click **Cancel**.
 - ▶ To save your changes, click **Submit**. The new address allocation template appears in the Address Allocation Template List.

Site Allocation Templates

The Site Allocation Templates feature allows you to define a site template so that you can allocate multiple address blocks in one step. This is especially useful for larger organizations where a new site

may require several subnets. Use the **Site Allocation Templates** option on the **Tools** menu to define a site template, and then invoke the template when creating a site under the **Management > Container View** menu.

Site Allocation Template Functions

You can choose from the following functions:

- Create a new site allocation template. For more information, refer to “Adding a Site Allocation Template” below.
- Modify an existing site allocation template. For more information, refer to “Editing a Site Allocation Template” on page 291.
- Delete a site template. For more information, refer to “Deleting a Site Allocation Template” on page 292.

Site Allocation Template Prerequisites

Before you can manage site allocation templates, the root/aggregate blocks need to be created. For more information, refer to “Add Root Block” on page 28.

Administrators need to have specific Administrator and Container policies set up to use the Site Allocation Template feature.

Administrator Policies

In **Tools > Administrator Roles**, access the Administrator Policies for the administrator role to which you want to grant Site Allocation Template privileges.

- On the **Authorized Functions** tab, ensure that the following checkboxes are selected:
 - ▶ In the System Setup section: **Site Allocation Templates**
 - ▶ In the Management section: **Management Containers** and **Add Sites**
- On the **Access Control List** tab, ensure that Write permission is enabled so that administrators can write blocks to the container.
- On the **Block Type Access** tab, ensure that administrators have access to the block types they will be using in the sites that they create.
- On the **Device Type Access** tab, ensure that administrators have access to the device types they will be using in the sites that they create.
- On the **Domain Access Control** tab, ensure that **Resource Record Write Access** checkbox is selected. This permits administrators to access the domains where resource records are created in any address allocation template in the site template.
- On the **Net Service Access Control** tab, if the **Enable Net Service Access Controls for this Administrator** option button is selected, ensure that the Write checkbox is selected for servers in the Net Service Access list.

For more information on administrator roles, refer to “Administrator Role Policies” on page 335.

Container policies

In **Management > Container Maintenance**, access the Edit Container (or Add Child Container) screen for the container where a Site Allocation Template is to be applied.

- On the **Valid Block Types** tab, ensure that selected block types match the block types specified in the Site Allocation Template you want to apply.
- On the **Valid Device Types** tab, ensure that the device types to which you want nested address allocation templates to be applied are selected.
- On the **Allow Allocation from Parent** tab, ensure that selected block types match the block types specified in the Site Allocation Template you want to apply.
- On the **Require SWIP/NetName** tab, select block types for which you want the same requirement in corresponding block types being added in this container by the site template.
- On the **Block Type Information Templates** tab, select UDFs you want entered on the Add Site screen for the Block Types specified in the Site Allocation Template.
- On the **Device Type Information Templates** tab, select UDFs you want entered on the Add Site screen for the Block Types specified in the Site Allocation Template.

Adding a Site Allocation Template

To add a site allocation template, follow these steps:

1. Select **Site Allocation Templates** from the SUBNET/BLOCK section of the **Tools** menu.
The Site Allocation Templates screen opens.



Figure 8-10 Site Allocation Templates

2. Select the **Add Site Allocation Template** link.
The Add Site Allocation Template screen opens.

Add Site Allocation Template

Site Allocation Template Name:

Container Type: ☒ Logical ☐ Device

[Add Block](#)

#	Block Type	IP Version	Block Size	Allocation Strategy	Block Name	Block Status	Address Allocation Template
---	------------	------------	------------	---------------------	------------	--------------	-----------------------------

Figure 8-11 Add Site Allocation Template

- Enter a name for the template in the **Site Allocation Template Name** field.
- Designate whether the template is for a **Logical** or **Device** container type.
- Click **Add Block**.

The Add Block Sequence screen opens.

Note: If you select **Device** container type, the Block Sequence screen displays two additional parameters: **Interface IP Address** and **Primary Subnet** in the **General** tab, as show in Figure 8-12.

Add Site Allocation Template

Add Block Sequence #1

General Policies

Block Type:

IP Address Version: ☒ IPv4 ☐ IPv6

Block Size:

Allocation Strategy: ☐ Best Fit ☐ Random ☐ Sparse

Exclude from Discovery: ☐

Discovery Agent: ☒ Inherit from Parent Block ☐ Inherit from Parent Container
☐ Select Agent

Interface IP Address:
 Addr 1: Auto allocate Offset From Start
☐ Default Gateway

Block Name:

Block Description:

Current Status:

Primary Subnet: ☐ (Checked=Yes)

Create Reverse DNS Domain(s): ☐ DNS Domain Type:

Allocation Template:

Starting Offset	Starting Offset From	Ending Offset	Ending Offset From	Address Type	Create Individual IP Objects	Create Resource Record	Device Type
-----------------	----------------------	---------------	--------------------	--------------	------------------------------	------------------------	-------------

Figure 8-12 Add Block to Site Allocation Template

- Fill out the parameters in the **General** tab, as described in the following table.

Table 8-4 Add Block Parameters

Field	Description
Block Type	Select from the user-defined block types that have been defined in the system. This assigns this block a specific type. The list that is displayed in the block type list is controlled by rules defined in the container maintenance option.
IP Address Version	Select the version of IP Address space that you are adding to the system, IPv4 or IPv6 . Note that the license key controls which versions of IP Address space are supported within the product.
Block Size	Select the block size that you are adding. The block sizes are listed in CIDR notation.
Allocation Strategy	Choose one of the following: <ul style="list-style-type: none"> To use the automated best fit allocation routine, select the Best fit option. IPv6 only. To use the automated random allocation routine, select the Random option. IPv6 only. To use the automated sparse allocation routine, select the Sparse option.
Exclude from Discovery	Select this checkbox if you want this address space to be ignored during the discovery process.
Discovery Agent	Allows you to specify the InControl Agent to be used to discover hosts on this subnet/block. Choose one of the following: <ul style="list-style-type: none"> Inherit from Parent Block – Indicates that the agent specified on the parent block is used for discovery. Inherit from Parent Container – Indicates that the agent specified on the container is used for discovery. Select Agent – Allows you to select and specify a specific agent that performs discovery for this subnet/block.
Interface IP Address	Interface IP Address(es) – Choose the number of IP addresses this block has on this interface. Typically, this is 1. However, there are some high-availability configurations where more than 1 is needed. If you are not sure, leave this at 1.
	Offset From Start – Specify the number of IP addresses you want to offset from the beginning of the subnet. The Interface Address is the Block Starting address plus this Offset. The default is 1.
	Default Gateway – Select this option to designate that the Interface IP Address is the default Gateway address.

Field	Description
Block Name	<p>Enter a name for the block. In addition to text, you can use the following tokens that are substituted after a site template is applied to a container:</p> <pre>%containername% %parentblocktype% %blocktype% %startaddrstring% %blocksize%</pre> <p>For example, the standard CIDR name for a block could be formed using: %startaddrstring%/%blocksize%</p> <p>Note: The block name appears on the container screen.</p>
Block Description	Enter a description of the block. In addition to text, you can use the tokens listed above.
Current Status	<p>The current status of this block. Choose one of the following:</p> <ul style="list-style-type: none"> • Aggregate – This block is an aggregate block. • In-Use/Deployed – The block is in use as a subnet. • In-Use/Fully Assigned – The block is in use and all IP Addresses are fully utilized. • Reserved – This block is reserved for future use.
Primary Subnet	Select this check box if the subnet you are creating should be the primary subnet. Otherwise, leave blank.
Create Reverse DNS Domain(s)	<p>When checked, the system automatically creates an in-addr.arpa reverse domain for this address space. You may optionally select the “type” if you have overlapping address space. DNS Domain Type values are defined within the System tab of the system.</p> <p>Note: This option only creates the reverse domain. You must still assign this domain to a DNS server or a DNS galaxy.</p>
Allocation Template	Select the allocation template to be used with the site allocation template. The allocation name and rules appear.

7. Select the **Policies** tab.

Figure 8-13 Add Block Sequence Policies Tab

8. Fill out the parameters, as described in the following table:

Table 8-5 Add Block Sequence Policies Parameters

Field	Description
Primary DHCP Server	Select the Primary DHCP server that serves this address space from the drop-down list.
Failover DHCP Server	Select the Failover DHCP server that serves this address space from the drop-down list.
Primary WINS Server	Enter the IP address of the Primary WINS Servers for this subnet. Used to provide this information to DHCP for Dynamic Address types. You may specify multiple IP addresses by typing them in a comma-separated format, for example: 192.168.1.1,192.168.1.2
DHCP Policy Set	Select the default DHCP Policy set to assign to dynamic devices on this subnet from the drop-down list.
DHCP Options Set	Select the default DHCP Option set to assign to dynamic devices on this subnet.
Forward Domains	Select the default DNS Forward domains for this subnet. These appear in the drop-down list when defining devices. If multiple domains are specified, then the default (indicated by an arrow) that is used when adding objects is the first one in the list. For more information on adding a forward domain, refer to “Searching for a Domain or a DNS Server.”
Reverse Domains	<i>Optional.</i> Select the default DNS Reverse domains for this subnet. This domain is used to hold DNS PTR records. If multiple domains are specified, then the default (indicated by an arrow) for adding objects is the first one in the list. If no default is specified, the system automatically calculates the correct reverse zone for DNS PTR records. For more information on adding a reverse domain, refer to “Searching for a Domain or a DNS Server.”

Field	Description
DNS Servers	Select the default DNS Servers for this subnet. Used to provide this information to DHCP for Dynamic Address types. If multiple DNS servers are specified, then the default that is used when adding objects is the first one in the list (an arrow appears next to the default). For more information on adding a DNS Server, refer to “Searching for a Domain or a DNS Server.”

9. Click **Submit**.

The block is added to the Add Site Allocation Template list (Figure 8-11 on page 287).

10. Choose from the following actions:

- ▶ To add another block, click **Add Block** and refer to step 5 above.
- ▶ To save the template, click **Submit**.
The message **Successfully saved Site Allocation Template: <templatename>** appears, and the template is added to the list in the Site Allocation Templates screen.




For information on invoking the template to create a site under the **Management > Management Containers** menu, refer to “Add Site” on page 31 (for Logical Containers) or “Add Site” on page 43 (for Device Containers).

Searching for a Domain or a DNS Server

To search for a domain or a DNS server in the **Policies** tab, follow these steps:

1. Click **Add Domains** or **Add DNS Server**.
2. Enter search criteria or leave blank to return all domains.
3. Click **Search**.
4. Select the **Add** check box beside each domain you want.
5. Click **Submit**.

The domain or DNS servers you selected appear in the **Policies** tab. If you selected more than one domain or server:

- ▶ To change the default, use the  or  buttons.
- ▶ To remove an entry altogether, select the entry you no longer want and click .

Editing a Site Allocation Template

You can modify a site allocation template that you no longer suits your original design. You can change the name, add new blocks, or modify and/or delete existing blocks. You cannot change the container type if the template has already been used to allocate blocks.

Note: Blocks already created using a specific site template will not change. Only new block allocations are affected by changes you make when you edit a site allocation template.

To edit a site allocation template, follow these steps:

1. Select the site template in the Site Template Name column that you want to modify.

The Edit Site Allocation Template screen opens.

Figure 8-14 Edit Site Allocation Template


2. Choose from the following actions:
 - ▶ To add another block, select **Add Block**, and follow the instructions in “Adding a Site Allocation Template” on page 286.
 - ▶ To modify an existing block, click **Edit** beside the block you want to change. Follow the instructions in “Adding a Site Allocation Template” on page 286.
 - ▶ To delete an existing block, click **Delete** beside the block you no longer want. The block is immediately removed.
3. When you have completed your changes, choose one of the following actions:
 - ▶ To save, click **Submit**.
 - ▶ To not save, click **Cancel**.

Deleting a Site Allocation Template

You can delete a site allocation template that you no longer need.

Note: Blocks already created using a specific site template will not be deleted.

Follow these steps:

1. Select the check box next to the site template in the Site Template Name column that you want to delete.
2. Click .

The message Are you sure? appears.

3. Click **OK**.

The site template is removed from the Site Template Name column.

RIR Organization IDs

This section describes the setup and maintenance of Regional Internet Registry Organizations. RIR Organizations are used to organize and define information that is associated to your address space. This includes information that is needed and/or required for reporting purposes by internet registries such as ARIN or RIPE. When an organization gets a new allocation of IP Address space from an Regional Internet Registry (RIR), the address space is essentially registered to that organization. The RIR assigns an identification number to each organization, which is sometimes referred to as an Organization ID (OrgID) or “organization”. This OrgID needs to be associated with the root block and all subsequent descendant blocks to facilitate tracking and proper utilization reporting. For instance, showing utilization by OrgID helps an organization when it becomes time to request more space from the RIR.

When the Regional Internet Registry Organizations icon or link is selected, the existing Organizations, if any, are shown.



Figure 8-15 Regional Internet Registry

Choose from the following actions.

- To delete one or more organizations, click the checkbox in the Select column for each item you wish to clear, and click . You are prompted for confirmation. Click **OK** to delete the selected Organizations, or cancel to return to the previous screen.
- To add a new Organization, click the **Add Organization** link. The Add Organization screen appears.

Add Organization

Organization Name:

Organization ID:

Registry:

Description:

Address:

City:

State/Province:

Postal Code:

Country Code:

Admin Contact:

Tech Contact:

Authorization Type:

Password:

Confirm Password:

Email Update to:

Notify Email to:

Figure 8-16 Add Organization

Table 8-6 Add Organization Parameters

Field Name	Usage
Organization Name	The name of this organization. The organization (or division within an organization) who manages the network.
Organization ID	(OrgID) A unique identifier of an organization.
Registry	Select the internet registry that this Organization will apply to.
Description	Enter a free text description for this Organization.
Address	Enter the address information for this Organization.
City	Enter the city of this Organization.
State/Province	Enter the state/province of this Organization.
Postal Code	Enter the postal code for this Organization.
Country Code	Enter the country code for this Organization.
Admin Contact	Enter the administrative contact information for this Organization.
Tech Contact	Enter the technical contact information for this Organization.
Authorization Type	When submitting an update that requires authorization, authentication information valid for this organization should be supplied. Different methods require different authentication information. Refer to the Internet Registry Documentation for additional details.
Password	Required for an Authentication Type of MD5-PW.
Confirm Password	Required for an Authentication Type of MD5-PW.

Field Name	Usage
Email Update to	Email address to send updates that occur to blocks assigned to this organization.
Notify Email to	Notify email address to send updates that occur to blocks assigned to this organization.

Fill in the fields with the desired values, and click **Submit** to store the definition. Or click **Cancel** to return to the previous screen.

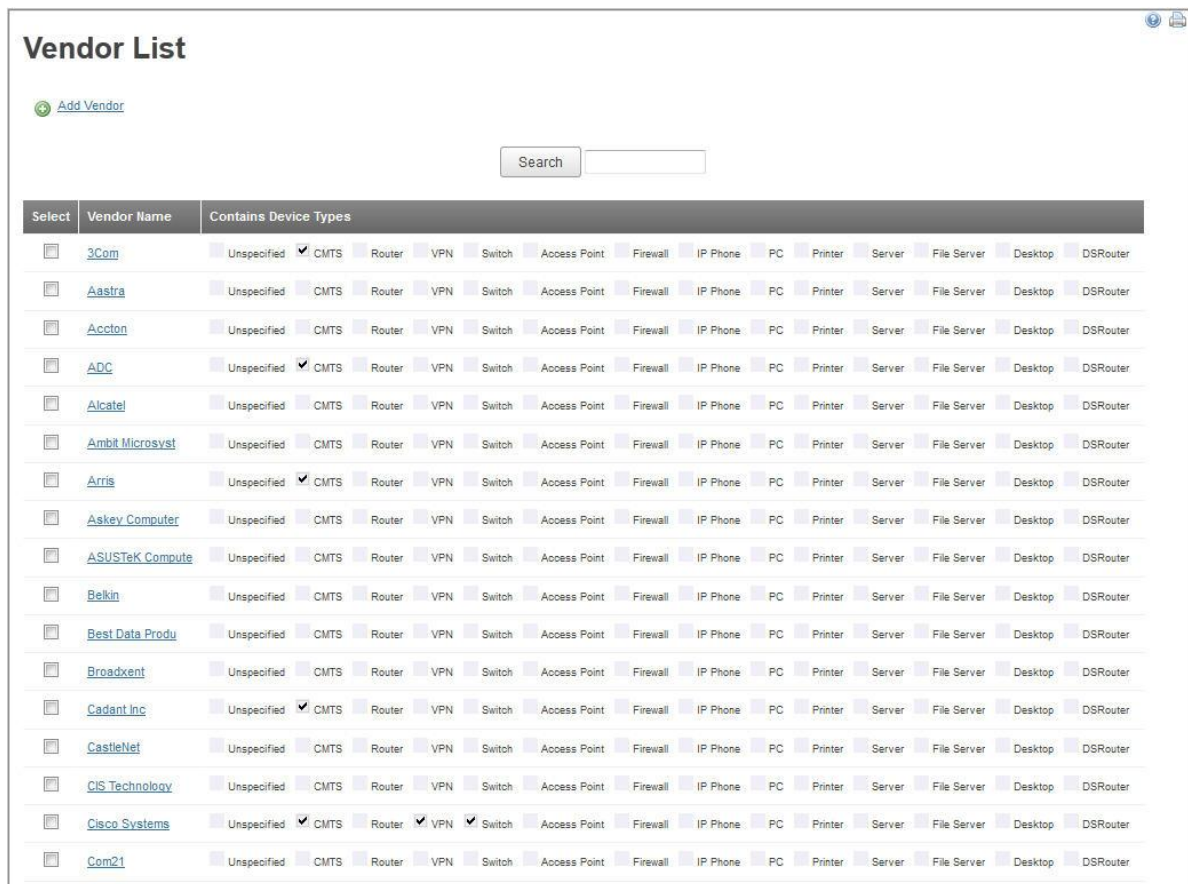
Chapter 9 Working with IP/Devices

Vendor/Models

Use the Vendor List screen to maintain the list of networking equipment vendors and their models. This section is divided into two parts: Vendor Maintenance and Model Maintenance. Vendors are maintained in the Vendor List, while types and models of equipment are maintained by selecting a specific vendor.

Vendor Maintenance

When you first choose **Vendor/Models** from the **Tools** menu, you are presented with a list of the vendors in the system, as shown in Figure 9-1.



The screenshot shows the 'Vendor List' interface. At the top, there is a title 'Vendor List' and an 'Add Vendor' button. Below the title is a search bar with a 'Search' button. The main part of the interface is a table with columns 'Select', 'Vendor Name', and 'Contains Device Types'. The table lists 20 vendors, each with a checkbox in the 'Select' column and a row of checkboxes in the 'Contains Device Types' column. The vendors listed are 3Com, Aastra, Accton, ADC, Alcatel, Ambit Microsyst, Arris, Askey Computer, ASUSTeK Compute, Belkin, Best Data Produ, Broadxent, Cadant Inc, CastleNet, CIS Technology, Cisco Systems, and Com21. The 'Contains Device Types' column includes checkboxes for Unspecified, CMTS, Router, VPN, Switch, Access Point, Firewall, IP Phone, PC, Printer, Server, File Server, Desktop, and DSRouter. Some checkboxes are checked, such as 'CMTS' for 3Com, 'CMTS' for Aastra, 'CMTS' for Accton, 'CMTS' for ADC, 'CMTS' for Alcatel, 'CMTS' for Ambit Microsyst, 'CMTS' for Arris, 'CMTS' for Askey Computer, 'CMTS' for ASUSTeK Compute, 'CMTS' for Belkin, 'CMTS' for Best Data Produ, 'CMTS' for Broadxent, 'CMTS' for Cadant Inc, 'CMTS' for CastleNet, 'CMTS' for CIS Technology, 'CMTS' for Cisco Systems, and 'CMTS' for Com21. Additionally, 'Router' is checked for Cisco Systems, 'VPN' is checked for Cisco Systems, and 'Switch' is checked for Cisco Systems.

Select	Vendor Name	Contains Device Types
<input type="checkbox"/>	3Com	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	Aastra	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	Accton	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	ADC	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	Alcatel	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	Ambit Microsyst	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	Arris	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	Askey Computer	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	ASUSTeK Compute	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	Belkin	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	Best Data Produ	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	Broadxent	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	Cadant Inc	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	CastleNet	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	CIS Technology	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	Cisco Systems	Unspecified <input checked="" type="checkbox"/> CMTS Router <input checked="" type="checkbox"/> VPN <input checked="" type="checkbox"/> Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter
<input type="checkbox"/>	Com21	Unspecified <input checked="" type="checkbox"/> CMTS Router VPN Switch Access Point Firewall IP Phone PC Printer Server File Server Desktop DSRouter

Figure 9-1 Vendor List

This list has been truncated for this document; the list of vendors maintained in IPControl is much longer. Note the following columns:

- **Select** – used to select a vendor or vendors for deletion.
- **Vendor Name** – the manufacturer of network equipment.
- **Contains Device Types** – allows you to see at a glance which types of equipment you have related to this vendor. In the figure above, 3Com has one or more CMTSs associated with it, and no routers, VPN gateways, or network switches. The same applies to ADC and Arris.

Choose from the following actions:

- To search for a particular vendor, enter a search string into the text block and hit Search.
- To delete one or more vendors, click the checkbox in the Select column for each item you wish to delete, and click **Delete Selected**. You are prompted for confirmation. Click **OK** to delete the selected vendors, or **Cancel** to return to the previous screen.

Note: When you delete a vendor, all models associated with the vendor are also deleted.

- To add a vendor, click the **Add Vendor** link.

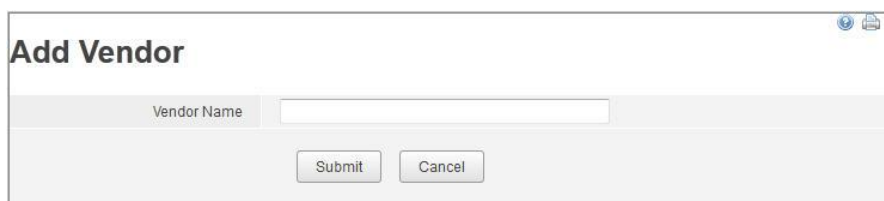


Figure 9-2 Add Vendor

Table 9-1 Vendor Parameters

Field	Description
Vendor Name	The name of the equipment manufacturer.

Click **Submit** to add the vendor, or **Cancel** to return to the previous screen.

Model Maintenance

Models of equipment are related to vendors. To add, change, or remove equipment models associated with vendors, follow these steps:

1. Pull up the vendor list.
2. Find the vendor of the equipment you wish to add, and click on their name. The Edit Vendor page opens.

Figure 9-3 Edit Vendor

3. In the **Model List** area, choose the type of device to add from the **Device Type Filter** drop-down list. This updates the Model List at the bottom of the screen and also updates the original **Add Model** link in the Model List to read **Add <device> Model**, where <device> is the type of device you are adding. Select this link to open the Add Model screen.

Figure 9-4 Add Model

The Vendor Name and Device Type are carried over from the previous screen.

4. Enter the Model Name for the device to add.
5. Click **Submit** to add the device, or **Cancel** to return to the previous screen. If the device was successfully added, the new model appears in the Model List of the Modify Vendor screen. Also note that the device count in the **Device Type Filter** has been incremented by one.

To modify a model in the model list, follow these steps:

1. Select the respective Device Type in the Device Type Filter.
2. Click the name of the model. The Edit Model screen appears.
3. Modify the model name as desired.
4. Click **Submit**.

To delete one or more models in the model list, follow these steps:

1. Click the checkbox in the **Select** column for each item you wish to delete.
2. Click **Delete Selected**.

You are prompted for confirmation before deleting.

Device Types

Use this screen to maintain Device Types. Use **Device Types** to differentiate your individual IP addresses by function, type, or role. For example, you may want to distinguish between printers, routers, or standard laptops. This powerful feature enables the IPControl engine to distinguish between different types of devices when creating default host names, displaying user defined fields, and for reporting purposes. In addition, the use of device types allows administrators to tightly control how the IP Address space is allocated, and where that type of device can be deployed.

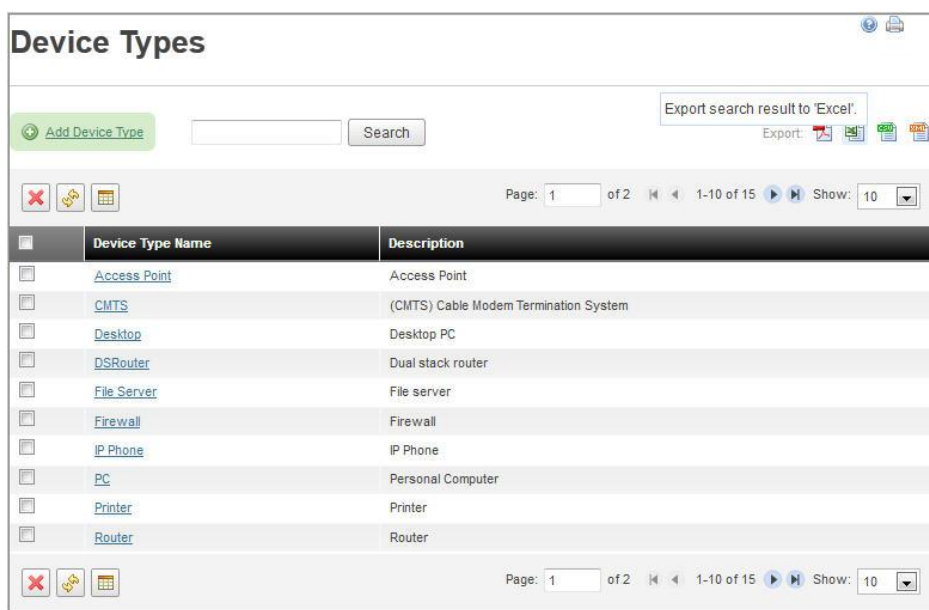


Figure 9-5 Device Types

Choose from the following actions:

- To delete one or more device type, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected device types, or **Cancel** to return to the Device Types screen.
- To refresh the display, click .
- To add a device type, click the **Add Device Type** link. The Add Device Type screen appears.

Figure 9-6 Add Device Type

Table 9-2 Device Type Parameters

Field	Description
Name	The name of the device type. This name will appear in drop-down lists, and on reports.
Description	An optional description that describes the device type.
Ignore devices of this type for Subnet Reclaim	When checked, devices defined with this Device type will be overlooked during a Subnet Reclaim.

Click **Submit** to add the device type, or **Cancel** to return to the Device Types screen.

Naming Policies

Use the Device Naming Policies screen to maintain Device Type Naming Policies. These policies allow you to standardize device names within your organization based on the device type. Using naming policies allows you to ensure unique host names for devices throughout your network. This is important if you are using DNS to help resolve the name to IP Address for your devices. A unique naming policy can optionally be assigned to each device type. When you create a device (allocate and IP Address), the system can optionally auto-generate the next available host name based on the policies you have established.

When you select **Naming Policies** from the IP/DEVICES section of the **Tools** menu, the existing device types and associated Naming Policy, if any, are shown.

	Device Type	Example
<input type="checkbox"/>	Access Point	ap-00001
<input type="checkbox"/>	CMTS	cmts00001
<input type="checkbox"/>	Desktop	corp-1-dtop
<input type="checkbox"/>	DSRouter	DSR-00001
<input type="checkbox"/>	File Server	fileserv-1
<input type="checkbox"/>	Firewall	fw-container-1
<input type="checkbox"/>	IP Phone	voip-container-1
<input type="checkbox"/>	PC	corp-pc-10-10-1
<input type="checkbox"/>	Printer	prtr-00001
<input type="checkbox"/>	Router	router-10-10-10-1

Figure 9-7 Device Naming Policies

Choose from the following actions.

- To delete one or more device naming policies, click the checkbox in the **Select** column for each item you wish to clear, and click . You are prompted for confirmation. Click **OK** to delete the selected device naming policies, or **Cancel** to return to the Device Naming Policies screen. Note that all device types are listed in this display, and naming policies are simply an association to these device types.
- To refresh the display, click .
- To add a naming policy for a device type, click the **Device Type** link. The Edit Naming Policy screen appears.

Figure 9-8 Edit Device Naming Policy

Table 9-3 Edit Device Naming Policy Parameters

Field	Description
Device Type	The name of the device type to which you are adding/editing the naming policy.
Example	An example of the naming policy that is established for this device type. Note: As you append

Click **Append Policy** to add the naming policy. You build up a naming policy by adding several components together.

A policy component line opens:

Figure 9-9 Device Naming Policy Component

Select the policy component type that you want to add:

Table 9-4 Device Naming Policy Parameters

Field	Description
Container Name	Displays the name of the container. The container name is used during the generation of the policy.
Free Text	Static text that is used during the generation of the policy.
IPv4 – Zero Filled	A dynamically generated component that is the IPv4 Address of a fixed sized, padded with zeros, without the dotted decimal notation. For example; 10.0.0.3 would generate the string 010000000003 198.200.121.2 would generate the string 198200121002
IPv4 – Dash Separated	A dynamically generated component that is the IPv4 Address, with dashes instead of dotted decimal notation. For example; 10.0.0.3 would generate the string 10-0-0-3 198.200.121.2 would generate the string 198-200-121-2
Incrementor	A dynamically generated global incrementor specifically unique for this naming policy. Each time this policy is used, a unique number will be generated.

Field	Description
Incrementor – Zero Filled	A dynamically generated global incrementor specifically unique for this naming policy. Each time this policy is used, a unique number will be generated. This field is padded to a fixed size of 5 characters. For example; 12 would generate the string 00012 1232 would generate the string 01232

Choose from the following actions.

- Click **Delete** on a line to remove a specific component of the naming policy.
- Click **Insert Row Above** to insert a new component of the naming policy above the current line.
- Click **Insert Row Below** to insert a new component of the naming policy below the current line.

Typically, the naming policy is a combination of static text, mixed with dynamic (system generated) components. The dynamic components ensure uniqueness of the host name.

Once you have completed modeling the naming policy, click **Submit** to save the naming policy, or **Cancel** to return to the Device Naming Policies screen.

Device Interface Template Maintenance

The Device Interface Templates List screen allows you to maintain device interface templates. A device interface template enables the IPControl administrator to define standard equipment interface configurations, and then duplicate those interface configurations easily across multiple devices (“Network Elements/Devices” on page 104) in IPControl.

To access the Device Interface Template List, select **Interface Templates** from the IP/DEVICES section of the **Tools** menu. The Device Interface Templates List screen opens, as shown in Figure 9-10.

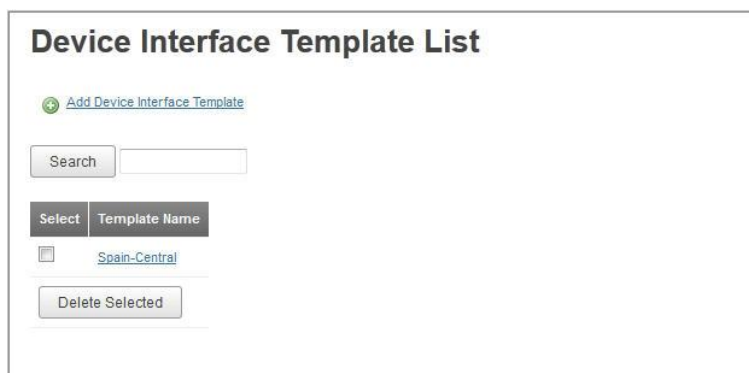


Figure 9-10 Device Interface List

Choose from the following actions:

- To search for a particular device template, enter a search string into the text block and hit Search.
- To delete one or more device templates, click the checkbox in the Select column for each item you wish to delete, and click **Delete Selected**. You are prompted for confirmation. Click **OK** to delete the selected device templates, or **Cancel** to return to the Device Interface Templates List screen.
- To add a device template, refer to next section.
- To edit a device template, refer to “Editing a Device Template” below.

Adding a Device Template

To add a device template, click the **Add Device Template** link. The Add Device Template screen appears.



Figure 9-11 Add Device Template

Table 9-5 Add Device Parameters

Field	Description
Template Name	Enter a name for the template.

Enter the desired template name. Click on the **Append Interface** button to add an interface to the template. The following screen appears.

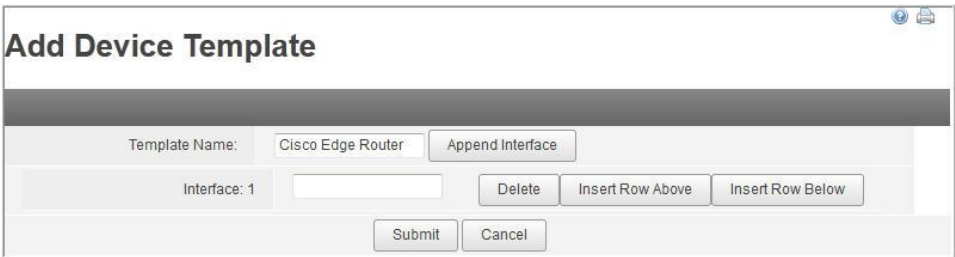


Figure 9-12 Add Device Template Interface

Assign a unique name to the interface. To add more interfaces, click the **Insert Row Above** or **Insert Row Below** button. To remove an interface, click its **Delete** button. Once finished, click **Submit** to save your changes, or **Cancel** to return to the Device Interface Templates List screen.

Editing a Device Template

To modify an existing device template, click on the template name in the Device Template List. This takes you to the Edit Device Interface Template screen.

Edit Device Interface Template			
Template Name:	Cisco Edge Router	Append Interface	
Interface 1:	eth1	Delete	Insert Row Above Insert Row Below
Interface 2:	eth2	Delete	Insert Row Above Insert Row Below
Interface 3:	eth3	Delete	Insert Row Above Insert Row Below
		Submit	Cancel

Figure 9-13 Edit Device Template

Edit the template fields as needed. You may change the name of the template in the **Template Name** field, or add/remove interfaces using the **Delete** or **Insert** buttons. Once finished, click **Submit** to save your changes, or **Cancel** to return to the Device Interface Templates List screen.

Chapter 10 Using Other Tools

Threshold Sets

Thresholds and Threshold Sets alert administrators when a particular condition occurs within IPControl. For example, you can configure IPControl to alert an administrator when the allocated IP addresses in a block exceed 90% of its capacity.

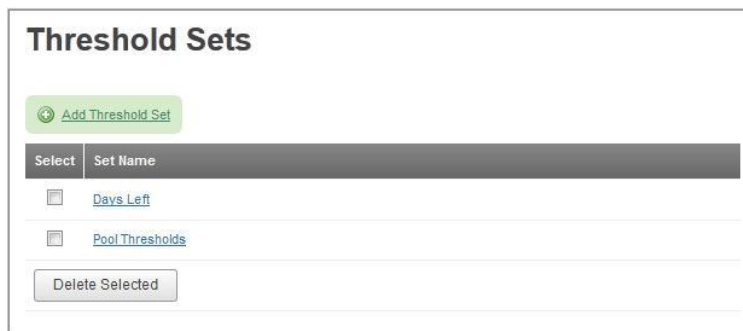


Figure 10-1 Threshold Sets

To use this feature, there are three steps:

1. Define a Threshold Set.
2. Add one or more Thresholds to the Threshold Set.
3. Associate a Threshold Set with a Container/Blocktype pair, a Block, or a Network Service.

This section describes steps 1 and 2. Refer to “Threshold Alert” on page 310 for instructions on Step 3.

To add a threshold set, click the **Add Threshold Set** link. The **Set Name** field and **Save** button appear, as shown in Figure 10-2.

Threshold Sets

[Add Threshold Set](#)

Set Name

Select	Set Name
<input type="checkbox"/>	Days Left
<input type="checkbox"/>	Pool Thresholds

Figure 10-2 Add Threshold Set

Enter the desired name and click **Save**. The new Threshold Set appears in the list.

To delete a threshold set, check the box next to it and click the **Delete Selected** button. You are prompted for confirmation. Click **OK** to delete the selected Threshold Sets, or **Cancel** to return to the Threshold Sets screen.

Editing a Threshold Set

Once the Threshold Set is created, the next step is to add individual Thresholds. Follow these steps:

1. Click on a **Set Name** link to display the **Edit Threshold Set** screen.

Edit Threshold Set: Days Left

[Add Threshold](#)

Set Name

Severity	Variable	Type	Comparator	Value	Confidence		
Warn	Available	Absolute	<=	10	0.0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Warn	Days Left	Absolute	<=	30	0.85	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Critical	Assigned	Percent	>	90	0.0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

Figure 10-3 Edit Threshold Set

2. Click on the **Add Threshold** link. The **Create Threshold** dialog box opens.



Figure 10-4 Create Threshold

3. Make your field selections, as described in Table 10-1.

Table 10-1 Create Threshold Parameters

Field Name	Usage
Severity	Choose one of Critical, Warn, or Info to indicate the importance of this condition.
Variable	Choose one of the following: <ul style="list-style-type: none"> Allocated, Assigned, and Available refer to the number of IP addresses in those categories in a block or address pool. Days Left refers to the calculated time remaining before the block or address pool runs out of space. Dynamic Available refers to the number of dynamic IP addresses that are available. Dynamic Days left refers to the calculated time remaining before the block or address pool runs out of dynamic space.
Type	Choose one of Percent or Absolute. This tells IPControl how to interpret the Value field.
Comparator	Choose one of >, >=, =, <, <=. This specifies the comparison between Variable and Value that triggers the Threshold.
Value	Enter the value that triggers the Threshold. If the Type is Percent, enter a value between 1 and 100.
Confidence	Specify a number between 0.0 and 1.0. This only applies when the Variable is Days Left. It specifies that the threshold is crossed <i>only</i> if the comparison of Days Left and Value is true <i>and</i> the confidence calculated (R2 or R-Squared) for Days Left is greater than this number.

4. Click **Submit** to add the threshold to the Threshold Set.
5. Choose from the following actions:
 - To edit a threshold, click the **Edit** button beside the threshold you want to edit.
 - To delete a threshold, click the **Delete** button beside the threshold you want to delete. At the Are you sure? prompt, click **OK**.

- To return to the Threshold Set page, click **Cancel**.

Threshold Alerts

Use the Alerts screen to enable Container, Block or Network Service alerts. Refer to “Threshold Set” on page 307 for instructions on defining Threshold Sets and Thresholds. Refer to “Alert Log” on page 246 for instructions on viewing pending alerts.

To access Alerts, select **Threshold Alerts** from the OTHER section of the **Tools** menu. The Alerts screen opens, as shown in Figure 10-5.

Container Name	Apply to Children	IP Address Version	Block Type	Threshold Set

Figure 10-5 Threshold Alerts

Container Alerts

When an alert is defined for a Logical Container, the alert is raised when the total space for a given block type triggers the conditions in the Threshold Set.

For a Device Container, the alert is raised when the total space for a given block type on any of the device’s interfaces triggers the conditions in the Threshold Set.

To set up a Container Alert, follow these steps.

1. Click on the **Add Container** link. The Container Search dialog box opens.

Figure 10-6 Container Search

2. Check the **Apply to Children** box if you wish this Alert to apply to this container and all its children. Leave it unchecked to have it apply only to this container.
3. Select the **IP Address Version** to which this Threshold Set will apply.
4. Select the **Block Type** to which this Threshold Set will apply.

Note: **Any** is a Block Type of its own, and does *not* mean that all Block Types are included.

5. Select the Container to which this Threshold Set will apply.
6. Once finished, click **Submit**.

The selected container name appears in the new row in the Container Alerts section and the new alert threshold has been created.

To delete an alert from a Container, click the **Delete** button on its row. You are prompted for confirmation. Click **OK** to delete the selected block types, or cancel to return to the Alerts screen. Note that the **Any** block type cannot be deleted.

Block Alerts

When an Alert is defined for a Block, the Alert is raised when the variables in that Block trigger the conditions in an associated Threshold Set.

To set up a Block Alert, follow these steps.

1. In the Alerts screen, select the **Block Alerts** tab.

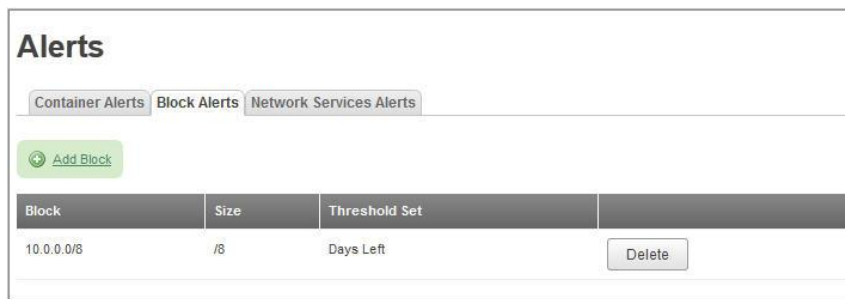


Figure 10-7 Block Alerts Tab

2. Click on the **Add Block** link. The Block Search dialog box opens.

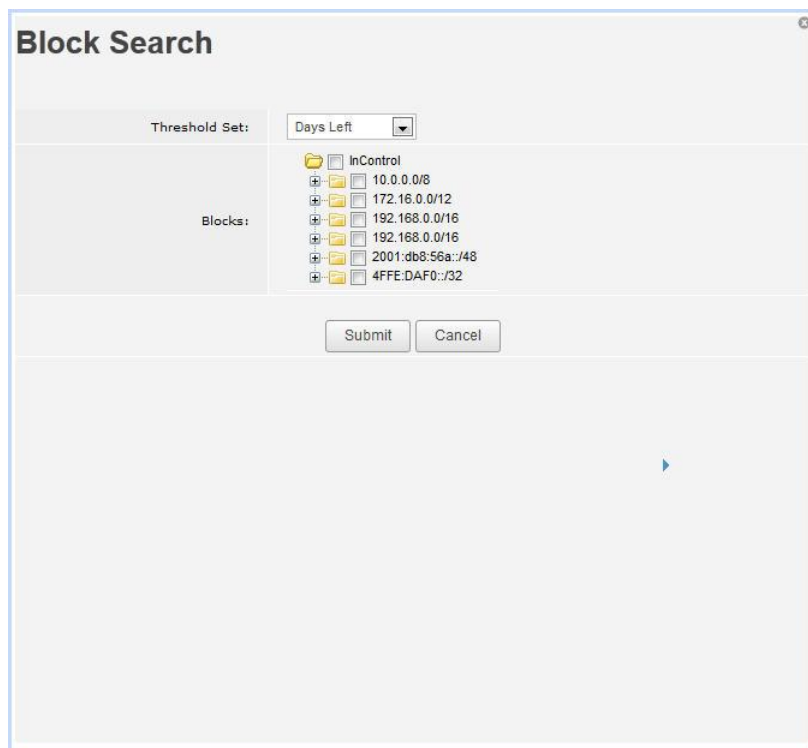


Figure 10-8 Block Search

3. Select a Threshold Set from the **Threshold Set** dropdown list.
4. Select a block by checking the checkbox next to it in the **Blocks** hierarchy.
3. Click **Submit**.

The selected block appears in the **Block Alerts** section.

To delete an alert from a Block, click the **Delete** button on its row. You are prompted for confirmation. Click **OK** to delete the selected block types, or **Cancel** to return to the Alerts screen.

Network Service Alerts

When an Alert is defined for a Network Service, the Alert is raised when any of the Address Pools managed by that Network Service triggers the conditions in the Threshold Set. If there are shared Address Pools, they are aggregated before testing the threshold.

To set up a Network Service Alert, follow these steps.

1. In the Alerts screen, select the **Network Services Alerts** tab.

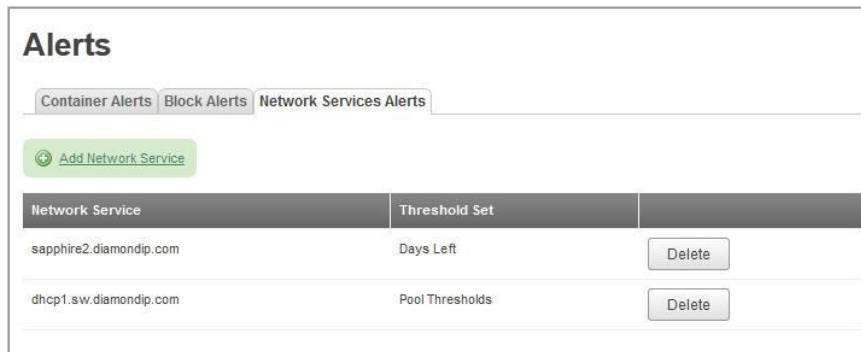


Figure 10-9 Network Services Alerts Tab

- Click the **Add Network Service** link. The Network Service Search dialog box opens.

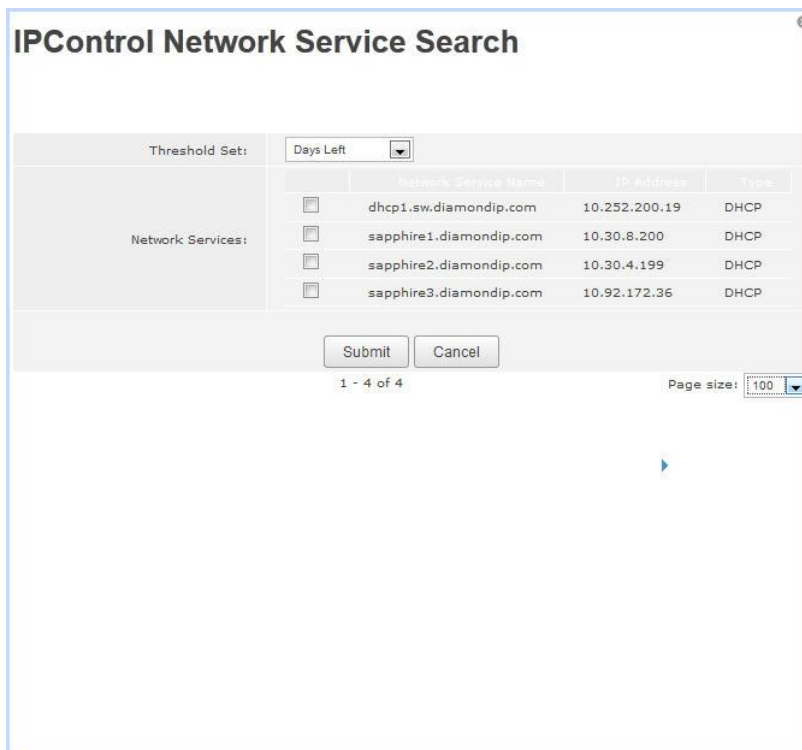


Figure 10-10 Network Service Search

- Choose a **Threshold Set** from the drop-down list.
- Select the desired Network Services by selecting the corresponding checkboxes.
- Click **Submit**. The new Alert Threshold is set.

To delete an alert, click the **Delete** button beside the alert you want to remove. . You are prompted for confirmation. Click **OK** to delete the selected network service alert, or **Cancel** to return to the Alerts screen.

User-Defined Fields

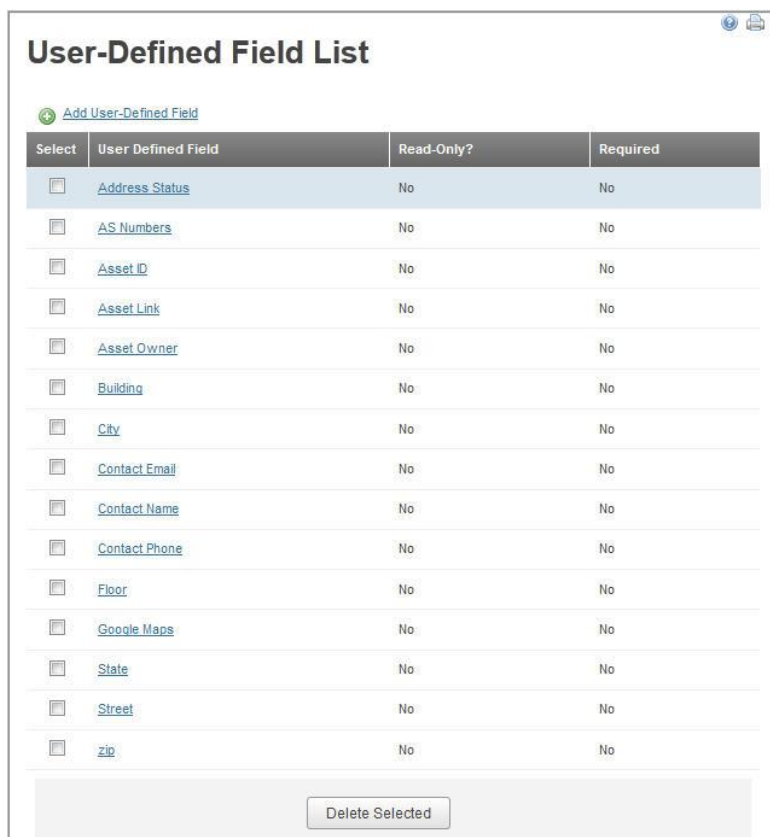
This section describes the setup and maintenance of user-defined fields.

User-defined fields allow the user to attach arbitrary data elements to containers, subnets, and IP addresses. For example, you could define a field called Customer ID to track blocks allocated to a particular customer, or a field called Asset Tag to track asset information about a specific device using an IP address.

There are three steps to defining user-defined fields and attaching them to subnets or IP addresses:

1. Create the user-defined field.
2. Create the Information Template and select the desired user-defined fields.
3. Attach the Information Template to a Container-Block (Subnet) pair, or a Container-IP Address (via Device Type) pair.

To access the User-Defined Field List, select **User Defined Fields** from the OTHER section of the **Tools** menu.



Select	User Defined Field	Read-Only?	Required
<input type="checkbox"/>	Address Status	No	No
<input type="checkbox"/>	AS Numbers	No	No
<input type="checkbox"/>	Asset ID	No	No
<input type="checkbox"/>	Asset Link	No	No
<input type="checkbox"/>	Asset Owner	No	No
<input type="checkbox"/>	Building	No	No
<input type="checkbox"/>	City	No	No
<input type="checkbox"/>	Contact Email	No	No
<input type="checkbox"/>	Contact Name	No	No
<input type="checkbox"/>	Contact Phone	No	No
<input type="checkbox"/>	Floor	No	No
<input type="checkbox"/>	Google Maps	No	No
<input type="checkbox"/>	State	No	No
<input type="checkbox"/>	Street	No	No
<input type="checkbox"/>	zip	No	No

Figure 10-11 User-Defined Field List

To add a user-defined field, follow these steps.

1. Click on the **Add User-Defined Field** link. The Add User-Defined Field screen opens.

Add User-Defined Field

Display Title:

Field Name/Tag:

Value Data Type:

Default Value:

Read-Only?: ☐

Required: ☐

Information Templates which include this field:

Asset	<input type="checkbox"/>
Contact	<input type="checkbox"/>
Geolocation	<input type="checkbox"/>
Location	<input type="checkbox"/>

Figure 10-12 Add User-Defined Field

- Fill in the fields with the desired values, as described in Table 10-2.

Table 10-2 Add User-Defined Field Parameters

Field Name	Usage
Display Title	The label displayed on input forms for this field.
Field Name/Tag	The name of this field. This name must be unique from other User-Defined Fields and must be made up of alphanumeric characters and underscores. No spaces are allowed.
Default Value	Choose the default value for this field if the user does not supply one on an input form. Note: this field is required if the Read-Only option is selected, or if the Data Type is Hidden.
Value Data Type	This controls how the data element is displayed on input forms. Choose one of Text, Checkbox, Radio Button, Text area, List, Hidden, or URL.

Field Name	Usage
URL Template	<p>Only visible if Data Type is URL. Enter the URL that will be used to call a different web screen. You may use FIELD TOKENS to represent the data of other fields on the screen. For example:</p> <pre></pre> <p>Valid field tokens include:</p> <ul style="list-style-type: none"> Device Level Tokens: hostname, description, fqdn, hwaddr, deviceTypeString, hostOperatingSystem, domainName, ipaddress Note: All user-defined fields using the “Field name/Tag” Block Level Tokens: name, blockstatus, blocksize, blocksizehosts, rootblock, rootblocktype, privateaddrspace, startaddrstring, servicetype, swipname Note: All user defined fields using the “Field name/Tag” Container Level Tokens: name, type, notes, createAdmin, createdate Note: All user defined fields using the “Field name/Tag”
Read Only	<p>Check this box for a read-only field.</p> <p>Note: The Default value is required for this option.</p>
Required	Check this box if the field cannot be left blank.

- Click **Save** to store the definition.

If you have already defined some Information Templates (see “Information Template” on page 318), you see them listed below the input fields.

You can associate the UDF with a template by checking that template’s box before clicking **Submit**.

Creating Radio Button and List Values

If you choose a **Value Data Type** of Radio Button or List, you must provide a list of the acceptable values for the field. A new window pops up where you can enter those values.

Define Options For Radio Button - Mozilla Firefox

198.134.150.61/incontrol/user_defined fld/selectedlist.do?id=0&dataType=Radio_Button

Define Options For Radio Button

Label

Value

Add new option

Select	Label	Value
--------	-------	-------

Save Cancel

Figure 10-13 Define Radio Button

Follow these steps.

1. Enter the form label for one of the allowed values in the **Label** field.
2. Enter its associated value in the **Value** field. The contents of the **Value** field is what is actually saved when a Block is saved.
3. Click **Add new option** to add the Label-Value pair to the acceptable values for this field. It appears in the list below.

Define Options For Radio Button - Mozilla Firefox

198.134.150.61/incontrol/user_defined fld/selectedlist.do?id=0&dataType=Radio_Button

Define Options For Radio Button

Label

Value

Add new option

Select	Label	Value
<input type="radio"/>	SouthEast	SE

Up
Down
Delete

Save Cancel

Figure 10-14 Options for Radio Button Definition

4. Choose one of the following actions.
 - ▶ To add additional options, simply repeat the process.
 - ▶ To edit existing options, change the contents of the **Label** or **Value** fields on the desired row.
 - ▶ To delete an option, check the **Select** box for that row, and click the **Delete Selected** button.
5. To save the additions, changes and deletions, click the **Save** button. The pop-up window closes.

Information Templates

Information Templates are groups of User-Defined Fields. A User-Defined Field can only be associated with a block through an Information Template.

To add an Information Template, follow these steps.

1. Select **Information Templates** from the OTHER section of the **Tools** menu. The Information Template List screen opens.

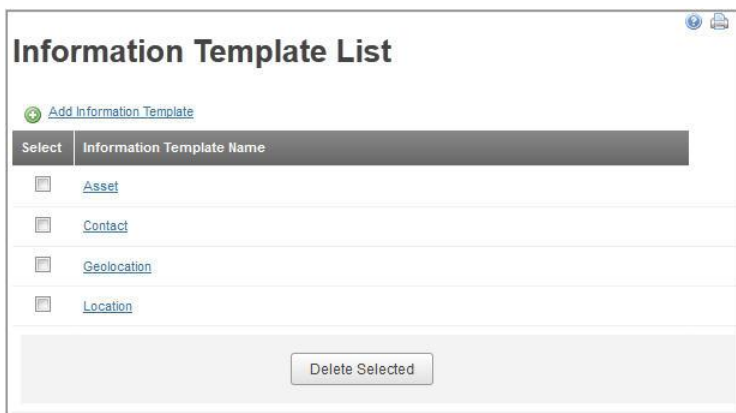


Figure 10-15 Information Template List

2. Click the **Add Information Template** link. The Add Information Template screen opens.

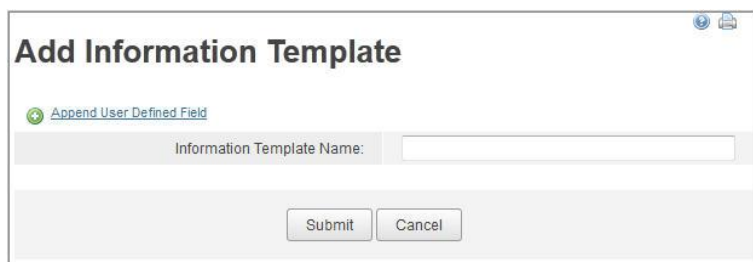


Figure 10-16 Add Information Template

3. Enter the desired name in the **Information Template Name** field.

- To attach a User Defined Field to this template, click the **Append User Defined Field** link. The Append UDFs (User Defined Fields) to Information Template dialog box opens, as shown in Figure 10-17.

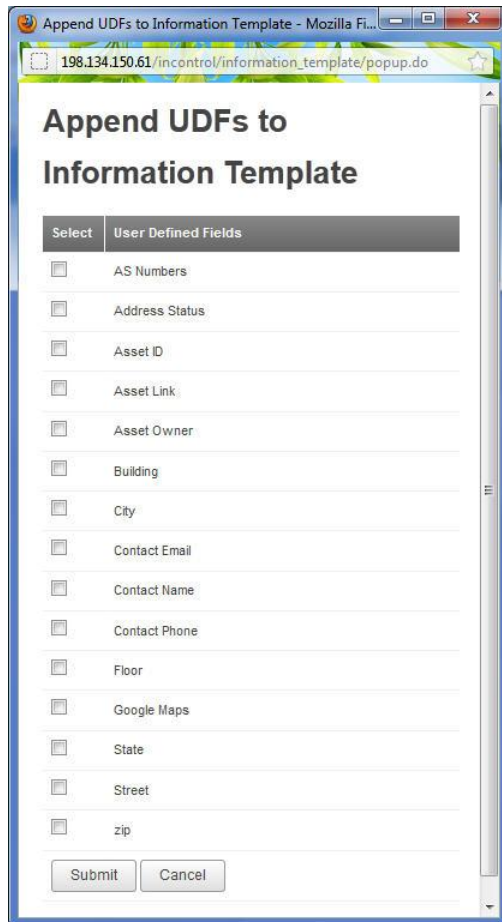


Figure 10-17 Append UDFs to Information Template

- Select the checkbox next to the fields to include with this user defined field template.
- Click **Submit** to attach these fields. The Add Information Template opens.

Add Information Template

[Append User Defined Field](#)

Information Template Name:

Field Name	List Display?	
Asset ID	<input checked="" type="checkbox"/>	Up Down Delete
Asset Link	<input checked="" type="checkbox"/>	Up Down Delete
Asset Owner	<input checked="" type="checkbox"/>	Up Down Delete

Submit Cancel

Figure 10-18 Add Information Template with Selected UDFs

- Choose how the UDFs are displayed, as described in Table 10-3.

Table 10-3 Add Information Template Parameters

Field Name	Usage
Field Name	The name of the user-defined field.
List Display?	Determines whether this user-defined field is displayed on main-level lists, such as the block list in the Management Containers screen, or the subnet list when viewing individual IP addresses.
Sequencing	Use the Up and Down buttons to arrange the order in which user-defined fields are displayed on the screen. Use the Delete button to remove a UDF entry from a template.

- Click **Submit** to save the new Information Template. The template appears in the Information Template List.

After you have saved the new template, you can activate it by choosing the template in the Edit Container screen (Container Maintenance on the Management menu). There, you can choose a template to be associated with a given Block Type within that Container, as shown in Figure 10-19.

Edit Container

Container: South America

General Information: InControl / Americas / South America

Type:	Logical
Name:	South America
Discovery Agent:	<input checked="" type="radio"/> Inherit from Parent Container <input type="radio"/> Select Agent Executive Agent
Description:	Expansion networks in Latin America
Information Template:	<div> Geolocation Location South America </div> <small>Press Ctrl-Click to select multiple information templates</small>
Asset ID:	SA001-97865
Asset Link:	View IP Asset
Asset Owner:	<input type="radio"/> Engineering <input type="radio"/> Development <input type="radio"/> Finance <input checked="" type="radio"/> Corporate
Building:	Los Torres Blancos
City:	Curitiba
Contact Email:	mquintero@example.com
Maintain History Records:	<input checked="" type="checkbox"/> (Checked=Yes)

Policy: Valid Block Types

☒ **Enable or disable all Block Types** - This screen allows you to configure the valid Block Types that can be used with this Management Container. Select the valid Block Types below by selecting the checkbox next to the type.

Block Types	Select
Any	<input type="checkbox"/>
Data	<input checked="" type="checkbox"/>

Figure 10-19 Information Template Selected for Data Block Type

Refer to “Rules Tabs” on page 100 for further information.

Once you have that set up, the next time you create or edit a block of that type in that Container, the User-Defined Fields appear on the input form.

IDN Converter

Internationalized Domain Names use characters drawn from a large repertoire (Unicode). IDNA (Internationalized Domain Names for Applications) as described in RFC 3490 allows the non-ASCII characters to be represented using only the ASCII characters already allowed in so-called host names today. This backward-compatible representation is required in existing protocols like DNS, so that IDNs can be introduced with no changes to the existing infrastructure.

IDNA is only meant for processing domain names, not other text.

IPControl supports IDNA as defined in RFC 3490. It allows for data to be entered using Unicode characters and ASCII characters both when entering domain names. IPControl also gives the users


the ability to switch between IDN and ASCII when viewing the data. The underlying data is always stored as ASCII or ASCII Compatible encoding (ACE).

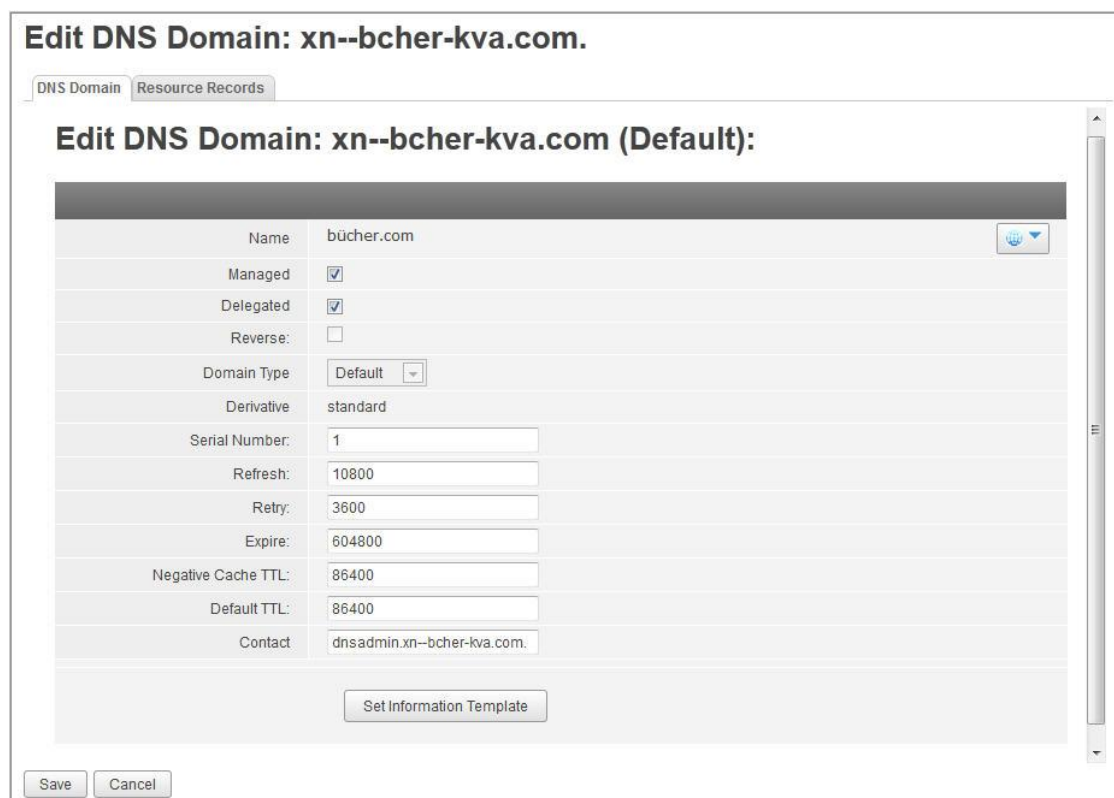
For example, for Internationalized Domain name 'bücher.com', the ACE equivalent is 'xn--bcher-kva'.

UI Treatment

Screens involving domain names, FQDNs and hostnames in case of domains/zones and owner and RDATA fields in case of resource records get special treatment for IDN support.

If an internationalized domain name is entered, hover the cursor over the IDN (Unicode character set) to see the ACE equivalent, as shown in Figure 10-20.

Whenever an Internationalized Domain Name is displayed, a  dropdown icon appears on the far right of the screen. Click the icon to toggle between IDN and ACE domain names.



Edit DNS Domain: xn--bcher-kva.com.

Edit DNS Domain: xn--bcher-kva.com (Default):


Name	bücher.com	
Managed	<input checked="" type="checkbox"/>	
Delegated	<input checked="" type="checkbox"/>	
Reverse	<input type="checkbox"/>	
Domain Type	Default	
Derivative	standard	
Serial Number	1	
Refresh	10800	
Retry	3600	
Expire	604800	
Negative Cache TTL	86400	
Default TTL	86400	
Contact	dnsadmin.xn--bcher-kva.com.	

Figure 10-20 Edit DNS Domain

Add/Edit Resource Records

Fields that participate in FQDN construction or store FQDN allow Unicode characters. For example:

- Owner field for A, AAAA records
- Data fields for PTR

- Alias and Data (Canonical Domain Name) fields for CNAME

Add/Edit IP Address

Unicode characters are supported in the Add/Edit IP Address screen since users can enter hostnames for the device that may appear in the resource records attached to a device in the form of a FQDN. If an internationalized hostname is entered, hover the cursor over the IDN (Unicode character set) to see the ACE equivalent.

Add/Edit Zone

The read-only Domain name field supports Unicode characters. If an internationalized domain name is entered, hover the cursor over the IDN (Unicode character set) to see the ACE equivalent.

Note: Although the file name field is auto-generated using the domain name, IPControl uses the ASCII name and not Unicode characters.

Search and IDN

Domain and resource record searches in IPControl are performed using the ASCII representations. If you have Internationalized Domain Names, put full IDN domain name or full/partial ASCII domain name in the search box to get back the desired result. Partial IDN search will not work.

For example, to search domain “bücher.com”, you may enter “bücher.com” or “xn--bcher-kva” (ASCII Compatible representation) or any part of the ASCII compatible name (for example, “bch”) and get back the desired result.

However, putting “büc” does not return the domain “bücher.com” since the searches are performed using the ASCII equivalent.

Chapter 11 Managing Appliances

Appliance Definition

Use the Appliance List screen to manage the INS Sapphire Appliances used by InControl.



Figure 11-1 Sapphire Appliance List

When you select **Appliance Definition** from the APPLIANCES section of the **Tools** menu, existing appliances, if any, are shown.

Choose from the following actions:


- To search for a particular appliance, enter a search string into the text block and click **Search**.
- To delete one or more appliances, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected appliances, or **Cancel** to return to the previous screen.
- To add a new appliance, click the **Add Appliance** link. The Add Appliance screen appears.

Figure 11-2 Add Sapphire Appliance

Table 11-1 Parameters

Field	Description
Name	The name of the appliance, in either simple or fully-qualified form.
IP Address	The IP address of the appliance. This is used by the InControl Executive to connect to the appliance.
Type	Choose from either Standard or High Availability. This will reflect either a Standalone or a Twin Mirror (High Availability) Agent in the Appliance Dashboard.
DNS	Choose this checkbox if this appliance will be used as a DNS server. A DNS Network Service will be automatically created in Management > DNS > Network Services if selected.
DHCP	Choose this checkbox if this appliance will be used as a DHCP server. A DHCP Network Service will be automatically created in Management > DHCP > Network Services if selected.

Click **Submit** to add/edit the agent, or **Cancel** to return to the previous screen.

Software Updates

The Application Version Management screen manages the software version of remote agents and Sapphire Appliances, allowing for bulk automated upgrading and downgrading.

To access Version Management screen, select **Software Updates** from the APPLIANCES section of the **Tools** menu. The Appliance Version Management screen opens, as shown in Figure 11-3.

Agent		IPControl	DNS	DHCP	Kernel	O/S
sapphire1.diamondip.com	Current	Not Set	Not Set	Not Set	Not Set	Not Set
	Desired	2.2.163	9.3.2	Not Set	Not Set	Not Set
sapphire2.diamondip.com	Current	Not Set	Not Set	Not Set	Not Set	Not Set
	Desired	2.2.163	9.3.2	Not Set	Not Set	Not Set
sapphire3.diamondip.com	Current	Not Set	Not Set	Not Set	Not Set	Not Set
	Desired	Not Set	Not Set	Not Set	Not Set	Not Set
sapphire4.diamondip.com	Current	Not Set	Not Set	Not Set	Not Set	Not Set
	Desired	Not Set	Not Set	Not Set	Not Set	Not Set

1 - 4 of 4 Apply Page size: 20

Figure 11-3 Appliance Version Management

The Application Version Management lists each appliance and the **Current** and **Desired** upgrade/downgrade schedule.

To upgrade an Appliance, set the **Desired** version for the Agent's component you wish to change, and then click **Apply**. Please be aware that no Desired versions will be available unless Software Packages have been registered on the Executive (see below). The next time that agent executes its Software Update function, it detects the change and downloads and installs the associated package.

Software Packages

The Software Packages screen lists the packaged software components contained in your installation of IPControl. It also enables you to load updated packages that you may receive from INS. The loaded packages can then be managed as described in "Software Updates" above.

Select	Product	Component	Version	File	Size	Registered	In-Use Count
<input type="checkbox"/>	INS IPControl	IPCONTROL	2.2.163	updatepkg-ipcontrol-2.2.163-signed.jar			0
<input type="checkbox"/>	INS Sapphire DNS	DNS	9.3.2	updatepkg-dns-9.3.2-signed.jar			0
<input type="checkbox"/>	INS Sapphire OS	OS	2.2.40	updatepkg-os-2.2.40-signed.jar			0

[Add Software Package](#)

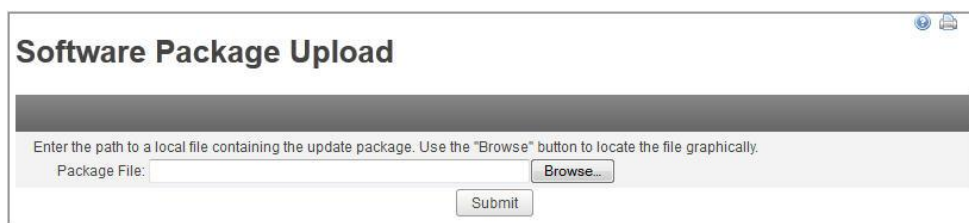
Delete Selected

Figure 11-4 Software Packages

This page always displays at least four fields for each package: the software product, its type and version, and the number of agents/appliances in your system that are running the software in the package. If there is a file containing the package loaded on your IPControl executive, some information about the file is also shown.

You may select one or more packages in the list and click **Delete Selected** to remove them from the IPControl executive. This does not remove them from the agents/appliances that are currently using them, but removes them from the **Desired** drop-down lists shown in “Software Updates” above.

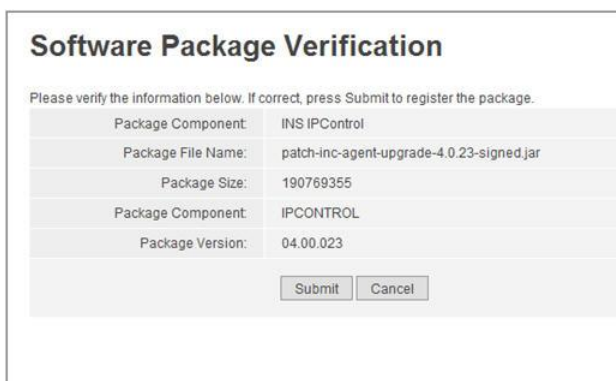
Clicking the **Add Software Package** link opens a file upload page.



The screenshot shows a web form titled "Software Package Upload". It has a dark header bar. Below the header, there is a text instruction: "Enter the path to a local file containing the update package. Use the 'Browse' button to locate the file graphically." The form contains a text input field labeled "Package File:" and a "Browse..." button. At the bottom of the form is a "Submit" button.

Figure 11-5 Software Package Upload

Here you can select a package file that you have received from BT Diamond IP, and load it onto the IPControl Executive. Only files that have been digitally signed by BT Diamond IP will be accepted. After uploading your file, the following screen shows you what package has been found inside.



The screenshot shows a web form titled "Software Package Verification". It has a light gray header bar. Below the header, there is a text instruction: "Please verify the information below. If correct, press Submit to register the package." The form contains a table with the following information:

Package Component:	INS IPControl
Package File Name:	patch-inc-agent-upgrade-4.0.23-signed.jar
Package Size:	190769355
Package Component:	IPCONTROL
Package Version:	04.00.023

At the bottom of the form are "Submit" and "Cancel" buttons.

Figure 11-6 Software Package Verification

Once the package has been verified, it appears on the listing of software packages and can be selected for the **Desired** version on the Appliance Version Management screen.

Chapter 12 Managing Administrators

Administrator Definition

Use the Administrator List screen to maintain IPControl administrators. Administrators have their own login credentials, and are assigned to specific Administrator Roles which control access to the system components.

To access the Administrator List, select **Administrator Definition** from the ADMINISTRATORS section of the **Tools** menu. The Administrator List screen opens, as shown in Figure 12-1.

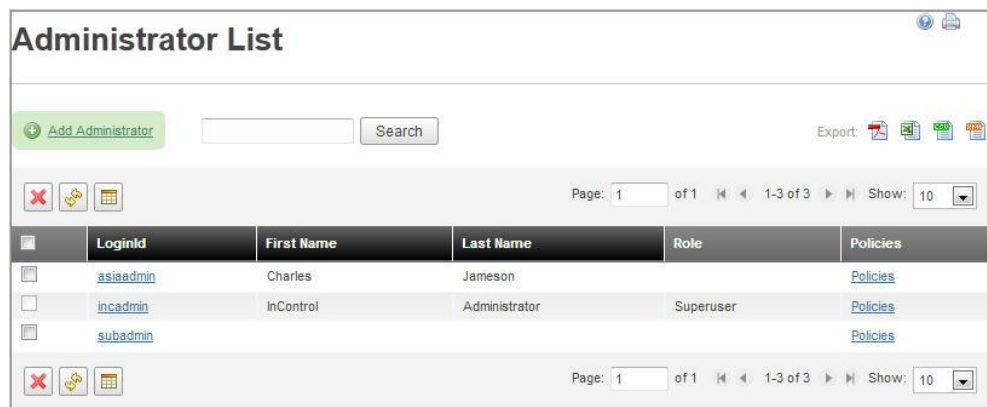




Figure 12-1 Administrator List

Choose from the following actions:

- To search for a particular administrator, type a search string in the text block and click **Search**.
- To delete one or more administrators, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected administrators, or **Cancel** to return to the Administrator List screen.
- To refresh the display, click .
- To add an administrator, refer to the next section.

Adding an Administrator

To add an administrator, click the **Add Administrator** link. The Add Administrator screen appears, as shown in Figure 12-2. Login ID, Password, and Role are mandatory fields; all other fields are optional.

Figure 12-2 Add Administrator

Table 12-1 Add Administrator Parameters

Field	Description
Login ID	New administrator's login ID (for example, jsmith). This is a mandatory field.
Password	New administrator's password. This is a mandatory field.
Verify Password	Re-enter the new administrator's password for verification purposes.
First Name	First (given) name of new administrator.
Last Name	Last (family) name of new administrator.
Address	Mailing address of new administrator.
Email	Email address of new administrator (for example, juser@example.com).
Phone	Phone number of new administrator.
Pager	Pager number of new administrator.
Fax	Fax number of new administrator.

Field	Description
Authorize Externally	<i>Disabled when Administrator Type is set to MASTER.</i> When this administrator logs in, use the external authorization callout for authentication purposes. This feature allows you to use corporate wide authentication such as LDAP, RADIUS, or TACACS.
Administrator Type	Choose from MASTER, NORMAL, or READONLY. MASTER users have full control over the entire IPControl system. NORMAL users have ordinary read-write permissions, and may be restricted to working with only certain portions of the IPControl system. READONLY users have read-only access to IPControl, and may be restricted to seeing only certain portions of the IPControl system.
Role	Select the Administrator Role from the roles that you have defined.
Assignable Role	Select the Administrator Assignable Role from the roles that you have defined. Assignable Roles are roles for which the Administrator can assign to another Administrator. Only Administrators with Superuser privileges may administer Assignable Roles.

Fill in the appropriate fields. Once finished, click **OK** to save your changes, or **Cancel** to return to the Administrator List screen. The new administrator appears in the administrator list.

Assignable Roles

The basic premise is that a Superuser creates all the roles in the system and grants authority to another administrator to assign all or a subset of these roles to other administrators. An administrator can have zero to many roles *assignable* to another administrator. Administrators without Superuser privileges cannot assign a role to themselves.

Administrator-specific Policies

Policies for an administrator are set using the **Policies** link in the Administrator List screen. The Administrator Policies screen opens.

The Administrator Policies screen works exactly as described in “Administrator Role Policies” on page 335. The only difference is that the policies set are assigned only to the Administrator being modified.

Note: It is important to note that the Administrator-specific policies are combined with the policies defined for all of the Administrator Roles to which the Administrator is assigned.

Determining Effective Rights for an Administrator

When an Administrator is assigned to multiple roles or is assigned to a single role but has Administrator-specific policies defined it may not be apparent as to what the effective rights or policies are applied to the given Administrator. This section will attempt to explain how these “effective” rights are computed.

When reading the descriptions, keep in mind that the Administrator-specific Policies are treated the same as the policies defined for a defined Administrator Role.

The general rule of thumb is that if the access right is “on” for any of the roles assigned to an Administrator, then the policy is considered “on” for the Administrator. For the **Policies** tab, the general rule of thumb is that the most restrictive policy will apply.

Authorized Functions

For the Authorized Functions, the rule is that if the Function is authorized for any role assigned to the Administrator, then the Function is authorized for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized for “Container Maintenance”, while Role B is not authorized for this. The effective right is that the Administrator is authorized for “Container Maintenance”.

Access Control List

For the Access Control Lists, the rule is that if the action on a specific Container (or Block) is authorized for any role assigned to the Administrator, then that action on that Container (or Block) is authorized for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized to Read and Write to Container “Region A”, while Role B is authorized for only Read access to “Region A”. The effective right is that the Administrator is authorized to Read and Write for the “Region A” container.

Block Type Access

For the Block Type Access, the rule is that if access is granted for a Block Type for any role assigned to the Administrator, then that access is granted to that Block Type for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized for Block Types “Any” and “Loopback”, while Role B is authorized only for Block Type “Point to Point”. The effective right is that the Administrator is authorized for “Any”, “Loopback”, and “Point to Point”.

Device Type Access

For the Device Type Access, the rule is that if access is granted for a Device Type for any role assigned to the Administrator, then that access is granted to that Device Type for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized for Device Types “PC” and “Printer”, while Role B is authorized only for Device Type “Router”. The effective right is that the Administrator is authorized for “PC”, “Printer”, and “Router”.

Policies

For the Policies, the rule is that the most restrictive policy defined for any role assigned to the Administrator will be honored.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized for “Allow Command Line Interface Access” and the “Allow Duplicate Hostnames Checking” policy is set to “Fail”, while Role B is not authorized for “Command Line Interface Access” and the “Allow Duplicate Hostnames Checking” is set to “Warn”. The effective policies are that the Administrator is **not** authorized for Command Line Interface Access and the Duplicate Hostnames Checking policy will be to “Fail”.

Domain Access Control

For the Domain Access Control Lists, the rule is that if the action on a specific Domain is authorized for any role assigned to the Administrator, then that action on that Domain is authorized for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized to Read and Write to Domain “ins.com”, while Role B is authorized for only Read access to Domain “ins.com”. The effective right is that the Administrator is authorized to Read and Write for the “ins.com” container.

Net Service Access Control

For the Net Service Access, the rule is that if access is granted for a Net Service for any role assigned to the Administrator, then that access is granted to that Net Service for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized to Read and Write to Net Service “DNS1”, while Role B is authorized for only Read access to Net Service “DNS1”. The effective right is that the Administrator is authorized to Read and Write for the Net Service “DNS1”.

Resource Record Type Access

For the Resource Record Type Access, the rule is that if access is granted for a Resource Record Type for any role assigned to the Administrator, then that access is granted to that Resource Record Type for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized for Resource Record Types “A”, “PTR” and “MX”, while Role B is authorized for only for Resource Record Type “A”. The effective right is that the Administrator is authorized for “A”, “PTR” and “MX”.

Address Type Access

For the Address Type Access, the rule is that if access is granted for an Address Type for any role assigned to the Administrator, then that access is granted to that Address Type for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized for Address Types “Static” and “Reserved”, while Role B is authorized for only for

Address Type “Static”. The effective right is that the Administrator is authorized for “Static” and “Reserved”.

Administrator Roles

Use the Administrator Roles screen to maintain Administrator Roles. Administrator Roles allow policies to be created for specific purposes. Once these policies are created, you may assign individual administrators to a role or multiple roles. Use Administrator Roles to define the following:

- Which management containers and/or blocks within the system can be accessed
- Which menu items are displayed to a user
- Which block types an administrator can manage
- Which device types an administrator can manage
- Which domains an administrator can manage
- What policies are applied to this user

You define administrator roles, and associate one or more users to a specific administrator role. This allows you to change an attribute of the administrator role and have it apply to all administrators that are assigned to that the role. This provides you an effective way to manage large groups of administrators, and allows you to manage groups of administrators in a consistent manner.

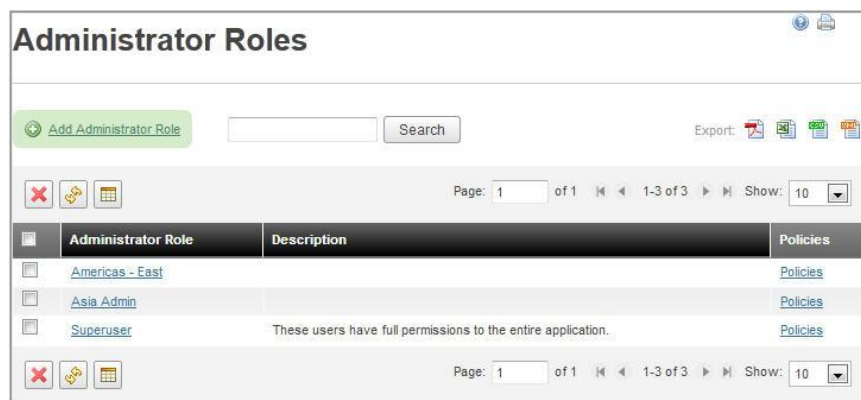


Figure 12-3 Administrator Roles

To delete one or more administrator roles, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation.

Note: Make sure that there are no administrators assigned to a role before you delete it.

Click **OK** to delete the selected administrator roles, or **Cancel** to return to the previous screen.

Adding an Administrator Role

To add an administrator role, click the **Add Administrator Role** link. The Add Administrator role screen appears, as shown in Figure 12-4.

Figure 12-4 Add Administrator Role

Table 12-2 Administrator Role Parameters

Field	Description
Role Name	The Role Name that you want to assign to this role (for example, 'Region A Admin Roles'). This is a mandatory field.
Description	A description of this role. This is an optional field.

Fill in the appropriate fields. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Administrator Role Policies

Policies for an administrator role are set using the **Policies** link in the Administrator Role List screen. Clicking the **Policies** link opens the Administrator Policies screen on the **Authorized Functions** tab, as shown in Figure 12-5.

Administrator Policies

Role Name: Americas - East

Description:

Authorized Functions
Access Control List
Block Type Access
Device Type Access
Policies
Domain Access Control

Net Service Access Control
Resource Record Type Access Control
Address Type Access

☐ Check/Uncheck All Authorized Functions

File	Network Services Policies & Options	Management	
Change Password	<input checked="" type="checkbox"/> DNS & DHCP Products	<input checked="" type="checkbox"/> Management Containers	<input checked="" type="checkbox"/>
	Transaction Keys	<input checked="" type="checkbox"/> Add Sites	<input checked="" type="checkbox"/>
System Setup	Server Pairs	<input checked="" type="checkbox"/> Address Blocks	<input checked="" type="checkbox"/>
System Policies/Options	<input checked="" type="checkbox"/> Address Match Lists	<input checked="" type="checkbox"/> Subnet Policy	<input checked="" type="checkbox"/>
Agents	<input checked="" type="checkbox"/> DHCP Option Master Dictionary	<input checked="" type="checkbox"/> Vlan Policy	<input checked="" type="checkbox"/>
Appliances	<input checked="" type="checkbox"/> DHCP Option Vendor Dictionary	<input checked="" type="checkbox"/> IP Address: Domain Search	<input checked="" type="checkbox"/>
Vendor/Models	<input checked="" type="checkbox"/> DHCP Option Sets	<input checked="" type="checkbox"/> IP Address: Resource Records Tab	<input checked="" type="checkbox"/>
Allocation Reason Codes	<input checked="" type="checkbox"/> DHCP Policy Sets	<input checked="" type="checkbox"/> General Tab	<input checked="" type="checkbox"/>
Device Types	<input checked="" type="checkbox"/> DHCP Client Classes	<input checked="" type="checkbox"/> Add Block	<input checked="" type="checkbox"/>
Device Interface Templates	<input checked="" type="checkbox"/> DNS Option Master Dictionary	<input checked="" type="checkbox"/> Delete Block	<input checked="" type="checkbox"/>
Administrator Roles	<input checked="" type="checkbox"/> DNS Option Vendor Dictionary	<input checked="" type="checkbox"/> Split Block	<input checked="" type="checkbox"/>
Administrators	<input checked="" type="checkbox"/> DNS Log Channels	<input checked="" type="checkbox"/> Join Block	<input checked="" type="checkbox"/>
Threshold Sets	<input checked="" type="checkbox"/> DNS Server Templates	<input checked="" type="checkbox"/> Move Block	<input checked="" type="checkbox"/>
Threshold Alerts	<input checked="" type="checkbox"/> DNS Domain Types	<input checked="" type="checkbox"/> Attach Blocks	<input checked="" type="checkbox"/>
User Defined Fields	<input checked="" type="checkbox"/>	Detach Blocks	<input checked="" type="checkbox"/>
Information Template	<input checked="" type="checkbox"/> Reports	Network Services	<input checked="" type="checkbox"/>
Block Types	<input checked="" type="checkbox"/> RIR Summary Report	<input checked="" type="checkbox"/> Configuration/Deployment	<input checked="" type="checkbox"/>
Address Pool Allocation Templates	<input checked="" type="checkbox"/> Low Pool Report	<input checked="" type="checkbox"/> DNS - All Files	<input checked="" type="checkbox"/>
Device Naming Policies	<input checked="" type="checkbox"/> SWIP/Net Name Report	<input checked="" type="checkbox"/> DNS - Changed Zones	<input checked="" type="checkbox"/>
RIR Organization IDs	<input checked="" type="checkbox"/> Container Audit Report	<input checked="" type="checkbox"/> DNS - Selected Zones	<input checked="" type="checkbox"/>
Software Updates	<input checked="" type="checkbox"/> Block Audit Report	<input checked="" type="checkbox"/> DNS - Config Only	<input checked="" type="checkbox"/>
Software Packages	<input checked="" type="checkbox"/> Block Utilization Report	<input checked="" type="checkbox"/> DNS - Changed RRs via DDNS	<input checked="" type="checkbox"/>
Site Allocation Templates	<input checked="" type="checkbox"/> Container Utilization Report	<input checked="" type="checkbox"/> DNS - All RRs via DDNS	<input checked="" type="checkbox"/>
Import Wizard	<input checked="" type="checkbox"/> Device Audit Report	<input checked="" type="checkbox"/> DNS - All User-created RRs via DDNS	<input checked="" type="checkbox"/>
	Resource Record Audit Report	<input checked="" type="checkbox"/> DHCP - All Files	<input checked="" type="checkbox"/>
Topology	Logged-In Administrators	<input checked="" type="checkbox"/> Pending Approvals	<input checked="" type="checkbox"/>
Container Maintenance	<input checked="" type="checkbox"/> Login Audit Report	<input checked="" type="checkbox"/> Discovery/Collectors	<input checked="" type="checkbox"/>
Network Elements/Devices	<input checked="" type="checkbox"/> Administrator Audit Report	<input checked="" type="checkbox"/> Search	<input checked="" type="checkbox"/>
Network Services	<input checked="" type="checkbox"/>	Reclaim	<input checked="" type="checkbox"/>
DNS Galaxies	<input checked="" type="checkbox"/>	Tasks	<input checked="" type="checkbox"/>
DNS Domains	<input checked="" type="checkbox"/>	Alerts	<input checked="" type="checkbox"/>
		Dashboard	<input checked="" type="checkbox"/>
		Manage	<input checked="" type="checkbox"/>

Figure 12-5 Administrator Policies

Authorized Functions Tab

Each function corresponds to a menu item. To allow an administrator to use that menu function, place a check in the box next to the description. To disallow a function, uncheck the checkbox.

Access Control Lists

Select the **Access Control List** tab to what containers and blocks are accessible to NORMAL or READONLY administrator types; by definition, MASTER administrators cannot be restricted.

Note: Administrator types are defined in “Adding an Administrator” on page 330.

Access controls allow you to define which management containers a specific administrator or a group of administrators may access.

Administrator Policies

Role Name: Americas - East
Description:

Authorized Functions | **Access Control List** | Block Type Access | Device Type Access | Policies | Domain Access Control
Net Service Access Control | Resource Record Type Access Control | Address Type Access

Container Name:	Read	Write	Delete	Apply to Children	
Exton	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete Add Block
Pittsburgh	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete Add Block

Add Container(s)

Block Name:	Container Name	Read	Write	Delete
Submit Cancel				

Figure 12-6 Access Control List Tab

Any existing Access Control Lists (ACLs) are shown. To add containers to the ACL for the currently selected administrator role, click **Add Container(s)**. The Container Search popup window shown in Figure 12-7 opens.

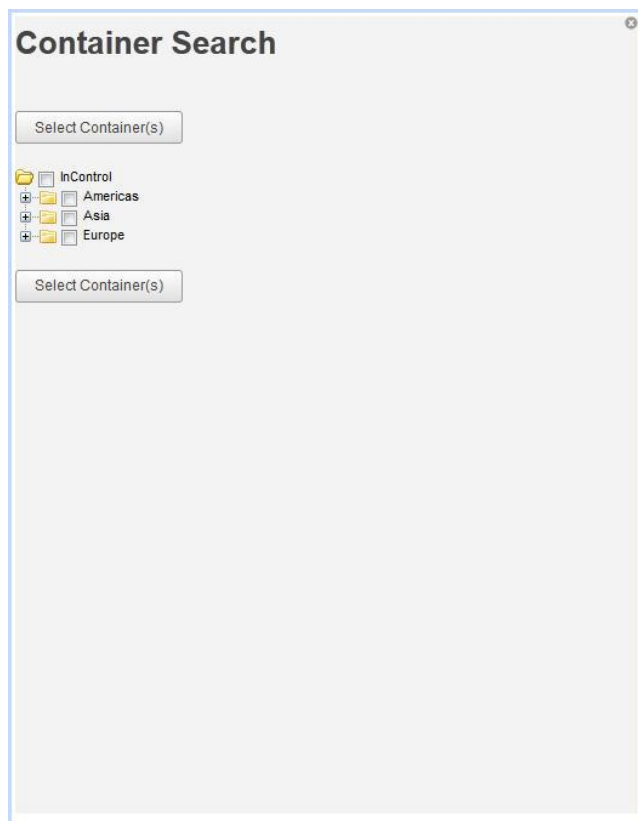


Figure 12-7 Container Search

Place checkmarks next to the containers this administrator role can access. Once finished, click the **Select Container(s)** button to return to the Administrator Roles Policies screen, where the containers you selected are added to the Access Control List for the administrator role.

You can now specify the privileges that apply to the added container for the role, as described in Table 12-3.

Table 12-3 Access Control List Parameters

Field	Description
Read	Administrator can view attributes of this container and all blocks assigned to this container.
Write	Administrator can write to this container and all blocks (and IP Addresses) assigned to this container. This includes deleting blocks and IP Addresses.
Delete	Administrator can delete this container.
Apply to Children	Determines whether the Read, Write, and Delete privileges also apply to the children of this container.

Adding Blocks to an Administrator Role ACL

In addition, you can add access control policies for individual blocks assigned to a container for which there is an access control policy specifically defined for this Role. To do this, click on the

Add Block button next to the container where the block resides. The Subnet/Block Search Results popup window opens with a list of the blocks in the container, as shown in Figure 12-8.

Search Result: Subnets/Blocks

Search

Page: 1 of 11 1-10 of 104 Show: 10

Name	Size	Type	Root	Status	Container	Parent Block	Created	Created By	User Defined Fields
4FFE:DAF0::/40	/40	IPv6 Lab	No	Aggregate	Americas	4FFE:DAF0::/32	2007-05-03 19:39:46.0	incadmin	
10.168.0.0/13	/13	VOIP	No	Aggregate	Americas	10.0.0.0/8	2007-05-04 13:51:44.0	incadmin	
10.172.0.0/14	/14	VOIP	No	Free	Americas	10.168.0.0/13	2007-05-04 13:51:43.0		
10.170.0.0/15	/15	VOIP	No	Free	Americas	10.168.0.0/13	2007-05-04 13:51:43.0		
10.169.0.0/16	/16	VOIP	No	Free	Americas	10.168.0.0/13	2007-05-04 13:51:43.0		
10.168.64.0/18	/18	VOIP	No	Free	Americas	10.168.0.0/13	2007-05-04 13:51:43.0		
10.168.32.0/19	/19	VOIP	No	Free	Americas	10.168.0.0/13	2007-05-04 13:51:43.0		
10.168.192.0/18	/18	VOIP	No	Free	Americas	10.168.0.0/13	2007-05-04 13:51:43.0		
10.168.128.0/19	/19	VOIP	No	Free	Americas	10.168.0.0/13	2007-05-04 13:51:43.0		
10.168.176.0/20	/20	VOIP	No	Free	Americas	10.168.0.0/13	2007-05-04 13:51:43.0		

Page: 1 of 11 1-10 of 104 Show: 10

Figure 12-8 Subnet/Block Search Results

Click on the name of the block you want to add to the Access Control List for the selected administrator role. The block is added to the Block Name list, where you can specify the privileges to apply to this block for the selected role, as described in Table 12-4.

Table 12-4 Block Name Parameters

Field	Description
Read	Administrator can view attributes of this block including IP Addresses.
Write	Administrator can change attributes of block. Also permitted to add, modify, and/or delete IP Addresses assigned to this block.
Delete	Administrator can delete this block.

You typically add blocks to an administrator role ACL when you want to override the privileges defined on the container for a specific block. For instance, if you want to “hide” a specific block from an administrator role while allowing access to all other blocks in the container, then give the administrator role full rights to the container, but then add the specific block and remove all rights. Thus when the administrator assigned to this role views the container, the specific block does not even appear in the list of container blocks.

Block Type Access Tab

The **Block Type Access** tab allows you to limit the **Block Types** that this administrator can manage. It limits the block types available on Add Child Block, Add Root Block and Attach Block operations. The net effect is that by limiting block types for an administrator, they can see blocks of any type, but can only create blocks of types for which they have permission.

The screenshot shows the 'Administrator Policies' web interface. At the top, there's a header 'Administrator Policies'. Below it, a form shows 'Role Name: Americas - East' and 'Description:'. A navigation bar contains tabs: 'Authorized Functions', 'Access Control List', 'Block Type Access' (selected), 'Device Type Access', 'Policies', 'Domain Access Control', 'Net Service Access Control', 'Resource Record Type Access Control', and 'Address Type Access'. The main content area has three radio buttons: 'Allow Full Access to All Block Types for this Administrator' (selected), 'Limit Access By Selected Block Type(s) for this Administrator', and 'Check/Uncheck All Block Types'. Below these is a table with columns for block types and checkboxes. The table has three rows: 'Any', 'IPv6 Lab', and 'Video'. Each row has a checkbox, a 'Block Sizes' link, and a 'Data', 'Management', or 'VOIP' label. At the bottom are 'Submit' and 'Cancel' buttons.

Block Type	Check	Block Sizes	Label	Check	Block Sizes
Any	<input type="checkbox"/>	Block Sizes	Data	<input type="checkbox"/>	Block Sizes
IPv6 Lab	<input type="checkbox"/>	Block Sizes	Management	<input type="checkbox"/>	Block Sizes
Video	<input type="checkbox"/>	Block Sizes	VOIP	<input type="checkbox"/>	Block Sizes

Figure 12-9 Block Type Access

To enable Block Type Access Controls for an administrator role, click the **Allow Full Access to All Block Types for this Administrator** option button. If you wish to specify certain block types for access restriction, choose the **Limit Access By Selected Block Type(s)** option button and check the box next to each Block Type for which create permission is desired. To check or uncheck all block types shown, select **Check/Uncheck All Block Types** check box.

Block Type Size Constraints

To further constrain the block type to discrete sizes of an address block, select the **Block Sizes** link next to the selected block type. The Edit Block Sizes dialog box opens for the given block type. Block size constraints are only effective if the **Limit Access By Selected Block Type(s)** button is selected and the block type is checked. All constraints defined here are applied to both child and root block allocation.



Figure 12-10 Edit Block Sizes

Select all block sizes allowable for allocation by the administrator role for the block type. Any unchecked block sizes are not allowed for allocation. Use the **IPv4** tab to edit settings for IPv4 block size addressing. Use the **IPv6** tab to edit settings for IPv6 block size addressing.

Select **Abstain and leave block sizes “undefined”** if you want this administrator role to abstain from deciding if a block type can be allocated for a particular block size and addressing (IPv4 or IPv6). All selected block sizes are then ignored, and the role defers to another administrator role to determine if a block type can be allocated for a block size.

Block Type Size Allocation Rules

Whether or not an administrator is allowed block allocation of a certain size for a block type will be determined by first examining the block size constraints defined at the block type definition. If there are no constraints defined for the definition, then the administrator block type policy rules are examined. If a user owns multiple administrator roles, the block type size constraints defined for the **least** restrictive role are used.

Block Type Definition Rules

The block type will be allowed block allocation for the block size if there are no constraints defined for the block size. Note if the block size is defined as not allowable by the block type definition, then the user will not be allowed allocation **regardless** of the constraints defined at any administrator role level.

Administrator Block Type Policy Rules

The block type will be allowable for allocation for the block size if any of the following conditions apply:

- The block type is **not** selected as “Limit Access By Selected Block Type(s)”.
- The block type **is** selected as “Limit Access By Selected Block Type(s)” **and** the block size is defined as allowable for the block type.

Note: If “Limit Access By Selected Block Type(s)” is selected **and** “Abstain and leave block sizes ‘undefined’” is flagged, the administrator role will defer to another role owned by the administrator. If in a case where there are no other roles defined, the block type definition rules will be used.

Device Type Access Tab

The **Device Type Access** tab allows you to limit the Device Types that this administrator can manage. It limits the device types available on the Add IP Address, or the Add IP Address Range screens. The net effect is that by limiting device types for an administrator, they can view devices of any type, but can only create, edit, or delete devices of types for which they have permissions.

Administrator Policies

Role Name: Americas - East

Description:

Authorized Functions | Access Control List | Block Type Access | **Device Type Access** | Policies | Domain Access Control

Net Service Access Control | Resource Record Type Access Control | Address Type Access

☒ Allow Full Access to All Device Types for this Administrator
☐ Limit Access By Selected Device Type(s) for this Administrator
☐ Check/Uncheck All Device Types

Access Point	<input type="checkbox"/>	CMTS	<input type="checkbox"/>	Desktop	<input type="checkbox"/>
DSRouter	<input type="checkbox"/>	File Server	<input type="checkbox"/>	Firewall	<input type="checkbox"/>
IP Phone	<input type="checkbox"/>	PC	<input type="checkbox"/>	Printer	<input type="checkbox"/>
Router	<input type="checkbox"/>	Server	<input type="checkbox"/>	Switch	<input type="checkbox"/>
Unknown	<input type="checkbox"/>	Unspecified	<input type="checkbox"/>	VPN	<input type="checkbox"/>

Submit Cancel

Figure 12-11 Device Type Access

To enable Device Type Access Controls for an administrator role, click the **Allow Full Access to All Device Types for this Administrator** option button. If you wish to specify certain device types

for access restriction, choose the **Limit Access By Selected Device Type(s) for this Administrator** option button and check the box next to each Device Type for which create permission is desired. To check or uncheck all device types shown, select the **Check/Uncheck All Device Types** check box.

Policies Tab

The **Policies** tab allows you to assign miscellaneous administrator policies to the current administrator role.

Figure 12-12 Administrator Policies

Table 12-5 Administrator Policies Parameters

Field	Description
Allow Command Line Interface Access for this Administrator	When checked, this administrator is permitted to use Command Line Interfaces to IPControl. Otherwise, this administrator is denied access to the Command Line Interfaces.
Allow Duplicate Hostnames Checking	Ignore – Ignores duplicate hostname checking for this administrator. Warn – When a duplicate hostname is encountered, provides a warning to this administrator. Fail - Does not allow this administrator to add duplicate hostnames.
Duplicate Hostname Checking Style	Fully Qualified Domain Name – Allows administrator to check for duplicate hostnames using the fully qualified domain name. Hostname Only – Allows administrator to check for duplicate hostnames using the hostname only.
Allow Duplicate A Record (Owner) Checking	Ignore – Ignores duplicate A record checking for this administrator. Warn – When a duplicate A record is encountered, provides a warning to this administrator.

Field	Description
	Fail - Does not allow this administrator to add duplicate A record.
Allow Duplicate Hardware Address (MAC) Checking	Ignore – Ignores duplicate MAC Address checking for this administrator. Warn – When a duplicate MAC Addresses are encountered, provides a warning to this administrator. Fail - Does not allow this administrator to add duplicate MAC Addresses.

Domain Access Control Tab

Domain Access controls allow you to define which domains a specific administrator or a group of administrators may access.

The screenshot shows the 'Administrator Policies' window with the 'Domain Access Control' tab selected. The window displays the role 'Americas - East' and a table of domain access controls. The table has columns for Domain, Read, Write, Delete, Resource Record Access, Resource Record Write Access, and Apply to Children. Three domains are listed: . (Americas), . (Default), and . (External), each with checkboxes for Read, Write, Delete, Resource Record Access, and Resource Record Write Access, and a 'Delete' button. At the bottom are 'Submit', 'Add Domain(s)', and 'Cancel' buttons.

Domain:	Read	Write	Delete	Resource Record Access	Resource Record Write Access	Apply to Children	
. (Americas)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
. (Default)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
. (External)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete

Buttons: Submit, Add Domain(s), Cancel

Figure 12-13 Domain Access Control

Any existing Domain Access Control Lists (ACLs) are shown. To add domains to this user's ACL, click **Add Domain(s)**. This brings up a window prompting you to select the domain this administrator role can access.

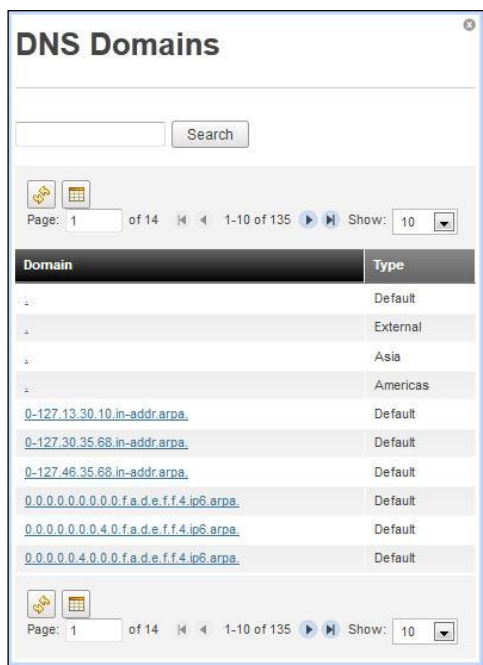


Figure 12-14 Domain Search

Select the domain link that this administrator role can access. The domain is added to Domain Access Control list, where you can specify the privileges that apply to this administrator role, as described in Table 12-6.

Table 12-6 Domain Access Control Parameters

Field	Description
Read	Administrator can view attributes of this domain excluding resource records. This also includes viewing attributes of zones for this domain.
Write	Administrator can make modifications to this domain. This effectively means that the administrator can: <ul style="list-style-type: none"> • Change SOA values (where appropriate) for this domain. • Create child domains • Create zones for this domain.
Delete	Administrator can delete this domain.
Resource Record Access	Administrator can read resource records within this domain.
Resource Record Write Access	Administrator can modify resource records within this domain.
Resource Record Approve Access	Administrator can approve/reject resource records added by others for this domain. Also if this option is checked, resource records added by the administrator in this domain do not require approval.
Apply to Children	Determines whether these privileges also apply to the children of the domain in the Domain field.

Net Service Access Control Tab

The **Net Service Access Control** tab controls allow you to define which Net Services a specific administrator or a group of administrators may access.

To **enable** Net Service Access Controls for an administrator, click on the button labeled “Enable Net Service Access Controls for this Administrator”. When this selection is enabled, only those Net Services listed will be accessible to the administrator. If the selection is **disabled**, all Net Services in the system will be accessible with full permissions (Read, Write, Deploy), as shown in Figure 12-15.

Administrator Policies

Role Name: Americas - East

Description:

Authorized Functions | Access Control List | Block Type Access | Device Type Access | Policies | Domain Access Control

Net Service Access Control | Resource Record Type Access Control | Address Type Access

☐ Enable Net Service Access Controls for this Administrator
☒ Disable Net Service Access Controls for this Administrator

Submit Add Net Service(s) Cancel

Figure 12-15 Net Service Access Control

Any existing Net Service Access Control Lists (ACLs) are shown. To add Net Services to this user’s ACL, click **Add Net Service(s)**. This brings up the Network Service Search screen where you to select the Net Services this administrator role can access.

Servers/Services

Search

Page: 1 of 1 1-10 of 10 Show: 10

Service Name	IP Address	Type
dhcp1.sw.diamondip.com	10.252.200.19	DHCP
ns-cn.diamondip.com	10.199.201.5	DNS
ns1-ip.diamondip.com	172.16.0.254	DNS
sapphire1.diamondip.com	10.30.8.200	DNS
sapphire1.diamondip.com	10.30.8.200	DHCP
sapphire2.diamondip.com	10.30.4.199	DNS
sapphire2.diamondip.com	10.30.4.199	DHCP
sapphire3.diamondip.com	10.92.172.36	DNS
sapphire3.diamondip.com	10.92.172.36	DHCP
sapphire4.diamondip.com	192.168.196.20	DNS

Page: 1 of 1 1-10 of 10 Show: 10

Figure 12-16 Network Service Search

Select the Net Service link you want this administrator role to access. The Administrator Net Service Access Control screen opens with the selected Net Service added to the Net Service table, where you can specify the permissions that apply to this administrator for the specified Net Service.

Table 12-7 Net Service Access Control Parameters

Field	Description
Read	Administrator can view attributes of this Net Service.
Write	Administrator can make modifications to this Net Service.
Deploy	Administrator can deploy to this Net Service.

Resource Record Type Access Control Tab

The **Resource Record Type Access Control** tab allows you to limit the Resource Record Types that this administrator can manage. It limits the Resource Record types available on the Add Resource Record screens. The net effect is that by limiting resource record types for an administrator, they can only create, edit, or delete resource records of types for which they have permissions.

Administrator Policies

Role Name: Americas - East

Description:

Authorized Functions | Access Control List | Block Type Access | Device Type Access | Policies | Domain Access Control

Net Service Access Control | **Resource Record Type Access Control** | Address Type Access

☒ Allow Full Access to All Resource Record Types for this Administrator

☐ Limit Access By Selected Resource Record Type(s) for this Administrator

☐ Check/Uncheck All Resource Record Types

A	<input checked="" type="checkbox"/>	A6	<input checked="" type="checkbox"/>	AAAA	<input checked="" type="checkbox"/>
AFSDB	<input checked="" type="checkbox"/>	CNAME	<input checked="" type="checkbox"/>	DNAME	<input checked="" type="checkbox"/>
DS	<input checked="" type="checkbox"/>	GPOS	<input checked="" type="checkbox"/>	HINFO	<input checked="" type="checkbox"/>
ISDN	<input checked="" type="checkbox"/>	KEY	<input checked="" type="checkbox"/>	KX	<input checked="" type="checkbox"/>
LOC	<input checked="" type="checkbox"/>	MB	<input checked="" type="checkbox"/>	MG	<input checked="" type="checkbox"/>
MINFO	<input checked="" type="checkbox"/>	MR	<input checked="" type="checkbox"/>	MX	<input checked="" type="checkbox"/>
NAPTR	<input checked="" type="checkbox"/>	NULL	<input checked="" type="checkbox"/>	NS	<input checked="" type="checkbox"/>
NSAP	<input checked="" type="checkbox"/>	NSAP-PTR	<input checked="" type="checkbox"/>	PTR	<input checked="" type="checkbox"/>
NXT	<input checked="" type="checkbox"/>	PX	<input checked="" type="checkbox"/>	RP	<input checked="" type="checkbox"/>
RT	<input checked="" type="checkbox"/>	SA	<input checked="" type="checkbox"/>	SIG	<input checked="" type="checkbox"/>
SOA	<input checked="" type="checkbox"/>	SRV	<input checked="" type="checkbox"/>	TKEY	<input checked="" type="checkbox"/>
TSIG	<input checked="" type="checkbox"/>	TXT	<input checked="" type="checkbox"/>	WKS	<input checked="" type="checkbox"/>
X25	<input checked="" type="checkbox"/>	ZONE RR	<input checked="" type="checkbox"/>	OTHER	<input checked="" type="checkbox"/>

Submit Cancel

Figure 12-17 Research Record Type Access Control

To enable Resource Record Type Access Controls for an administrator role, click the **Allow Full Access to All Resource Record Types for this Administrator** option button. If you wish to

specify certain resource record types for access restriction, choose the **Limit Access By Selected Resource Record Type(s) for this Administrator** option button and check the box next to each Resource Record Type for which create permission is desired. To check or uncheck all resource record types shown, select the **Check/Uncheck All Resource Record Types** check box.

Address Type Access Tab

The **Address Type Access** tab allows you to limit the Address Types that this administrator role can manage. It limits the Address types available on the Add IP Address, Add IP Range and Add IP Address pool screens. The net effect is that by limiting address types for an administrator, they can only create, edit, or delete IP Address of Address types for which they have permissions.

Administrator Policies

Role Name: Americas - East

Description:

Authorized Functions | Access Control List | Block Type Access | Device Type Access | Policies | Domain Access Control

Net Service Access Control | Resource Record Type Access Control | **Address Type Access**

☒ Allow Full Access to All Address Types for this Administrator

☐ Limit Access By Selected Address Type(s) for this Administrator

☐ Check/Uncheck All Address Types

Static	<input checked="" type="checkbox"/>
Dynamic DHCP	<input checked="" type="checkbox"/>
Automatic DHCP	<input checked="" type="checkbox"/>
Manual DHCP	<input checked="" type="checkbox"/>
Reserved	<input checked="" type="checkbox"/>

Submit Cancel

Figure 12-18 Address Type Access

To enable Address Type Access Controls for an administrator role, click the **Allow Full Access to All Address Types for this Administrator** option button. If you wish to limit access by selected address type, choose the **Limit Access By Selected Address Type(s) for this Administrator** option button and check the box next to each Address Type where access is desired. To check or uncheck all address types shown, select the **Check/Uncheck All Address Types** check box.

Once finished, click **Submit** to save all changes on the Administrator Policies screen, or **Cancel** to discard all changes and return to the Administrator Roles screen. If the Administrator Policy was successfully updated, the Administrator List screen displays `Policy for <admin-role> saved`.

Chapter 13 Performing Advanced Administration Activities

This chapter provides administrators with “how to” information on common operational functions that need to be accomplished within the product.

Configuring INS DNS for Selected or Changed Zone Push

IPControl has the ability to perform selective DNS zone configurations using the Configuration/Deployment menu option.

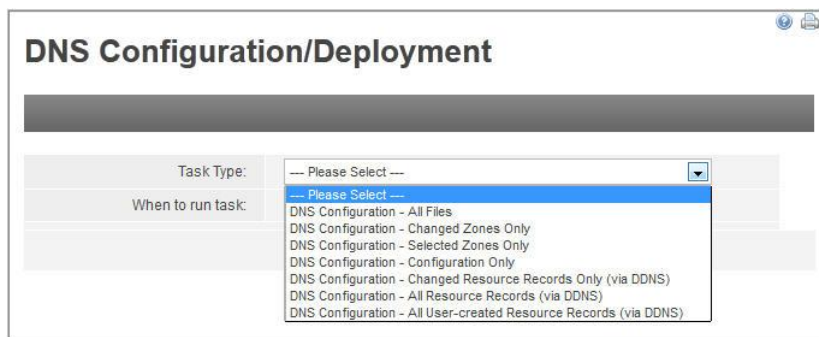


Figure 13-1 Configuration/Deployment

Specific Configuration/Deployment options include the following:

- **DNS Configuration - Changed Zones Only** - when an administrator makes a change to a resource record in a domain, all zones associated with that domain are marked as “dirty”. The IPControl administrator can then schedule a “Changed Zones Only” deployment push, and only zones that have changed since the last file generation are created and sent to the DNS server.
- **DNS Configuration - Selected Zones Only** - an administrator may want to immediately push changes to a specific zone to a specified DNS server, without necessarily pushing every changed zone.

To support either of these configuration/deployment options, some additional configuration is required on the DNS server. This is because these tasks make use of the “rndc” utility to only load the selected zones, instead of forcing the DNS service to completely stop and start. This provides seamless loading of new data without affecting name resolution for your users.

To configure the INS DNS server for this support, perform the following steps:

1. Choose from the following actions.

Server Type	Steps
Windows	<ol style="list-style-type: none"> 1. Run the following command: <code>C:\Program Files\Diamond IP\InControl\dns\bin\rndc-confgen -a -k rndc-key.</code> 2. Open the file <code>C:\Program Files\Diamond IP\InControl\dns\etc\rndc.key</code> in a text editor (such as Notepad).
UNIX	<ol style="list-style-type: none"> 1. As the 'root' user, run the command: <code>/opt/incontrol/dns/sbin/rndc-confgen -a -k rndc.key.</code> <p>Note: On Solaris, you may be required to input some key strokes manually; this is normal and helps generate randomness.</p> 2. Open or cat the file <code>/etc/rndc.key</code>.

2. Copy the secret part of the file, excluding quotes. For example:

f72ISy9MFntJ4In1sSRtOQ==

3. In IPControl, select **Transaction Keys** from the DNS section of the **Management** menu.
4. In the Transaction Keys screen, select **Add Transaction Key**. The Add Transaction Key screen opens.
5. In the **Key Name** field, type `rndc-key.` (note the trailing period).
6. Paste the key from step 3 into the **Secret** field. (To review the string, select the **Unmask Secret** checkbox.)
7. Repeat for the **Confirm Secret** field. Your screen should look similar to Figure 13-2.

Add Transaction Key

Key Name:	<input type="text" value="rndc-key."/>
Key Algorithm:	<input type="text" value="HMAC-MD5"/>
Secret:	<input type="text" value="f72ISy9MFntJ4In1sSRtOQ=="/>
Confirm Secret:	<input type="text" value="f72ISy9MFntJ4In1sSRtOQ=="/>
Unmask Secret:	<input checked="" type="checkbox"/>
Generate a Secret:	<input type="button" value="Generate"/> <input type="text" value="128 Bits"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Figure 13-2 Add Transaction Key

8. Click **Submit** to save the key.
9. Select **Servers/Services** from the DNS section of the **Management** menu.

10. Select the DNS Server to which you are performing a Changed or Selected Zone push.
11. Click on the **Advanced** tab. In the **Allow Messages From** list box, make sure **localhost** is selected. In the **Keys (Used by rndc)** section, select the `rndc-key` key you created above. Your screen should look similar to Figure 13-3.

The screenshot shows a web interface titled "Edit DNS Server: sapphire2.diamondip.com". Below the title are tabs: General, Logging, Extensions, Root Hints File, Zones, **Advanced**, Options, and Views. The "Advanced" tab is active, displaying a "Controls" section. On the left, there are two radio buttons: "TCP Port Control Channel Settings:" (selected) and "Unix Domain Socket Channel Settings:". The "TCP Port Control" section includes fields for "Listen on IP Address:", "Listen on Port:" (set to 953), "Allow Message From:" (set to localhost), and "Keys (Used by rndc):" (with a dropdown menu showing "rndc-key", "ipc-sapphire1.diamondip.com.", and "ns1-ns2.diamondip.com."). The "Unix Domain Socket" section includes fields for "Unix Domain Socket:", "Permissions (in Octal Format):", "Owner (in Numeric Format):", and "Group (in Numeric Format):". At the bottom are "Submit" and "Cancel" buttons.

Figure 13-3 Edit DNS Server

12. Click **Submit** to save the server.

Your server is now configured for Changed or Selected Zone pushes.

Configuring IPControl to use External Authentication

IPControl can use an external authentication mechanism when users log into the system. This allows you the ability to establish administrative roles within the system, and then use an external authentication data store for password credentials.

There are two approaches to using external authentication.

- The first is to define each administrator (USERID) within IPControl, assign an administrator role to that admin, and then only use the external authentication mechanism for password authentication purposes. This allows you the ability to control admin rights at a very granular level, while still leveraging a single sign on method.
- The second approach involves creating a small set of userids (administrators) within the IPControl system, and assigning unique roles to each. You can then use your external script to map the userid attempting to login to IPControl, to a specific user within IPControl. This

allows you to control your administrative roles at a higher level, and allows you to leverage your external authentication system to help control access.

You must create a script, or use/modify one of the sample scripts that have been provided with your installation. By default, the installation routine copies a number of PERL based scripts to the `$INCHOME/etc/support/sample-scripts` directory. Sample scripts that are included are:

- `extauth-ldap.pl` – LDAP Authentication
- `extauth-msad.pl` – Microsoft Active Directory Authentication
- `extauth-tacacs.pl` – Cisco TACACS authentication

Please refer to these scripts as examples and note the input and outputs to these scripts.

Input

When this script is executed, IPControl passes three variables to the script:

- The `USERID` entered on the IPControl login page
- The `PASSWORD` entered on the IPControl login page
- The Product name “IPControl”

Output

On a successful authentication:

- When your script executes, it should send to `STDOUT`, the line “SUCCESS”, and then the `USERID` that is used by IPControl to establish administrative roles (that is, the `USERID` to look up within IPControl). You can optionally change the `USERID` that is returned to IPControl: it does not necessarily have to be the `USERID` entered by the user on the IPControl login page.

On an unsuccessful authentication:

- Your script should send the line “FAILURE”, followed by a line of text that appears on the login page. You can use this second line to send a reason why the login failed. The message appears on the IPControl Login page.

Configuration Steps

To configure the system to use external authentication, perform the following steps:

1. Select **Policies and Options** from the **SYSTEM** section of the **Tools** menu. The System Policies/Options screen opens.
2. In the **External Authentication Script** field, type the authentication script name and click **Submit**.

Note 1: If you are using PERL, you must enter the path and name of the PERL interpreter, as well as the script name, for example: `c:\perl\bin\perl test.pl`

Note 2: To call an external authentication script that resides in a directory with a space in the directory name, you must enclose the full path and script name in quotes, for example:

```
c:\cygwin\bin\perl.exe "c:\Program Files\success.pl"
```

3. After you have saved the script name, click the **Test** button next to the **External Authentication Script** field to run a test.
4. The test dialog appears, as shown in Figure 13-4. If necessary, enter a different userid and password to exercise the script, and then click **Test**.

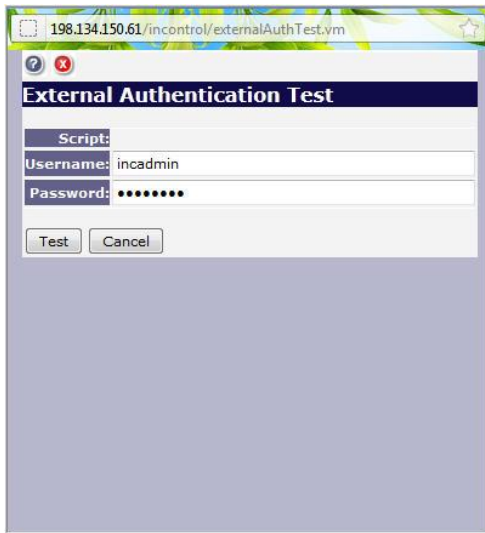


Figure 13-4 External Authentication Test

5. After the script executes, a success or failure message is provided back to the script.
6. After you are sure your script is operating correctly, set an administrator option for each administrator that you want to have use this external authentication method. Select **Administrators** from the ADMINISTRATORS section of the **Tools** menu and select the administrator entry you want to edit.
7. Select the **Authorize Externally** check box to turn on external authentication for this user and click **Submit**.

Edit Administrator	
Login ID:	subadmin
Password:	
Verify Password:	
First Name:	
Last Name:	
Address:	
Email:	
Phone:	
Pager:	
Fax:	
Authorize Externally:	<input checked="" type="checkbox"/>
Administrator Type:	NORMAL
Role:	Add Administrator Role
Assignable Role:	Add Administrator Assignable Role
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Figure 13-5 Edit Administrator: Authorize Externally

Interfacing with Microsoft Active Directory and Microsoft DNS

Many enterprise IT organizations find themselves faced with the challenge of managing a dichotomy of two Domain Name System (DNS) technologies: the original Internet standards-based BIND (Berkeley Internet Name Domain) and Microsoft Windows DNS. While these two DNS technologies are very similar and even interoperate in some ways, they are at the same time vastly different.

This section provides an overview of each technology and discusses various interoperable configurations supported within standard Microsoft Windows and Internet Systems Consortium BIND. It also reviews deployment configurations supported with the help of IPControl software, from pure Microsoft Active Directory DNS configurations to a mix of Microsoft and BIND DNS.

IPControl IP address management software system is designed to provide centralized IP address management (IPAM) features for customers who manage a number of DHCP and DNS servers from various suppliers, including ISC and Microsoft. The benefits that can be derived from supplementing Microsoft and BIND DNS deployments with IPControl's IP address management functions include:

- **Centralized IP address inventory** - The IPControl centralized IP management system can serve as a centralized IP address inventory database across both technologies.
- **Unified IP inventory and DNS configuration** - IPControl can leverage IP inventory information and associate it with corresponding DNS domains, zones, and options. This inherent association reduces errors and saves time by reducing duplicate entries of similar

information in multiple systems (for example, in a BIND text file and in a Microsoft DNS server).

- **Simplified IP management** – Manually configuring and managing DNS configurations and resource record updates is complex enough when using either BIND or Microsoft. When using both, the technical challenges of performing these updates accurately and efficiently are potentially overwhelming. IPControl supports the consistent deployment of DNS configuration information across multi-vendor DNS servers including BIND and Microsoft.
- **High availability services** – While Microsoft’s multi-master architecture is targeted to provide high availability, using IPControl, you can incorporate BIND servers into the multi-master mix.
- **Extensive user definability** – Centrally defining policies and implementing them across an IP network can promote consistency, reduce configuration errors, and allow tracking of additional information with the elements of the IP network. IPControl can define device types, define naming policies per device type, and associate a rich set of user definable fields with each device type and address type to allow individualized management of the IP network.

The following sections explain the different configuration options that are available using IPControl with Microsoft Active Directory and Microsoft DNS.

BIND DNS

Internet-standardized DNS servers have historically been based on an IETF (Internet Engineering Task Force) RFC 1034-5 (and its successors) reference implementation known as BIND (Berkeley Internet Name Domain). BIND is currently supported and maintained by the Internet Systems Consortium (ISC) and supports storage of name server and zone configuration information in text files stored on each DNS server. BIND has been extended significantly over the years, including a total rewrite of BIND with version 9, and provides extensive flexibility in terms of configurability. As is often the case, with the benefit of increasing flexibility comes increasing complexity. IPControl software can ease the complexity of configuring these very enabling features.

BIND Redundancy

BIND provides for redundancy using a master/slave relationship. A single master DNS server maintains the authoritative, administrator-created and -modified copy of information for a particular DNS domain. DNS slaves acquire their information from the master using a special copy mechanism called a zone transfer. There are two types of zone transfers: a full transfer, called AXFR, and a partial or incremental transfer (changed information only since the last full transfer), called IXFR.

AXFR Zone Transfer

The single master DNS server domain information can be manually edited by an administrator. The administrator must also update the zone serial number. When this update is complete, the slaves detect a change in the domain’s configuration via their periodic “zone refresh” polling of the master DNS server’s Start of Authority (SOA) record, which contains the current serial number. Upon detecting a serial number change, the slave may then request a full or incremental zone transfer.

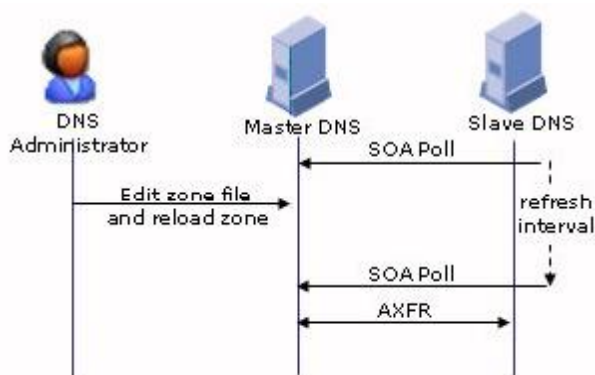


Figure 13-6 AXFR Zone Transfer

IXFR Zone Transfer

Updates may also be made dynamically from a DHCP server, for example. In this scenario, upon providing a device an IP address via DHCP, the DHCP server can dynamically update the master DNS server with the IP address to host name/domain name mapping (A and PTR records). When the master receives and accepts such a dynamic update, it will initiate a notify message to its slaves. The notify message instructs the slaves to request an IXFR to receive the dynamic updates sooner than they otherwise may have received it via zone refresh polling.

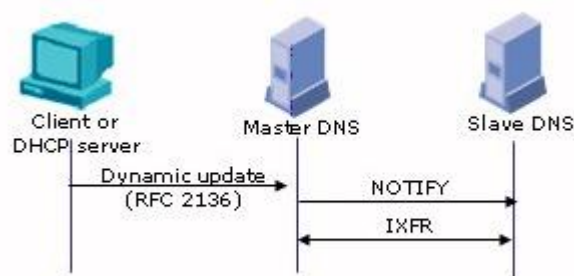


Figure 13-7 IXFR Zone Transfer

Microsoft DNS

Microsoft Windows 2003 Server and 2008 Server products provide DNS services, which support Internet standard name resolution in accordance with RFCs 1034-5. This allows standard resolver clients, Windows-based or otherwise, to query Microsoft DNS as they would BIND DNS. As we shall see, there are some areas where Microsoft supports Internet standard interfaces, such as for dynamic updates, and other areas where Microsoft supports a variation, though in some cases also Internet standards-based (for example, GSS-TSIG [Generic Security Specification Transaction Signature] *vs.* TSIG).

Microsoft's DNS services can be configured via Windows Registry, configuration files stored on the server, or AD integration of DNS zones on specially configured Windows 2003/2008 servers called Domain Controllers (DCs). The Active Directory implementation option is the most common approach as it provides the ability to run multiple master DNS servers, which can be kept in close synchronization via Active Directory replication.

Domain Controller Query

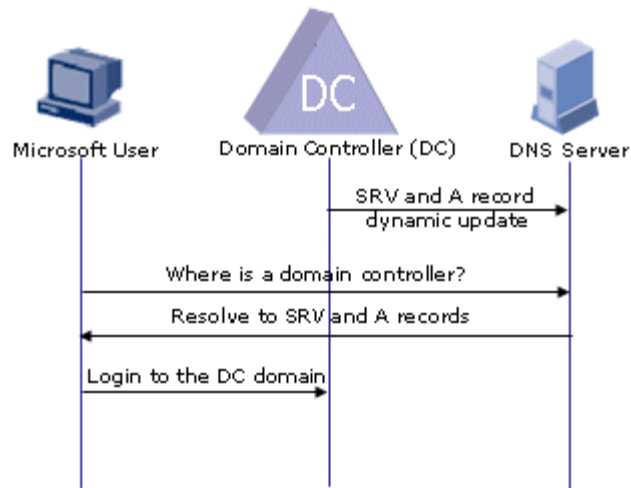


Figure 13-8 Domain Controller Query

Microsoft's AD is based on a replicated LDAP compliant directory and is used for provisioning of all authentication and network services. This AD resides on DCs. When Windows AD participating clients connect to the network, they must find a DC for validation and to access a catalog of Windows services (mainly file and print). A DC is located by querying a DNS server for a number of specialized DNS records called SRV records. Although SRV records are a standard part of the DNS system, the information returned in these records for AD are specific to Microsoft. The DNS domain in which these SRV records reside must be the same as the AD Primary Domain name in which the Microsoft client participates. (The DNS domain and the Windows Primary Domain are not the same thing; they are, however, named the same.)

These SRV records are dynamically added to the DNS space by the Windows 2003/2008 DCs using standard dynamic DNS updates, as described by the IETF RFC 2136. Beyond this element of commonality, the "normal" or standardized DNS servers begin to have a problem with Microsoft's requirements for Active Directory and DCs.

BIND DNS and Microsoft DNS Compared

The BIND master/slave philosophy is very different from Microsoft's approach to AD, where every copy of the directory is identical and replicated frequently to keep them synchronized; each AD copy is a peer to all the others. Where BIND DNS updates always go to the master first, updates to the AD can go to any peer copy. That instance of the AD then initiates a replication of that information to all other copies.

The following table highlights a few of the key differences and similarities of BIND 9 DNS and Microsoft AD-integrated DNS. Note that there are hundreds of attributes that could be compared; the point here is that each implementation of DNS brings its relative advantages with respect to the other. In most situations today, you either need to pick one implementation or the other in all but the most trivial scenario of BIND DNS supporting an Active Directory environment that itself is

not running DNS. But IPControl can help expand the possibilities by supporting additional BIND and Microsoft configurations highlighted in this section.

Table 13-1 Feature Comparison

Feature	BIND 9 DNS	Microsoft AD-Integrated DNS
Dynamic Update via RFC 2136	Yes	Yes
Support for AXFR/IXFR	Yes	Yes
Multi-Master DNS	No	✓ Yes
Slave DNS	✓ Yes	No
TSIG Support	✓ Yes	No
GSS-TSIG Support	No	✓ Yes
Standard configuration file format	✓ Yes	No
LDAP-based replication	No	✓ Yes
SRV Record support (RFC 2782)	Yes	Yes
Split DNS	✓ Yes	No
Hints file	Yes	Yes

Joint Implementation Scenarios

With both technologies bringing respective advantages, coordinated support of both technologies in various scenarios can provide significant benefits for your DNS infrastructure. IPControl software facilitates this joint technology approach by providing support for both technologies in various implementation scenarios. This section reviews five such scenarios outlining IPControl's support of standalone and mixed BIND and Microsoft DNS deployments.

Case 1: BIND DNS Supporting Non-DNS AD Environment

This case is the simplest of scenarios and requires no special interworking per se, as the DNS service resides only on BIND DNS servers. The AD environment leverages the BIND DNS server as its DNS repository and domain controllers send SRV record updates to the master DNS server when it boots. This allows Windows clients to locate their domain controller for login. Utilizing IPControl in such an environment provides the benefits of centralized configuration and leverages the many BIND configuration parameters supplied by IPControl.

IPControl can be used to not only define the servers, views, domains, and associated configuration, but additionally for centralized IP inventory. Thus, when a new IP address is assigned to a static device for example, the IP inventory can be updated via IPControl. IPControl can then automatically send a dynamic update to the master DNS server for the associated zone if desired, thereby keeping DNS information in synch with the IP inventory. Note that this update can be unsigned or signed for added security. IPControl enables simplified transaction signature (TSIG) key creation and association with pair-wise server connections, including DNS-DNS, DHCP-DNS, and IPControl-DNS connections.

As a dynamic device receives an IP address via DHCP, the DHCP server can send a dynamic update to the master DNS server on behalf of the client. The master DNS server can send a notify message to each of its slaves. The master would also be configured to also-notify IPControl (DNS Listener service) for the purpose of capturing such notify messages and executing IXFRs to capture changes

or updates to the DNS information and IP inventory in IPControl. In this manner, the IPControl centralized inventory can be kept up-to-date and accurate with respect to static device entries as well as dynamic clients obtaining IP addresses.

Figure 13-9 illustrates this configuration and these update scenarios.

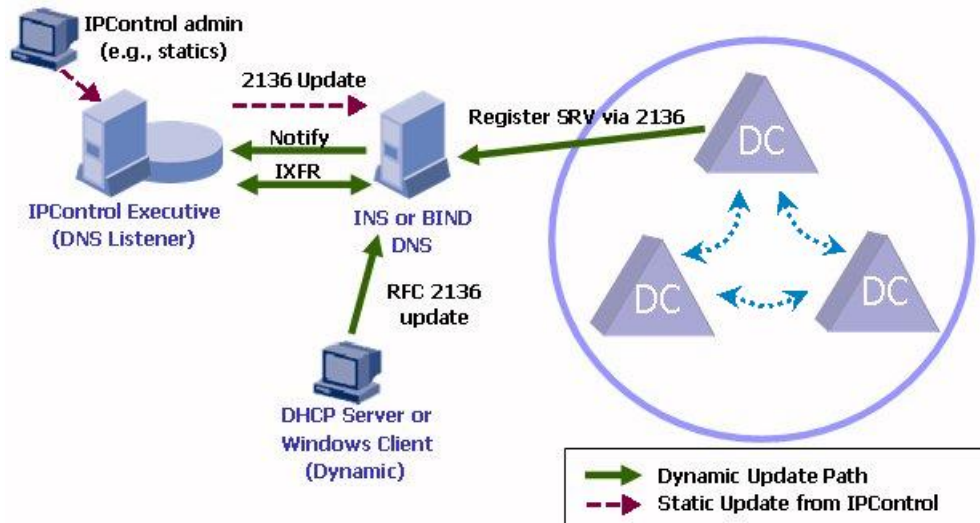


Figure 13-9 BIND DNS Supporting Non-DNS AD Environment

Reviewing Figure 13-9, following the magenta dash arrows (static update from IPControl), IPControl administrators can enter static addresses into the system, and it can automatically update the master DNS server via an RFC 2136 dynamic update (TSIG-signed or unsigned). The master can then notify its slaves of the update and perform IXFRs with each (not shown in the figure). For dynamic devices such as clients or domain controllers, they can either update the master DNS server directly or clients can update via DHCP servers as shown via the green solid arrows (dynamic update path) above. The master DNS server notifies its slaves and also-notifies the IPControl DNS Listener. The slaves and the DNS Listener perform IXFRs to get updated zone information. IPControl can then update its database with the host name, domain name, and IP address information.

Configuring Case 1 in IPControl

INS DNS (and BIND 8.x/9.x) can accept dynamic updates of SRV records from AD servers, and accept dynamic updates (A/PTR) from AD clients. Any dynamic updates accepted by INS DNS can be forwarded to IPControl (to update the IPControl database) via Notify/IXFR to the DNS Listener. Minimally, this requires that DNS options for Allow Update, Also Notify, and Allow Transfer be set appropriately for any dynamic zones.

To configure Case 1 within the IPControl system, follow these steps:

1. Create an Address Match List (select **Address Match Lists** in the DNS section of the **Management** menu) that contains all the IP addresses of your AD servers, IPControl Agents, DHCP Servers, and any specific AD clients that are updating DNS.

Edit Address Match List

Match List: DNSUpdaters

[Add to Match List](#)

Address Match List Name:

Not	Match Entry	Type	Action
	dhcp1.sw.diamondip.com	Net Service	Up Down Delete
	sapphire1.diamondip.com	Net Service	Up Down Delete
	sapphire2.diamondip.com	Net Service	Up Down Delete
	sapphire3.diamondip.com	Net Service	Up Down Delete

Submit Cancel

Figure 13-10 Edit Address Match List

- Configure the **Allow update** option on the zone to allow updates from your known Microsoft Domain Controllers, DHCP Servers, and/or IPControl Agents. Select the **Address Match List** that you defined in step 1.

Edit Zone:diamondip.com

Zone Type	master
Domain Name	<input type="text" value="diamondip.com (External)"/>
Filename	<input type="text" value="db.diamondip.com"/>
Automatic Generation of NS/GLUE Records	<input checked="" type="checkbox"/>
Use Alternative MNAME	<input type="checkbox"/>
Allow DNS Listener to Accept Zone Transfers	<input checked="" type="checkbox"/>

Submit Cancel

Zone Options Zone Extensions

☐ Show All Product Options

Enabled	Option	Value
<input checked="" type="checkbox"/>	Allow update	<input type="text" value="DNSUpdaters"/> Address List

Figure 13-11 Zone Options: Allow update

3. Configure the **Allow transfer** and **Also notify** options to allow transfers of data to the IPControl DNS Listener. In this example, the InControl Executive (DNS Listener) is at IP address 10.10.10.1.

The screenshot shows the 'Edit Zone:diamondip.com' window. The 'Zone Type' is 'master'. The 'Domain Name' is 'diamondip.com (External)'. The 'Filename' is 'db.diamondip.com'. The 'Automatic Generation of NS/GLUE Records' checkbox is checked. The 'Use Alternative MNAME' checkbox is unchecked. The 'Allow DNS Listener to Accept Zone Transfers' checkbox is checked. Below these are 'Submit' and 'Cancel' buttons.

Below the main configuration area, there are tabs for 'Zone Options' and 'Zone Extensions'. The 'Zone Options' tab is selected. A checkbox labeled 'Show All Product Options' is checked. Below this is a table with three columns: 'Enabled', 'Option', and 'Value'.

Enabled	Option	Value
<input checked="" type="checkbox"/>	Allow transfer	10.10.10.1 Address List
<input checked="" type="checkbox"/>	Allow update	DNSUpdates Address List
<input checked="" type="checkbox"/>	Also notify	also-notify { 10.10.10.1; }; Edit

Figure 13-12 Zone Options: Allow transfer and Also notify

4. Distribute the new DNS configuration to your DNS server using the **Configuration/Deployment** option, and the server will now accept updates from Active Directory, and update the IPControl as well.

Case 2: IPControl Centralized Inventory of AD DNS Environment

The next case could be viewed as the converse of Case 1. Instead of using a pure BIND DNS approach to support DNS services for an AD environment, this case utilizes a pure AD-integrated DNS approach to supporting DNS services. Case 1 demonstrated the entry of static IP addresses into IPControl, and propagation to the master Microsoft DNS server. While this scenario still applies in this case, many organizations employing AD-integrated DNS desire to alternatively have their AD administrators update AD DNS with static entries. These two “static update” scenarios are broken out in Figure 13-13.

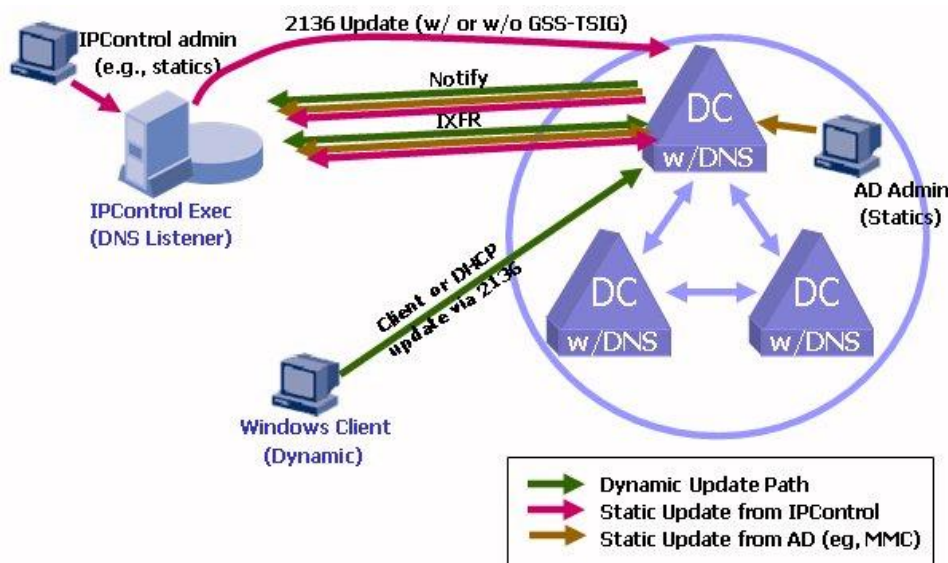


Figure 13-13 IPControl Centralized Inventory of AD DNS Environment

Static Update from IPControl

The magenta arrows once again illustrate entry of static IP addresses via IPControl. As in Case 1, IPControl can automatically update the master DNS server, which in this case is an AD domain controller running DNS. The update can be signed or unsigned, though Microsoft does not support TSIG as supported by BIND. Microsoft supports GSS-TSIG for update signing. Microsoft's implementation of GSS-TSIG utilizes Kerberos for key distribution. IPControl can participate in obtaining a key via Kerberos to sign updates to AD DNS.

Static Update from AD

The brown arrow represents static address updates from a Windows administrator, for example, via the Microsoft Management Console (MMC). The updating of IPControl with this information requires the Microsoft DNS server to have the IPControl DNS Listener configured for also-notify. When a record is updated via MMC, the AD-integrated DNS servers synchronize the update via LDAP replication and also-notify IPControl, which in turn performs an IXFR and inventory update. In this manner, organizations may manage IP inventory with IPControl, whether static devices are entered via IPControl or Windows MMC.

Dynamic Updates

Dynamic addresses would be updated in AD DNS via RFC 2136 updates from domain controllers, DHCP servers, or directly from Windows clients. Following the green arrows in Figure 13-13, this update is replicated among the AD DNS servers and the IPControl DNS Listener is also-notified. IPControl then updates its database with this dynamic host name, domain name, and IP address information.

Configuring Case 2 in IPControl

To configure Case 2 within the IPControl system, follow these steps:

1. You must first define the DNS Master Zone within Microsoft AD using the supplied Microsoft DNS “New Zone” wizard.



Figure 13-14 New Zone Wizard Welcome

2. Follow the wizard to create a new Primary Zone Active Directory integrated zone.

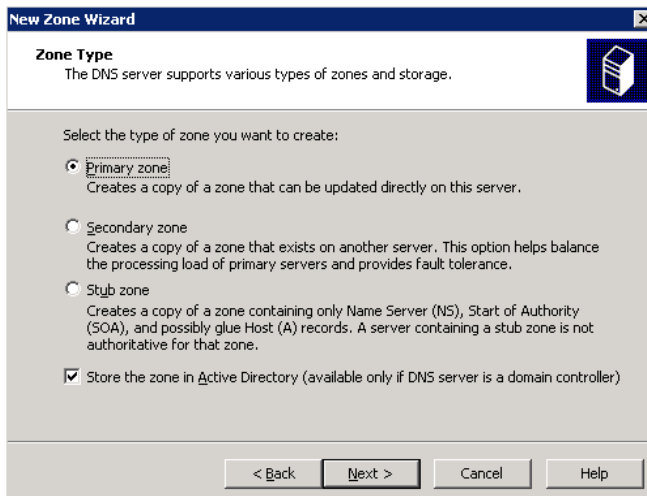


Figure 13-15 Select Zone Type

3. Select how you want to replicate zone data throughout your Active Directory Replication scope.

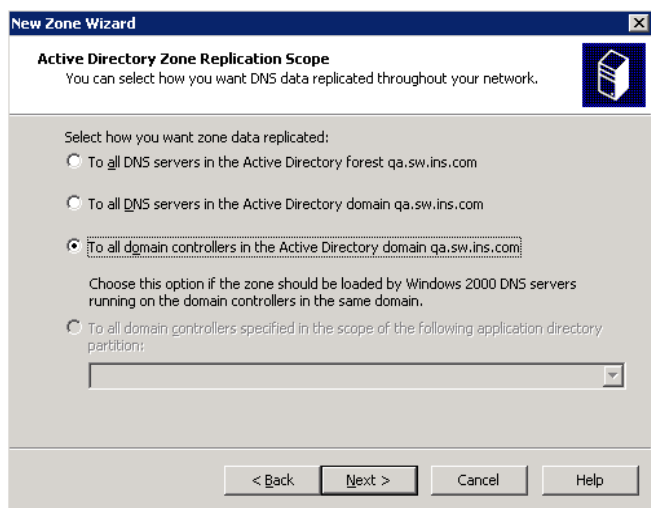


Figure 13-16 Active Directory Zone Replications Scope

4. Enter the zone name of your new zone.

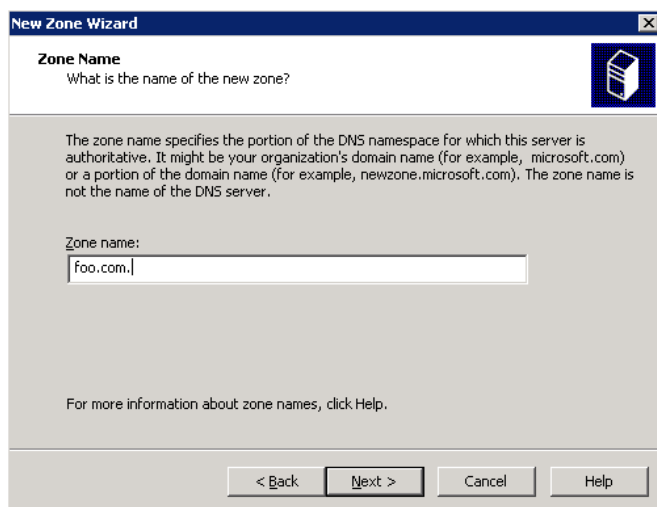


Figure 13-17 Zone Name

5. Select the dynamic update options for this zone. Select **Allow only secure updates** if you are using the GSS-TSIG secure update support within IPControl, or select **Allow both nonsecure and secure dynamic updates** if you are not using GSS-TSIG.

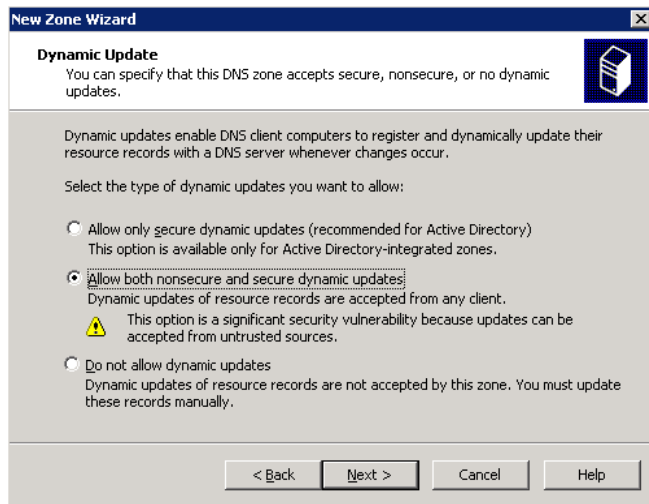


Figure 13-18 Dynamic Update

6. Complete the creation of your new zone by selecting **Finish**.

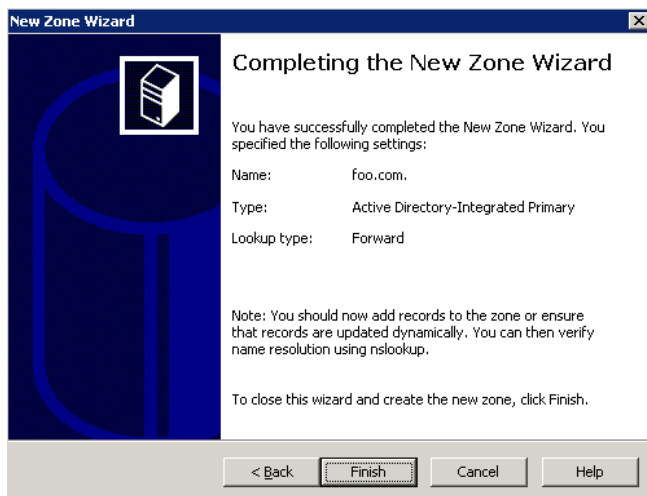


Figure 13-19 Completing the New Zone Wizard

7. Once the zone has been created, you must allow zone transfers to the IPControl DNS listener. Use the **Zone Transfers** tab of the DNS Management Console to configure the IP Address of the IPControl DNS Listener on the zone.

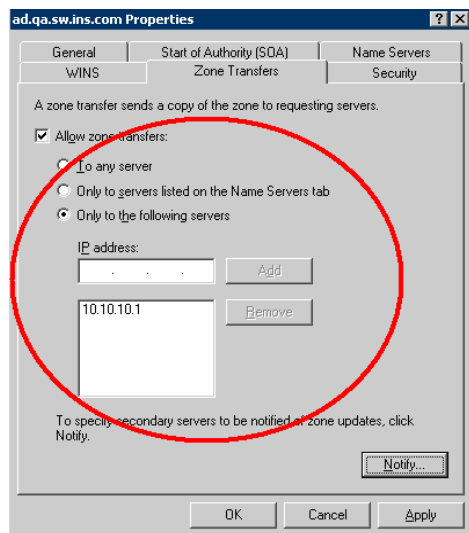


Figure 13-20 Zone Transfers Tab

8. Note that the above configuration explicitly lists the IP address of the IPControl DNS Listener (10.10.10.1). Alternatively, the **To any server** option could be selected. However, **Only to servers listed on the Name Servers tab** is not a good selection, because then the DNS Listener would need to be listed as an actual DNS server for this domain, which is not correct, since it cannot respond to queries. The DNS Listener should also be explicitly listed in the Notify list as follows. Use the **Notify** tab of the DNS Management Console to configure the IP Address of the IPControl DNS Listener.

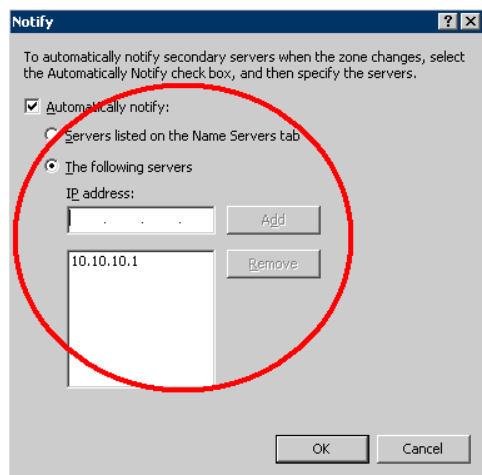


Figure 13-21 Notify Tab

9. Make sure you configure and define the Domains that you are managing within IPControl system.

Case 3: AD Multi-Master DNS with BIND DNS Slave

This case is the first of the mixed technology scenarios with one or more BIND DNS slave servers supporting AD DNS multi-master servers. The benefits of deploying this configuration include:

- **Technology diversity** – minimize implementation specific issues and reduce upgrade outages
- **Platform diversity** – especially if you run your BIND servers on Linux or Solaris; minimizes OS vulnerabilities
- **Flexible network design** – depending on design, it may make sense to deploy low end boxes running BIND in remote offices while running DCs “on the backbone.”

As displayed in Figure 13-22, this scenario is similar to Case 2, with the addition of one (or more, not shown) BIND slaves. In fact, one variation on this case is one exactly as in Case 2, with the additional also-notify for each BIND slave configured in each AD DNS server. However, referring to Figure 13-22, static IP device entries may be made either via IPControl or Windows MMC.

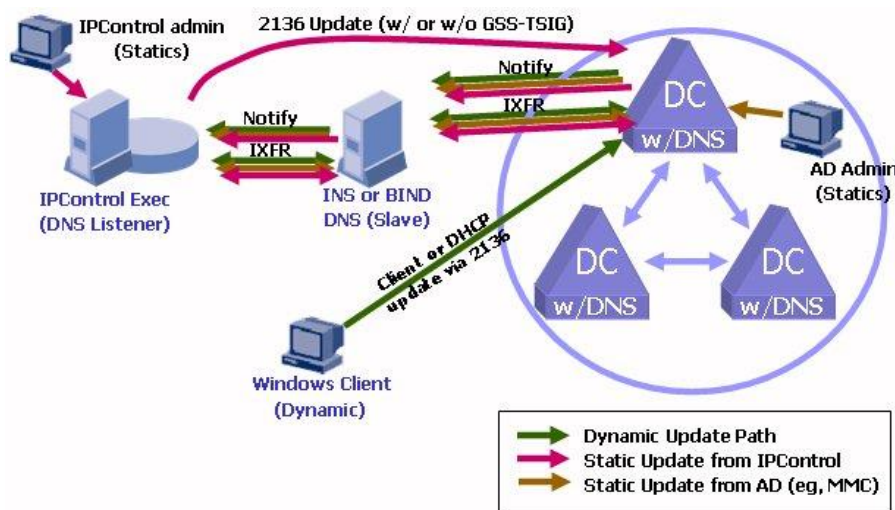


Figure 13-22 AD Multi-Master DNS with BIND DNS Slave

Updates from IPControl, following the magenta arrows (static update from IPControl) in the figure, are forwarded via signed or unsigned updates to a master domain controller. The DC updates its fellow-AD-integrated DNS servers and also-notifies the BIND DNS slaves. The BIND slaves perform an IXFR to refresh their zone data with the new static address and associated host and domain name information. The slave BIND server can in turn also-notify the DNS Listener, which in this case ignores the update given that it originated it.

Note that a variation on this case employs non-AD integrated DNS from Microsoft as master with BIND DNS as slaves. With a Microsoft file- or registry-based DNS server performing as master, updates would follow the same path described in this section, with the exception that no multi-master support and no LDAP replication would be provided. The master DNS server would receive updates statically from a Microsoft administrator or via dynamic updates from clients, DHCP servers or IPControl. The notify/IXFR process would then be invoked to update BIND or other Microsoft DNS servers acting as slaves.

Configuring Case 3 in IPControl

To configure Case 3 within the IPControl system, follow these steps:

1. Configure your domain within your Microsoft DNS infrastructure. Refer to the Microsoft documentation to create a new domain.
2. Create a slave domain within IPControl.

Case 4: BIND DNS Master with a Microsoft DNS Slave

The same basic motivations driving Case 3 also apply to Case 4. Use of diverse technologies, platforms, and design reduce exposure to particular implementations' vulnerabilities or nuances. Case 4 highlights the use of a BIND DNS server as master for a set of zones, with Microsoft DNS as slave servers. Note that AD-integrated DNS only functions as multi-master; it cannot function in a slave configuration. However, when using Microsoft's file- or registry-based implementation, Microsoft DNS servers can function as slaves.

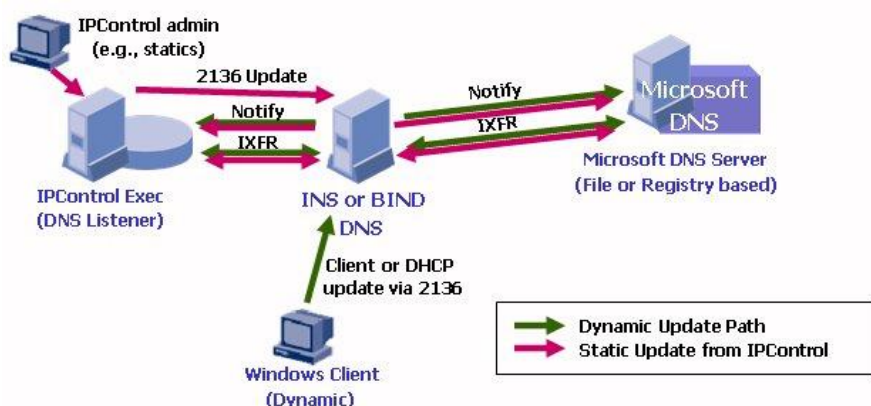


Figure 13-23 BIND DNS Master with a Microsoft DNS Slave

As illustrated in Figure 13-23, static addresses are configured via IPControl, which drives a signed or unsigned dynamic update to the master BIND server (magenta line). The master server utilizes notify/IXFR to update the Microsoft (and/or BIND) slaves as well as the DNS Listener, which ignores this update. A dynamic client's IP address to host/domain name mapping is updated in the master BIND server by the DHCP server or client itself. Utilizing the same notify/IXFR mechanism, Microsoft (and/or BIND) slaves are updated, as is IPControl via its DNS Listener service.

Configuring Case 4 within IPControl

To configure Case 4 within the IPControl system, follow these steps:

1. Configure your domain within your IPControl infrastructure.
2. Using the Domain wizard available on the Microsoft Windows 2003/2008 server GUI, create a secondary zone on your Microsoft DNS infrastructure.

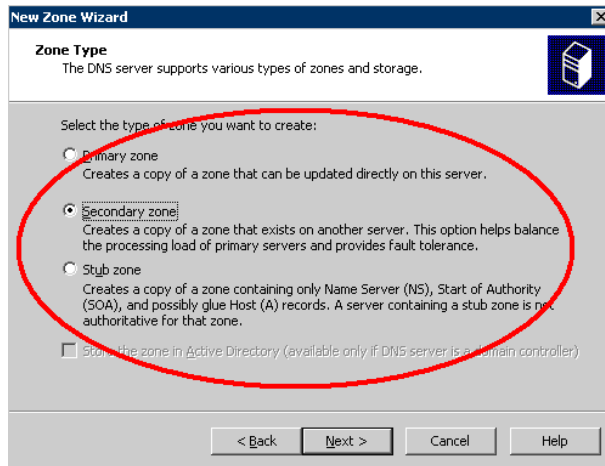


Figure 13-24 Zone Type

3. Select **Secondary zone** and click **Next**. The Zone Name screen appears.

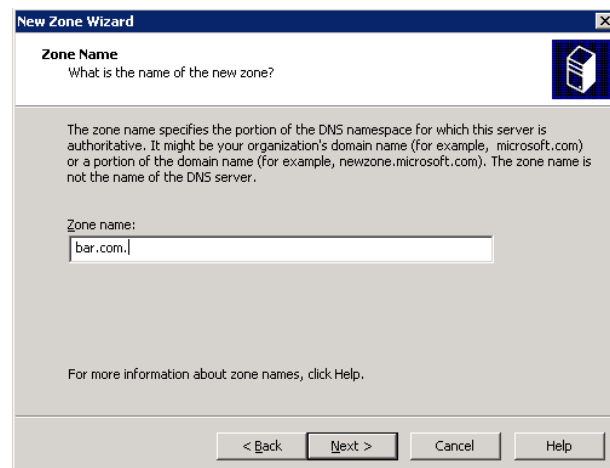


Figure 13-25 Zone Name

4. Enter the name of your domain name, and click **Next**. When prompted for the addresses of the master servers, enter the IP Address of the INS DNS server that is master for the zone.

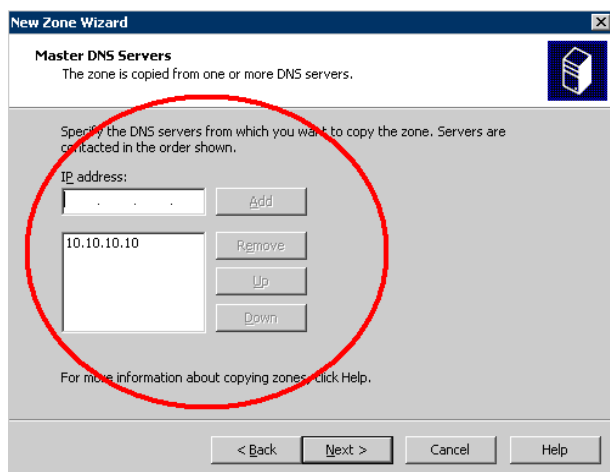


Figure 13-26 Master DNS Servers

5. In the IPControl GUI, the IP Address of the Microsoft DNS slave must be added to the **Allow transfer** and **Also notify** lists of the INS DNS master server. In the following example, the IP address of the MS DNS slave is 11.11.11.1.

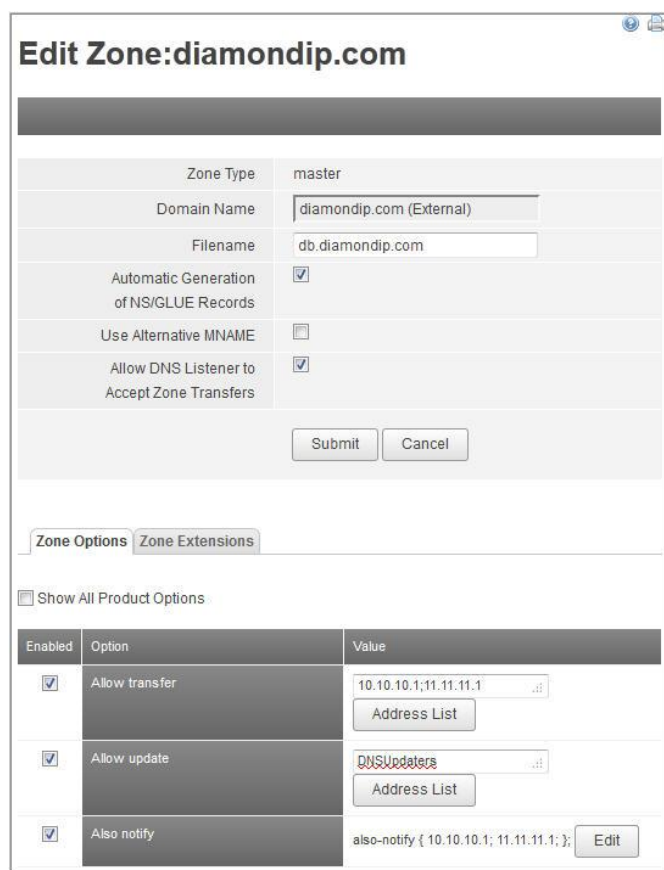


Figure 13-27 Zone Options

6. Note that alternatively, the IP address of the MS DNS slave (11.11.11.1) could be added to an Address Match List along with either the IP address of the IPControl DNS Listener or the name of a TSIG key which identifies IPControl. The named Address Match List could then be referenced in the Allow Transfer option.
7. Push your configuration file to your DNS secondary server, using the Deployment options from the IPControl system.

Case 5: PeerMaster – Effective BIND-Microsoft Multi-Master DNS

The last case is another unique case where IPControl provides substantial value in maximizing the flexibility of DNS deployments. The PeerMaster approach effectively provides multi-master DNS using both Microsoft AD DNS and BIND servers. This means that updates to either the AD DNS master or the BIND DNS “master” will be communicated to the other masters automatically.

This configuration requires use of BIND 9.2 or later. The BIND server is actually configured as a slave, but with 9.2 or later, BIND supports update-forwarding. This allows updates to be sent to the BIND slave as if it were a master, while allowing other masters to be updated automatically. This is the most complex yet enabling configuration presented to maximize the benefits of managing BIND and AD-integrated DNS together. Figure 13-28 illustrates this configuration with the four update methods:

- Static update via IPControl
- Static update via Windows (MMC)
- Dynamic update to Windows DNS
- Dynamic update to BIND DNS

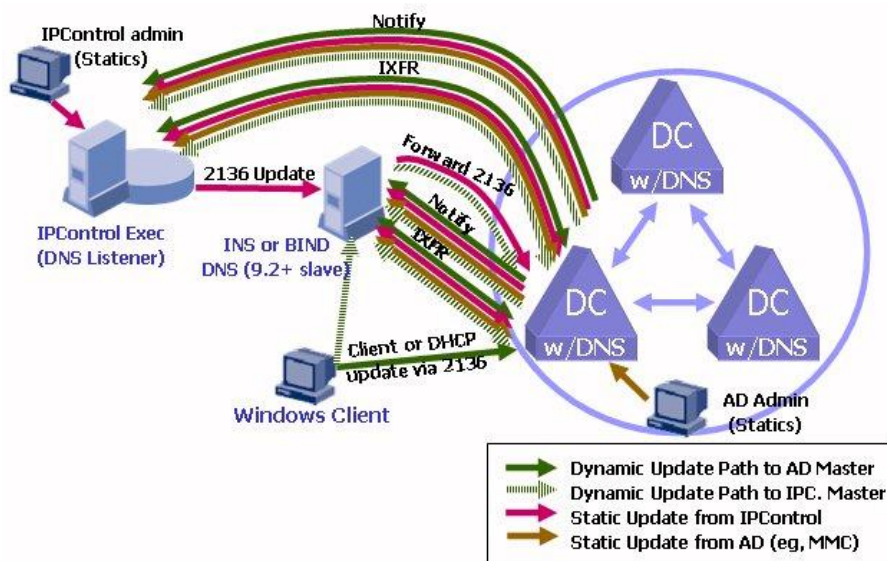


Figure 13-28 PeerMaster – Effective BIND-Microsoft Multi-Master DNS

Static Update via IPControl

If an organization's policy is to drive static address assignments via IPControl, two sub-scenarios exist for this case. Only one is shown in Figure 13-28 to keep it relatively simple. Following the magenta arrows (static updates from IPControl) in the figure, when the IPControl database is updated with the new device information, IPControl can then issue a dynamic update to a master DNS server. The first sub-scenario consists of an IPControl signed or unsigned update to a BIND slave server. With update forwarding on, the BIND slave forwards the update to its master, an AD-integrated master DNS server. The second sub-scenario comprises IPControl sending a signed or unsigned update directly to a master AD DNS server. At this point, both sub-scenarios converge, and the AD DNS server replicates the update to its AD peers, and then executes also-notify to the BIND slaves and IPControl's DNS Listener.

Static Update via Windows (MMC)

The brown arrows in Figure 13-28 indicate the flow of information when updating an AD master DNS directly via Windows, for example, via MMC. The AD master replicates to its peer AD masters via LDAP, and executes also-notify to the BIND slaves and IPControl DNS Listener, each of which initiate an IXFR to capture the update.

Dynamic Update to AD DNS

The green arrows in Figure 13-28 highlight the update path for dynamic updates to AD DNS. The master AD DNS server replicates this update to other AD masters and executes also-notify to its BIND slaves and IPControl's DNS Listener for updating of IPControl's database.

Dynamic Update to BIND DNS

The hashed green arrows in Figure 13-28 illustrate the flow for a DHCP server or client update to a BIND DNS server, appearing as a master but technically a slave. The BIND server is configured to forward updates to an AD DNS server. The AD DNS server performs its replication of the data to peer AD masters and executes also-notify to slave BIND DNS servers and IPControl's DNS Listener.

Configuring Case 5 within IPControl

To configure Case 5 within the IPControl system, follow this step:

- Configure your domains within the Microsoft DNS system. The zone should be created and defined as master for a zone, and an INS IPControl DNS server as slave for the same zone. In the slave zone definition, you need to use the "Allow Update Forwarding" option. There are two possible values to support the PeerMaster configuration:
 - ▶ **Any** - This allows any updates sent to the slave to be forwarded to the master. Any such forwarded updates are assumed to be unsecured. This is because the Microsoft AD DNS server provides only secure (GSS-TSIG) or unsecured updates as options for dynamic zones. The INS IPControl DNS slave cannot negotiate GSS-TSIG with MS AD, so the zone must be configured for unsecured updates.

- ▶ **Authorized updaters only** - Authorized updaters include IPControl Agents and Microsoft Domain Controllers (DC). This configuration places the security enforcement on the slave; however the zone master must still be configured for unsecured updates. The security on the slave is unfortunately static by nature, so as new IPAgents and/or DCs are added to the environment, the Allow Update Forwarding ACL on the slave must be updated.

Creating GSS-TSIG enabled account in Microsoft MMC

Overview

IPControl can exchange GSS-TSIG signed messages with Microsoft DNS. To make use of this mechanism, a user ID must be created on the Microsoft side, and this account must have certain attributes.

Microsoft Active Directory

Follow these steps:

1. Launch MMC and open the Users and Computers snap-in.
2. Create a new user and set the password.
3. Once user is created, right-click on the user and choose **Properties**.
4. Choose the **Account** tab.
5. Select the following checkboxes:
 - ▶ Use DES encryption types for this account
 - ▶ Do not require Kerberos preauthentication

Note: Due to various configuration options with MS AD security, if IPControl cannot authenticate with MS AD, and you receive SERVFAIL messages in the IPControl Agent log file when performing a DDNS Configuration/Deployment, you must deselect **Use DES encryption types for this account** and **Do not require Kerberos preauthentication**.

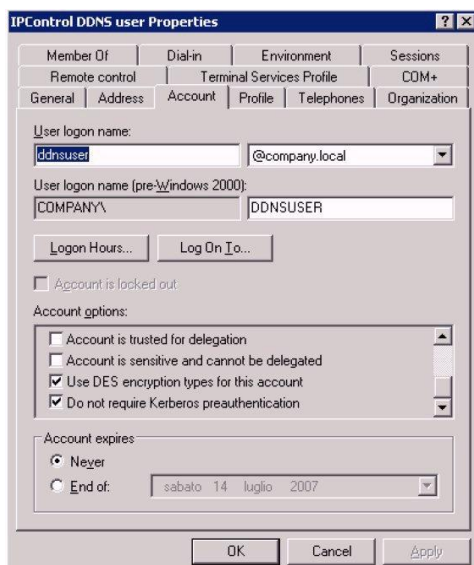


Figure 13-29 DDNS User Properties

6. Save the changes by clicking **OK**.
7. Right-click on the user and choose **Reset Password**, and set the password again.

IPControl

Follow these steps:

1. Navigate to System > Network Services Policies & Options > Server Pairs.
2. Create a server pair and ensure the following:
 - ▶ Realm name is in all capital letters
 - ▶ Realm name matches the realm used in Active Directory
 - ▶ User name and password match the case used in Active Directory

Other Considerations

Follow these steps:

1. If the Executive is running on UNIX, ensure that the FQDN of the AD server appears *before* the short hostname in /etc/hosts. Ex:
10.30.8.46 adsrvr.example.com adsrvr
2. The AD account can be either a normal user or a service account
3. The AD account must be allowed “Full Control” to each domain that is to be dynamically updated.
4. Target server must be in Notify List
5. Target server must be in Zone Transfer list.

IPControl Management of Windows DHCP Server

Overview

IPControl has the ability to create Microsoft Windows DHCP Server configuration information, providing an alternative management console that can be used enterprise wide for DHCP configuration. Dynamic objects can be defined within IPControl and then “pushed” to the remote MS Windows Server. All active lease information from MS Windows Server is displayed within the IPControl console. IPControl can also be used to create the policy that governs how the Microsoft DHCP Server performs dynamic DNS updates.

Prerequisites

- In the IPControl Executive
 - Configured Address Pools, and so on.
- On the Microsoft Windows 2003/2008 Server
 - DHCP Server running
 - IPControl Agent installed

Windows Server Procedures

Install DHCP Service

Use the Configure My Server window to add DHCP if it is not already installed. It is accessible via **Start > Control Panel > Administrative Tools > Configure Your Server Wizard**.

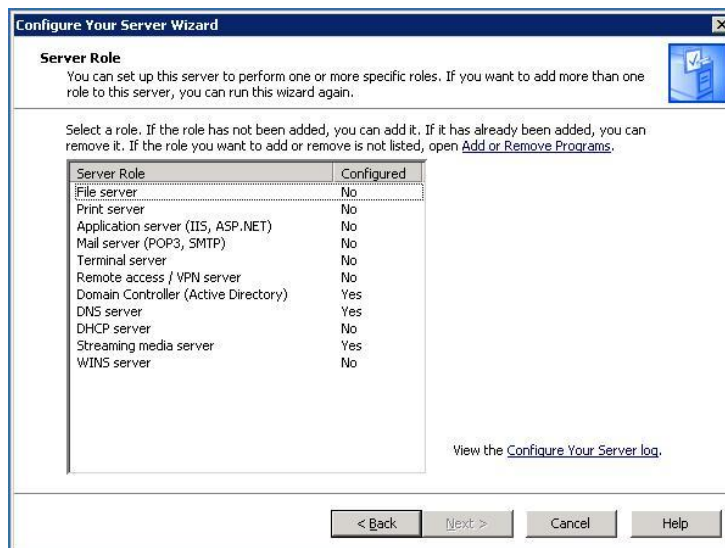


Figure 13-30 Configure Your Server

Run DHCP Configurator

Start the DHCP configuration tool using the Start Menu as shown in Figure 13-31. This application allows you to authorize DHCP and monitor all scopes, address pools, and options.

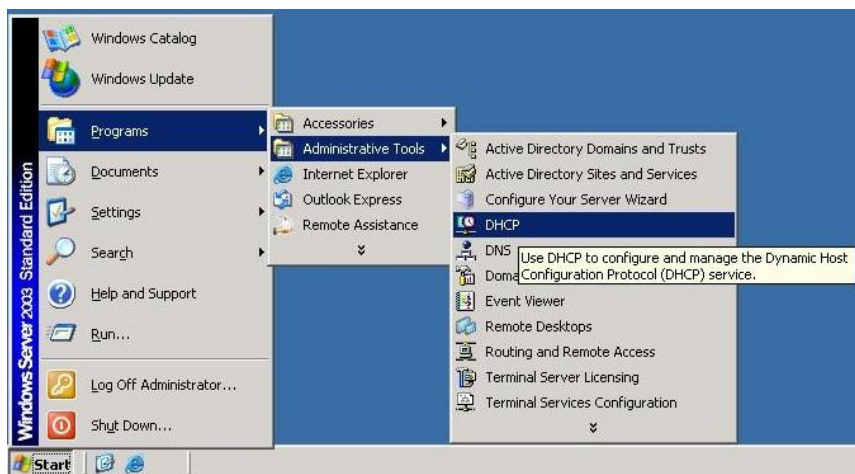


Figure 13-31 Starting DHCP Configuration Application

Verify Server is Authorized

If the server is a member of an AD Domain, the DHCP server must be authorized for the domain if it is not already. A green arrow appears on the DHCP server icon if the server is authorized. A red arrow appears if it is not authorized.

MS DHCP is now ready to be configured. This is done automatically from within IPControl – you do not have to manually add scopes from within the Microsoft application.

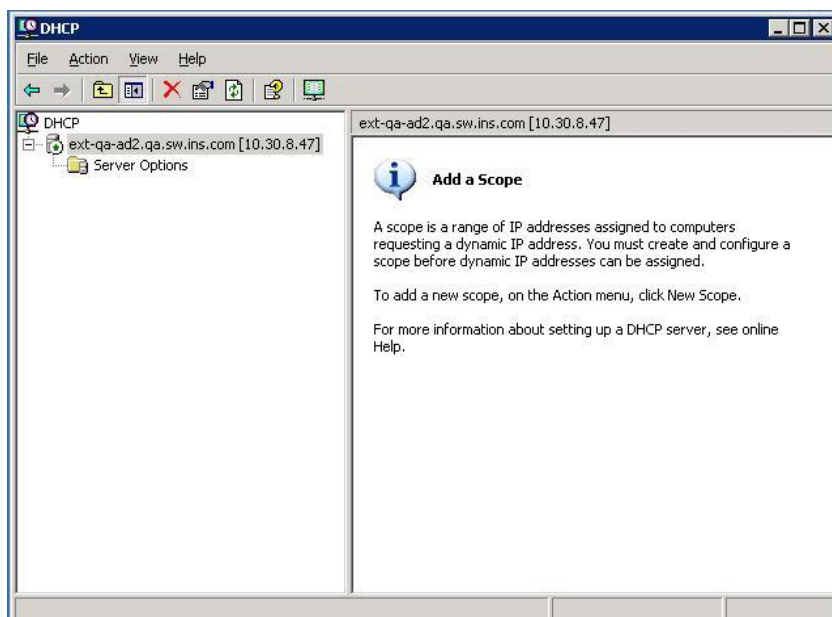


Figure 13-32 DHCP Configuration

Non-AD Domain Agent Configuration

Microsoft DHCP servers do not need to be a member of an AD Primary Domain. However, the IPControl Agent *must* be running as an account that is authorized to read and modify the DHCP options and parameters. Since a Windows Service, by default, runs as a “System” account, this authorization is not implicitly defined. Therefore, you must configure the Agent to run as an account that is authorized to access the DHCP server. This account can be a Domain user or it could be a local user, just as long as the DHCP authorizations allow that local or domain account “Write” or “Full Control” access to the DHCP server.

To modify what account a service runs as, follow these steps.

1. Open up the Window Services dialog (**Start > Program Files > Administrative Tools > Services**).

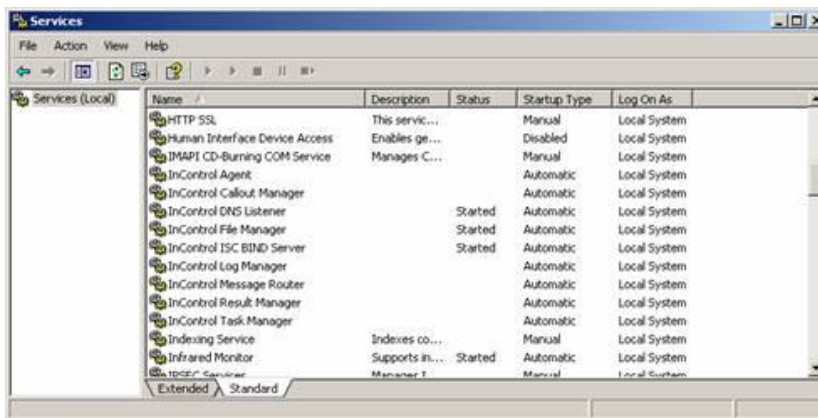


Figure 13-33 Window Services

2. Highlight the InControl Agent, right-click and select **Properties**.



Figure 13-34 InControl Agent Properties

3. Select the **Log On** tab.

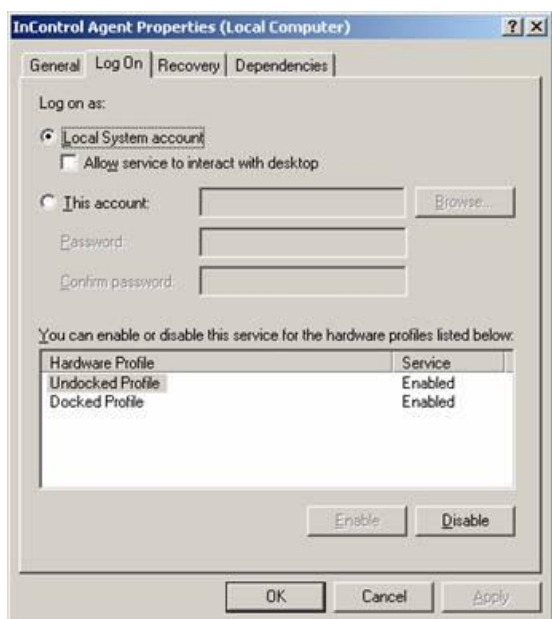


Figure 13-35 Log On Tab from InControl Agent Properties

4. Select the **This Account** option, and enter the user account and password for either a Windows Domain Account or a Local User that has access rights to the DHCP server.

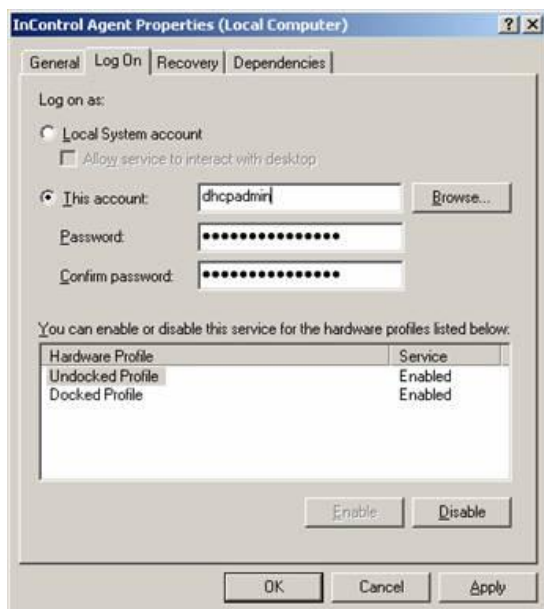


Figure 13-36 Entering Authorized Username and Password Info

5. Click **OK**.

Running the Agent as something other than the local SYSTEM account should not have an adverse effect on other Agent functions. IPControl is not impeded by and does not use or rely on Windows authentication.

IPControl Procedure

To manage the Windows DHCP configuration, a new Network Service and Agent must be added within IPControl. Follow these steps

Add Agent for MS Windows Server

Within IPControl, the Agent for the Windows Server box must be registered.

1. Select **Agents** from the Tools menu and click on **Add Agent**. Define an MS DHCP Agent and assign an IP address, as shown in Figure 13-37.

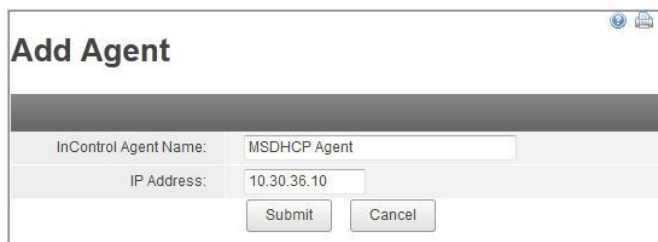


Figure 13-37 Add MS Windows Agent

Create the DHCP Network Service

2. Define the MS DHCP network service by selecting **Servers/Services** from the DHCP section of the **Management** menu.
3. Select **Add Network Services** and add the path for the DHCP configuration and lease files in the **General** tab, as shown in Figure 13-38.

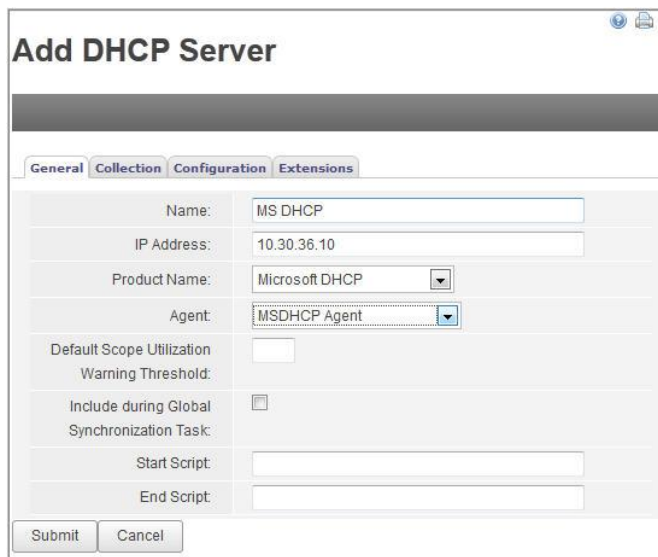


Figure 13-38 Add DHCP Server

4. In the **Configuration** tab, select the Microsoft Windows choices for the Option and Policy sets, as shown in Figure 13-39.

The screenshot shows the 'Add DHCP Server' dialog box with the 'Configuration' tab selected. The 'General' tab is also visible. The 'Configuration' tab contains the following settings:

- Perform Dynamic DNS Updates:** ☐
- Option Set:** Microsoft Windows 2000/2003 DHCP Option Set
- Policy Set:** Copy of Microsoft Windows 2000/2003 DHCP Policy Set
- DHCP Client Classes:** Add DHCP Client Class

At the bottom, there are 'Submit' and 'Cancel' buttons.

Figure 13-39 DHCP Configuration Tab

Create Address Pools

- Address Pools need to be created for dynamic assignment. Refer to “Address Pool Allocation Template” on page 281 for more information.

Deployment

- Once the DHCP Network Service and Remote Agent are defined, initiate the DHCP Push task by selecting **Configuration/Deployment** from the DHCP section of the **Management** menu and selecting **DHCP Configuration – All Files** as the **Task Type**, as shown in Figure 13-40. Ensure that you include your MS DHCP server in the **Network Service** field.

The screenshot shows the 'DHCP Configuration/Deployment' dialog box. The 'Task Type' is set to 'DHCP Configuration - All Files'. The 'When to run task' section has three radio buttons: 'Immediate' (selected), 'Scheduled', and 'Recurring'. The 'Network Service' field is empty, and there is a 'Search' button next to it. The 'Submit' button is at the bottom.

Figure 13-40 Perform Immediate DHCP Push

Successful DHCP Push

Figure 13-41 shows the Microsoft DHCP application after the DHCP Push from IPControl successfully completed. Note the new Scopes and related information.

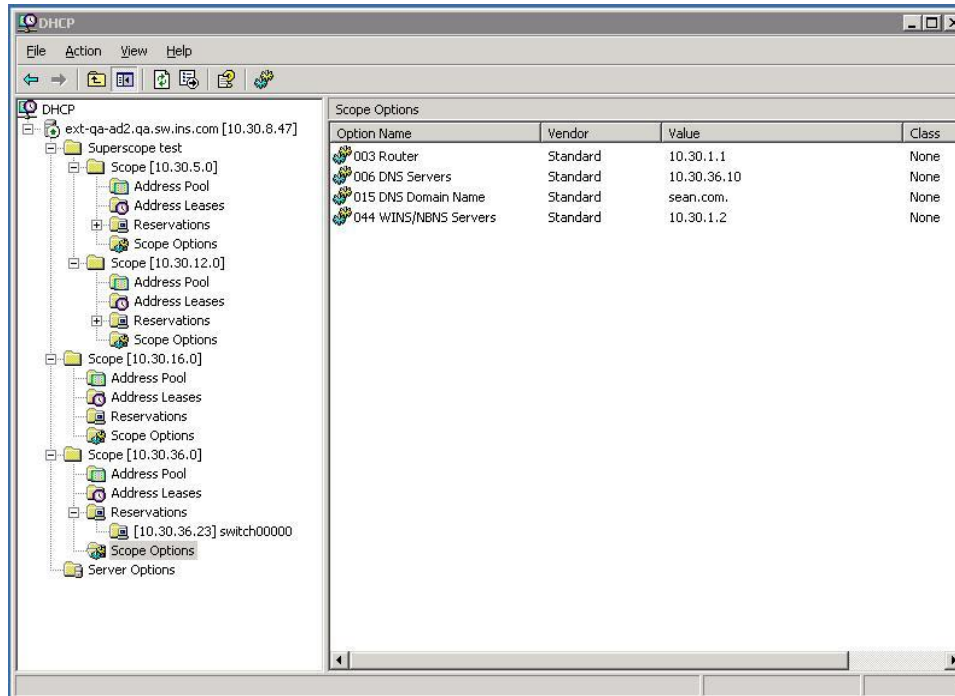


Figure 13-41 MS DHCP Application Showing Pushed Scope Information

Configuring DHCP Failover

DHCP failover is a protocol designed to allow a backup (Failover) DHCP server to take over for a main DHCP server (Primary) if the primary server is taken off the network for any reason. You can use DHCP failover to configure two DHCP servers to operate as a redundant pair (failover peers).

The INS DHCP server, working in conjunction with a powerful management tool such as IPControl, offers the unprecedented ability to configure simple or complex failover scenarios that are easy to manage.

As always, best practices for DHCP failover is to make your configuration as simple as possible, based on your unique requirements for your network.

Failover Scenarios

There are two basic scenarios for DHCP failover:

- **Simple Failover** - One server acting as the primary, and its partner acting as backup.
- **Many to One Failover** - Two or more primary DHCP servers having the same failover (backup) server.

Simple Failover

Simple failover involves a single primary server and a single failover server pair. In this example, both servers are configured with the same DHCP Scopes.

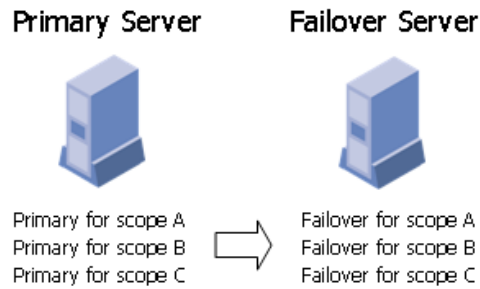


Figure 13-42 Simple Failover

The advantages of simple failover over the other scenarios are:

- You can set the failover properties within IPControl at the subnet level and you do not need to worry about managing failover settings at the individual IP Address, or IP Address Pool (scope) level.
- It is the easiest to manage as the network changes, as it is the simplest to understand, configure, and has the fewest messages.
- Provides the greatest performance benefits.

Many to One Failover

Many to One failover involves two (or more) primary DHCP servers that share a single failover server.

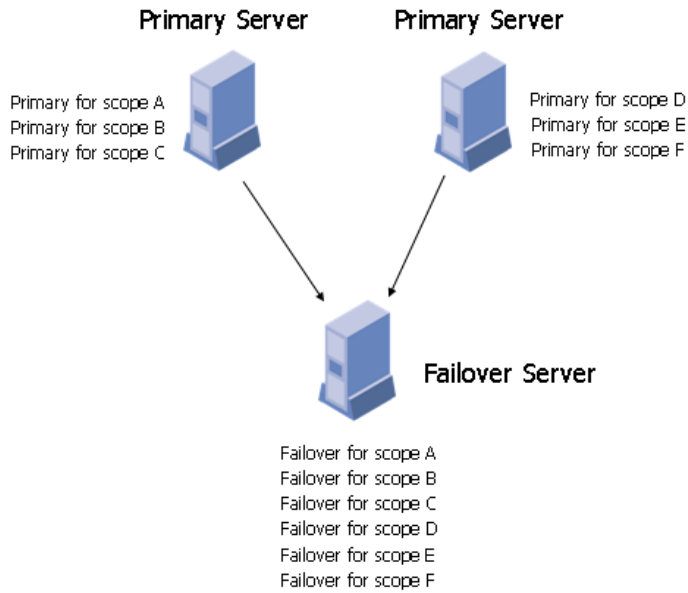


Figure 13-43 Many to One Failover

The advantages of many to one failover over the other scenarios are:

- It reduces the number of servers managed. You do not need to put a pair of servers (both primary and failover) in each location where you want to utilize failover.
- There are some disadvantages of many to one failover over the other scenarios which include:
 - ▶ The backup server must be sized to handle the sum of the configurations.

Failover Checklist

Use this checklist to prepare for an effective failover configuration:

- Design your failover strategy by selecting which type of failover scenario you will be using.
- Define your common DHCP Options Sets and DHCP Policy Sets.
- Decide on the Peering relationships that you will be using, and decide on the communication parameters that will be used between the peers.
- Duplicate the scope, policy, DHCP option, and address configurations on the partner servers. This is accomplished automatically when you perform a configuration creation task utilizing IPControl.
- Ensure that both partners are configured with a wide enough range of addresses so that the failover server can provide leases while the primary server is down for a reasonable amount of time.
- If you change any of the following configurations on the primary server, also change them on the failover server:
 - ▶ IP Addresses, IP Address Pools, IP Address Ranges

- ▶ Subnet Profiles for subnets containing Dynamic DHCP Addresses
- ▶ DHCP Policy Sets
- ▶ DHCP Option Sets
- ▶ Peer Relationship communication parameters
- ▶ User Classes / Client-classes
- ▶ Dynamic DNS update policies
- ▶ DHCP extensions
- If you use BOOTP /DHCP relays (IP helpers), configure all BOOTP/DHCP relay agents to point to both partners. This cannot be detected by IPControl or by the DHCP server. You can only detect BOOTP/DHCP configuration errors by performing live tests in which you periodically take the primary server out of service to verify that the failover server is available to DHCP clients.

Configuring Failover within IPControl

You can use the IPControl web interface to configure DHCP failover server pairs. The types of configuration options supported by managing failover server pairs are:

- Policy properties and DHCP options, including vendor-specific options
- DHCP server properties
- Scope properties and ranges
- Clients and client-classes
- DHCP Extensions

To add a failover pair, you must set the failover attributes on the DHCP server or scope level.

Configuring IPControl for Failovers

To configure IPControl for failover servers, perform the following steps:

1. Choose from the following actions.

To configure a...	Then...
Simple Failover	Define two DHCP servers (select Servers/Services from the DHCP section of the Management menu).
Many to One Failover	Define at least three DHCP servers (select Servers/Services from the DHCP section of the Management menu).

2. Create and assign the same DHCP Policy Sets, DHCP Option Sets, and DHCP Client Classes for each server, as shown in Figure 13-44. **Policy Sets**, **Option Sets**, and **Client Classes** are all created from the DHCP section of the **Management** menu.



Edit DHCP Server:
dhcp-hq.sampleco.com

General | Collection | Configuration | **Failover Peer** | Extensions

Perform Dynamic DNS Updates: ☒

Option Set: Standard ISC DHCP 3.0 Option Set

Policy Set: Standard ISC DHCP 3.0 Policy Set

DHCP Client Classes: [Add DHCP Client Class](#)

Submit Cancel

Figure 13-44 Edit DHCP Server Configuration Tab

3. Within each Primary Server's configuration, define the DHCP Failover Peer. In the My Failover Peers section of the **Failover Peer** tab, select the **Add Failover Peer** link, shown in Figure 13-45.



Edit DHCP Server: dhcp-hq.sampleco.com

General | Collection | Configuration | **Failover Peer** | Extensions

Failover IP Address:

Failover Port: 647

My Failover Peers [Add Failover Peer](#)

My Primary Peers [Add Primary Peer](#)

Submit Cancel

Figure 13-45 Edit DHCP Server Failover Peer Tab

The Add Failover Peer screen opens, as shown in Figure 13-46.

Figure 13-46 Add Failover Peer

4. Select the failover peer server from the **Peer Server** drop-down list. Note that the failover server must already be defined as a DHCP server within IPControl, before you can assign it to a primary as a peer.
5. Define a Block/Subnet to hold the DHCP address scopes (select Container View from the **Management** menu and after you have selected a Container in the hierarchy, click **Add Child Block**). In the **Policy** tab, select the **Primary DHCP Server** and **Failover DHCP Server** to be used for this subnet. Also select the **DHCP Policy Set** and **DHCP Option Set** to be used for this subnet. Click **Submit** to save.

Figure 13-47 Define Child Block for DHCP Address Scopes

6. Select the IP Address of the Block you created by highlighting the container and clicking on the IP Address of that subnet or block. Select either Define IP Addresses, IP Address Ranges, or IP Address Pools to make the desired IP address configuration. Note that you do not need to select the Primary DHCP Server, Failover DHCP Server, DHCP Policy Set, or DHCP Option Set. These can all default from the Subnet Profile that was defined in step 3, which simplifies your management over these IP Addresses. For example, if you want change any of the settings for all IP Addresses within this subnet; you can simply change the subnet profile to effect the change on all IP Addresses.
7. Perform a DHCP Configuration File Generation by selecting **Configuration/Deployment** from the DHCP section of the **Management** menu and creating configuration files for the primary and failover DHCP servers.

Administrator Access Control Use Cases

This section outlines some general Access Control use cases and how to configure either Administrator or Administrator Role policies to handle them.

Use Case - Regional Administrators

Problem

The customer has administrators that should only have access to Containers and Blocks within a specific region, say North America. Furthermore, some administrators should be able to modify items within North America, but require Read-only access to both Europe and Asia.

Solution

1. Create a role that specifies the Authorized Functions for this type of administrator, but specifies no other Access Control Lists or Domain Access. Call this **Regional Functions**.
2. Create another role that contains no Authorized Functions, but specifies North America in the Access Control List with full rights (that is, Read, Write, Delete, and Apply to Children). No other containers are listed in the Access Control List. Call this **Regional North America - Full Access**.
3. Create another role that contains no Authorized Functions, but specifies Europe in the Access Control List with only Read and Apply to Children access specified. No other containers are listed in the Access Control List. Call this **Regional Europe - Read Only**.
4. Create another role that contains no Authorized Functions, but specifies Asia in the Access Control List with only Read and Apply to Children access specified. No other containers are listed in the Access Control List. Call this **Regional Asia - Read Only**.
5. Create one or more Administrators using the combination of these four roles.

Benefits

- All Regional administrators would be given the same set of Authorized Functions. And changing this set of Authorized Functions once would propagate to all Regional Administrators automatically.
- The Administrators defined with this set of roles would have Full Access to blocks and containers within North America, and would be able to view all of the blocks and containers within Europe and Asia but could not modify them.
- Following this pattern of roles, different types of Administrators could be created easily with a mix of Full vs. Read Only access rights to each region.

Use Case - Specific Block Access Required

Problem

An administrator who is not to be granted access to a particular block type on a global basis needs access to a specific block of the denied type.

For instance, the administrator is denied access to blocks of type “Infrastructure”, but needs access to the specific block 192.168.2.0/24 in container “Miami”.

Solution

Using one of the roles specified for the given administrator (or create a new role and assign it to the Administrator), add the Container “Miami” to the Access Control List with only Read access turned on. Then add the block “192.168.2.0/24” and grant full rights.

Benefits

Using this approach the Administrator will gain access to the block necessary, but at the same time be restricted from accessing other Infrastructure blocks.

Use Case - DNS Administrator

Problem

The customer has administrators that solely handle DNS administration and they would like to assign specific Domains to groups of DNS Administrators.

One group of DNS Administrators controls all domains under “subsidiary1.com” and the “23.43.in-addr.arpa” reverse domain. Another group controls all domains under “company.com” and the “43.in-addr.arpa” reverse domain.

Solution

A privileged administrator would create a “functional” role that defined Authorized Functions which limited the user to mainly DNS related functions. We’ll call this role “DNS Functional” as an example. This role has no Containers or Domains specified in its Access Control Lists.

Another role would be created with all Authorized Function check boxes turned off and only the “subsidiary1.com” and “23.43.in-addr.arpa” domains specified on the Domain Access Control tab. This role would be called “DNS Domain subsidiary1.com” for example.

Another role would be created with all Authorized Function check boxes turned off and only the “company.com” and “43.in-addr.arpa” domains specified on the Domain Access Control tab. This role would be called “DNS Domain company.com” for example.

Finally, one set of Administrators would be created with the Administrator Roles of “DNS Functional” and “DNS Domain subsidiary1.com”. While the second set would be created using the roles of “DNS Functional and “DNS Domain company.com”.

Benefits

- This approach saves the privileged administrator from having to remember to set each of the “DNS Domain *” roles with the same Authorized Functions since the “DNS Functional” role is shared by all DNS Administrators.
- Following this pattern, if an administrator needed access to both subsidiary1.com and company.com as well as the reverse domains, the above roles could easily be added to that administrator’s profile and the administrator would immediately gain access to these domains.

Use Case - Third Party Access

Problem

Some organizations, especially ISPs, may wish to allow their customers to have access to IPControl in an effort to let them manage their own address blocks or domains. However, they do not wish to create an Administrator Role and an Administrator for each client. Furthermore, it is likely to be the case that these third party administrators would all have the same functional access, but would differ only on the objects (Blocks, Domains, Containers, etc) they could access.

Solution

Create a “Customer Function” role that defined just the Authorized Functions to be assigned to 3rd party administrators. Then, for each customer, create an Administrator using the Customer Function role. In addition, assign the appropriate objects (Blocks, Domains, and / or Containers) to the Administrator itself.

Benefits

- All 3rd party administrators would automatically get the same level of functional access to the system. Changes made once would be propagated to all administrators using the role.
- The need to create a separate Administrator Role for each Administrator is eliminated.

Configuring DNS on a TwinMirror Appliance

Running DNS on a TwinMirror requires some additional configuration due to the TwinMirror's use of a virtual IP address. Both the primary and secondary nodes in a TwinMirror configuration have a real IP address associated with their network adapters. In addition, the active node uses a virtual address to communicate with the rest of the network. When failover occurs, the secondary node takes over the virtual address, allowing uninterrupted service.

Other nodes in the network should use the virtual IP Address when communicating with the TwinMirror. This avoids the need to reconfigure those other nodes when failover occurs.

By default, DNS uses the active node's real IP address for Notifies and Zone Transfers. If other DNS nodes are using ACLs, then Notifies and Zone Transfers will no longer work after a failover.

To circumvent this, a DNS server running on a TwinMirror should be configured to use the virtual IP Address for Notifies and Zone Transfers. Any ACLs, or Also-Notify settings on other servers should also reference the virtual IP Address.

Figure 13-48 shows these two options set for a virtual IP Address of 10.11.12.13.

Add DNS Server from template "Standard for INS Sapphire DNS (BIND 9.6)"

General Logging Extensions Root Hints File Advanced **Options**

☐ Show All Product Options

Enabled	Option	Value
<input checked="" type="checkbox"/>	Notify source	10.11.12.13undefined Edit
<input checked="" type="checkbox"/>	Transfer source	10.11.12.13undefined Edit

[Submit](#) [Cancel](#)

Figure 13-48 Add DNS Server Options

Supported RFCs

IP Addressing

- [RFC2373](#) IP Version 6 Addressing Architecture
- [RFC1918](#) Address Allocation for Private Internets

DHCP

- [RFC2131](#) Dynamic Host Configuration Protocol
- [RFC2132](#) DHCP Options and BOOTP Vendor Extensions

DNS

- [RFC1034](#) Domain Names – Concepts and Facilities
- [RFC1035](#) Domain Names – Implementation and Specifications

RFC1995	Incremental Zone Transfer in DNS
RFC1996	Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
RFC2136	Dynamic Updates in the Domain Name System (DNS UPDATE)
RFC2317	Classless IN-ADDR.ARPA delegation
RFC2782	A DNS RR for specifying the location of services (DNS SRV)
Other	
RFC 2050	Internet Registry IP Allocation Guidelines