Professional Expertise Distilled

Citrix Access Gateway VPX 5.04 Essentials

A practical step-by-step guide to provide secure remote access using the Citrix Access Gateway VPX

Andrew Mallett

[PACKT] PUBLISHING enterprise professional expertise distilled

Citric Access Gateway VPX 5.04 Essentials

A practical step-by-step guide to provide secure remote access using the Citrix Access Gateway VPX

Andrew Mallett

[PACKT] PUBLISHING enterprise
professional expertise distilled

BIRMINGHAM - MUMBAI

Citrix Access Gateway VPX 5.04 Essentials

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: January 2013

Production Reference: 1170113

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-84968-822-2

www.packtpub.com

Cover Image by Artie Ng (artherng@yahoo.com.au)

Credits

Author
Andrew Mallett

Reviewers
Jack Cobben
Daniele Tosatto

Acquisition Editor
Rukhsana Khambatta

Lead Technical Editor
Ankita Shashi

Technical Editor
Kaustubh S. Mayekar

Copy Editors
Brandt D'Mello
Laxmi Subramanian
Aditya Nair
Alfida Paiva
Ruta Waghmare

Project Coordinator
Abhishek Kori

Proofreader
Lydia May Morris

Indexers
Hemangini Bari
Tejal Soni

Graphics
Aditi Gajjar

Production Coordinator
Arvindkumar Gupta

Cover Work
Arvindkumar Gupta

About the Author

Andrew Mallett has worked in the IT industry for more years than he cares to mention—well, since 1986—and with Citrix technologies since Metaframe 1.8 in 1999. He not only has Citrix skills and certification, but also teaches Linux, Novell, and Microsoft's official courses and supports many of these products. Being well-versed and certified in Linux gives him interest and skills in security and remote access, which made this an ideal book for him to write, combining Linux and Citrix into one product and book.

He currently freelances as an instructor and consultant in the UK.
You can follow him on twitter, `@theurbanpenguin`, or visit his website, `http://www.theurbanpenguin.com`.

This is my first book; having authored courseware before, venturing into books made this the next logical step. I particularly wish to thank Maddie, my first granddaughter; having my first grandchild and book in the last one year is amazing, and moreover, Maddie gave me the happiness and purpose to see it through.

About the Reviewers

Jack Cobben, with over thirteen years of systems management experience, is no stranger to the challenges enterprises can experience when managing large deployments of Windows systems and Citrix implementations. Jack writes in his off time for his own blog, `www.jackcobben.nl`, and is active on the Citrix support forums. He loves to test new software and shares the knowledge in any way he can. You can follow him on twitter, via `@jackcobben`.

While he works for Citrix, Citrix didn't help with, or support, this book in any way or form.

Daniele Tosatto is a Senior Systems Engineer based in Venice, Italy. He is a Microsoft Certified IT Professional, Microsoft Certified Technology Specialist, Microsoft Certified Solutions Expert, and Citrix Certified Administrator and has been working with Microsoft products since 2000 as a system administrator. In February 2008, he started working for the first italian Citrix Platinum Partner. He is focused on Active Directory design and implementation, application virtualization and delivery, and IT infrastructure management.

He maintains a blog at `http://www.danieletosatto.com`, and he is the author of the book *Citrix XenServer 6.0 Administration Essential Guide*, *Packt Publishing*.

www.PacktPub.com

Support files, eBooks, discount offers and more

You might want to visit www.PacktPub.com for support files and downloads related to your book.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.PacktPub.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at service@packtpub.com for more details.

At www.PacktPub.com, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.

PACKTLiB™

http://PacktLib.PacktPub.com

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can access, read and search across Packt's entire library of books.

Why Subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print and bookmark content
- On demand and accessible via web browser

Free Access for Packt account holders

If you have an account with Packt at www.PacktPub.com, you can use this to access PacktLib today and view nine entirely free books. Simply use your login credentials for immediate access.

Instant Updates on New Packt Books

Get notified! Find out when new books are published by following @PacktEnterprise on Twitter, or the *Packt Enterprise* Facebook page.

Table of Contents

Preface 1

Chapter 1: Getting Started with the Citrix Access Gateway Product Family 7

Security and Remote Access Solutions addressed by Citrix Access Gateway 8

Citrix Access Gateway hardware 10

NetScaler Model 2010 Appliance 10

NetScaler Model MPX 5500 Appliance 11

Citrix Access Gateway versions 12

Access Gateway Milestones 12

Access Gateway 10 13

Access Gateway 9.3 Enterprise Edition 14

Access Gateway 9.2 Enterprise Edition 14

Access Gateway 5.x 15

Citrix Access Gateway VPX Edition 15

Designing a secure Remote Access solution 17

Availability 17

Using ICA Proxy to access XenApp/XenDesktop 18

Ensuring there is no path for a single protocol to traverse the DMZ 18

Resolving remote access issues using Citrix Access Gateway 19

If you need access to other resources, we have full VPN connections 20

Authentication 20

PKI Certificates 20

Summary 20

Chapter 2: Licensing the Citrix Access Gateway 21

Overview of licensing CAG 21

License Grace Period 22

Platform License 22

Universal License 23

Concurrent connections 23
Citrix Access Gateway Express 23
License Server options 24
Obtaining licenses 25
Deploying Microsoft Windows Server and VPX License Server 25
Installing License Server 11.10 26
Importing License Server VPX into Citrix XenServer 28
Importing licenses and management 30
License Server Administration 33
Securing the dashboard 34
Securing License Server with HTTPS 35
Summary 36
Chapter 3: The Citrix Access Gateway Initial Setup 37
Understanding the network architecture 37
Downloading the virtual appliance from Citrix 38
Importing the Citrix Access Gateway into VMware 39
Importing the Citrix Access Gateway into XenServer 39
Initiating the Access Gateway setup from the command line 40
Completing the initial configuration from the web portal 44
Setting the admin password 45
Add a static route to a private network 45
Licensing the Citrix Access Gateway 47
Adding SSL certificates 48
Monitoring the Citrix Access Gateway 52
Summary 54
Chapter 4: Configuring a Basic Logon Point for XenApp/XenDesktop 55
Identifying the need for using CAG as a remote access solution 56
Configuring a Citrix Web Interface site for use with the Citrix Access Gateway 57
Web Interface placement 58
Configuring a website for remote users 59
Changing the Secure Access method 62
Configuring an Access Gateway basic logon point 65
Logon point 66
XenApp and or XenDesktop access controls 70
Secure Ticket Authority 71
Accessing XenApp Server farms securely with the Citrix Access Gateway 72

Extending the basic logon point to access other internal web-based resources 73
Keeping your users happy 77
Auditing access to the Citrix Access Gateway 78
Summary 80
Chapter 5: Creating Authentication Profiles 81
Authentication profiles 82
Creating a RADIUS authentication profile 83
Configuring Gemalto Protiva 86
Configuring SafeWord 87
Creating RSA SecurID authentication profiles 88
Creating LDAP authentication profiles in Microsoft's Active Directory 90
Authentication using the Active Directory sAMAccountName 92
Authenticating using the Active Directory userPrincipalName 93
Tracking user access 94
Creating LDAP authentication profiles in Novell's eDirectory Directory 94
Creating LDAP authentication profiles to Linux openLDAP 95
Customizing the Citrix Access Gateway logon page 96
Allowing users to change passwords on the logon page 98
Implementing two-factor authentication on the Citrix Access Gateway 100
Summary 102
Chapter 6: Beyond the Basics 103
Adding universal licenses 103
Citrix Access Gateway plug-in installation 104
Obtaining the plug-in 105
Installing the plug-in 105
Configuring the plug-in properties 107
Integrating the Access Gateway plug-in with the Citrix Receiver 111
Distributing the Access Gateway plug-in with the Citrix Merchandising Server 112
Configuring deliveries with the Merchandising Server 114
Summary 117
Chapter 7: Address Pools 119
Creating address pools 119
Before we connect with the plug-in 122
Ping after the VPN is created with the plug-in 123

Accessing the welcome page on the web server 123
Smart logon points use universal licenses 125
System Administration Options 126
Networking 127
Appliance failover 127
Name service providers 127
Static routes 128
Address pools 128
Deployment mode 128
Password 128
Date and time 129
Licensing 129
Logging 129
Summary 130
Chapter 8: Device Profiles and Endpoint Analysis 131
Device profiles 132
File 133
Process 133
Registry 134
Operating System 135
Ports 136
Building an effective scan expression 137
Installing the endpoint analysis plug-in 138
Control Access to network using device profiles 141
Summary 141
Chapter 9: Defining Network Resources 143
Network resources 143
Network lists 148
General Properties 149
Protocols and port ranges 149
Introducing the Citrix Branch Repeater 150
Citrix Branch Repeater products 150
Summary 153

Chapter 10: SmartAccess Logon Points 155
Defining SmartAccess logon points 155
General Properties 157
Authentication 158
Defining the term Logon Point Visibility 160
Branding the logon point 161
Summary 162
Chapter 11: Linking It All Together with SmartGroups 163
Defining SmartGroups 164
General Information 164
Home Page 165
Group Criteria 166
Logon Points 166
Device Profiles 166
Group Membership 167
Group Settings 169
Network Resources 169
Address Pools 171
Advanced Properties 172
Defining SmartGroup priority 174
Summary 175
Chapter 12: Connecting to SmartAccess Logon Points 177
Delivering the Access Gateway plug-in 177
Configuring Access Gateway Plug-in settings 180
Managing the client plug-in 182
Connecting to resources on the private network 184
Summary 186
Chapter 13: Monitoring the Citrix Access Gateway 187
Accessing and interpreting logfiles 187
System Information 188
Running Information 189
Active Sessions 190
Configuration and Warnings 192
Audit Log 192
Info Log 193
EPA Log 193
Debug Log 193

Logfile settings and log transfer **194**
Creating configuration snapshots and importing firmware updates **196**
Implementing appliance failover **198**
Configuring the master device 199
Configuring the slave device 200
Summary **202**
Chapter 14: Command Line Management of the Citrix Access Gateway **203**
Enabling SSH access to the command line **203**
Managing the Citrix Access Gateway from the command line **205**
Express Setup 205
System 206
Troubleshooting 207
Help 209
Summary **210**
Index **211**

Preface

No matter how new you are to Citrix or for how long you have used it, we are going to show you how you can extend the use of Citrix products to beyond the confines of your corporate network, making full use of the "any device anywhere" tag line used in Citrix marketing. Citrix Access Gateway can provide full VPN access to your network or simple ICA Proxy, and Citrix Access Gateway VPX 5.04 Essentials will show you how to step through the complete process of configuring the appliance. Providing easy-to-follow guides that you will be able to follow as a seasoned Citrix professional or newbie, this book will take you through the full and complete deployment of the appliance.

What this book covers

Chapter 1, *Getting Started with the Citrix Access Gateway Product Family*, will describe the purpose of Citrix Access Gateway and the models that are available and their associated features. This chapter will serve as a good introduction to the product range and will help in choosing the correct model to meet a required business need.

Chapter 2, *Licensing the Citrix Access Gateway*, will walk you through Citrix licensing and its available options. You will discover the MyCitrix website, where licenses are obtained, and this will help with the assignment of hostnames to licenses. Licenses can be delivered from CAG or from a specific license server.

Chapter 3, *The Citrix Access Gateway Initial Setup*, will enable you to complete the first step in using CAG, which is to import it into our virtualization hosts and to configure networking, passwords, and adding SSL certificates.

Chapter 4, *Configuring a Basic Logon Point for XenApp/XenDesktop*, will provide guidance in the usage of the platform license, which you can use to establish unlimited connections to XenApp/XenDesktop servers and is widely used in this manner as an ICA Proxy. We will look at how to create this proof-of-concept system by creating a basic logon point and using authentication at the web interface server. This is the simplest form of CAG and provides a quick and easy start into using this system.

Chapter 5, *Creating Authentication Profiles*, will walk you through the authentication at the Citrix web interface, which is a simple solution but limits the usage of CAG; that is, being limited to just basic logon points. From a security perspective, passing authentication to the web interface server is allowing traffic to pass to another device that, as yet, had not been authenticated; authentication should be handled at the point of entry and nowhere else.

Chapter 6, *Beyond the Basics*, will introduce SmartAccess logon points and what is available with the universal licenses. Not only can we connect to XenApp and XenDesktop, but we now also have full VPN access to internal resources, such as internal e-mails, intranets, and network file shares.

Chapter 7, *Address Pools*, will show you how Address Pools allow your SmartAccess clients to be issued with an IP address to access internal resources. These may be required for some services that do not allow multiple connections from a single device.

Chapter 8, *Device Profiles and Endpoint Analysis*, will talk about using device profiles with SmartAccess, which enables us to identify different classifications of client machines the device profiles can control (which resources they can access and which policies will apply if they access XenApp or XenDesktop). Typically, we may need to be able to differentiate between corporate-managed computers and personal computers.

Chapter 9, *Defining Network Resources*, will walk you through CAG SmartAccess, which allows you access not only to Citrix XenApp and Citrix XenDesktop but also to internal resources, such as network file shares and e-mails. In this chapter, we will look at specifying network resources that we wish our users to have access to and those that they should not.

Chapter 10, *SmartAccess Logon Points*, will talk about how, when we are nearing the end of the configuration, we add SmartAccess logon points to the management console, providing full VPN access to internal networks.

Chapter 11, *Linking It All Together with SmartGroups*, will discuss Smart Groups that enable resources to be linked to logon points. These are added through the management console and can be described as the glue of the SmartAccess solutions.

Chapter 12, *Connecting to SmartAccess Logon Points*, will investigate how we can connect to our newly created SmartAccess logon points by using a web browser or the secure access plug-in.

Chapter 13, *Monitoring the Citrix Access Gateway*, will discuss how to monitor and maintain CAG. Having set up the gateway, it is important to be able to keep it running effectively. This will involve monitoring connections and logs, backing up the configuration with snapshots, and upgrading the firmware. Once we have this in the bag, we need to look into providing high availability using appliance failover.

Chapter 14, *Command Line Management of the Citrix Access Gateway*, will explain using the command line, and we will investigate some of the options available. Although most management is maintained via the web console, some elements can be managed from the command line, and we look at when and why we use this.

What you need for this book

To make full use of this book, you will need to have basic knowledge of Citrix products such as XenApp (or its predecessor, Presentation Server) or XenDesktop, and we will be implementing or investigating remote access solutions. Although no prior knowledge of virtual private networks is required, we would expect that you have basic grounding in IP-based networks and routing.

Who this book is for

This booked is aimed at system administrators implementing or working with the Citrix Access Gateway 5.x virtual appliance, and it is also for those who are looking for a detailed handbook on the day-to-day administrative tasks that managing a Citrix remote access solution entails.

Conventions

In this book, you will find a number of styles of text that distinguish between different kinds of information. Here are some examples of these styles, and an explanation of their meaning.

Code words in text are shown as follows: "On 64-bit systems, this defaults to `c:\Program Files (x86)\Citrix`."

Any command-line input or output is written as follows:

```
xe vm-import -s 192.168.0.12 -u root -pw Password1
filename="c:\tmp\cag_5.0.4.223500.xva
```

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "If using the CAG as License Server, the CAG name must be in the **HOST ID** field".

> Warnings or important notes appear in a box like this.

> Tips and tricks appear like this.

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book—what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to `feedback@packtpub.com`, and mention the book title via the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on `www.packtpub.com/authors`.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books—maybe a mistake in the text or the code—we would be grateful if you would report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting `http://www.packtpub.com/support`, selecting your book, clicking on the **errata submission form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded on our website, or added to any list of existing errata, under the Errata section of that title. Any existing errata can be viewed by selecting your title from `http://www.packtpub.com/support`.

Piracy

Piracy of copyright material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works, in any form, on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at `copyright@packtpub.com` with a link to the suspected pirated material.

We appreciate your help in protecting our authors, and our ability to bring you valuable content.

Questions

You can contact us at `questions@packtpub.com` if you are having a problem with any aspect of the book, and we will do our best to address it.

1
Getting Started with the Citrix Access Gateway Product Family

If you have ever tried navigating the range of products and vendor websites, you will be able to sympathize with those poor souls trying to come to terms with all of the different options that Citrix has for the Access Gateway products. So many choices! Soon, you will also find out that the costs of these products will vary from nothing to many thousands of dollars. The aim of this introduction is to help you become familiar with the range and make some informed decisions about which product is right for you. Throughout the book, we will work with the VPX edition (virtual appliance); however, most of the configuration remains consistent between the models. Additionally, at this stage, we also need to show you where **Citrix Access Gateway** (**CAG**) will fit into your corporate remote access and security environment.

Specifically, in this chapter, the following topics will be looked at in detail:

- Security and Remote Access solutions addressed by CAG
- Citrix Access Gateway hardware
- Citrix Access Gateway specifications
- Citrix Access Gateway versions
- Citrix Access Gateway VPX
- Designing a secure Remote Access solution

Security and Remote Access Solutions addressed by Citrix Access Gateway

Firstly, let us address a little of the history of Citrix Systems, the purpose of CAG, and why this is used within corporates, from small companies to large enterprise networks.

Citrix has been providing levels of remote access since 1989, first with their Multi-User OS2 terminal server. Following the success of Citrix-Multi-User, they went on to develop for the Microsoft Windows operating systems and the milestones include:

- 1993 – WinView releases
- 1995 – WinFrame releases
- 1998 – MetaFrame releases
- 2008 – XenApp releases

In the early days of WinFrame and MetaFrame terminal servers, you would have to provide some third-party **virtual private network** (**VPN**) solution to be able to access these servers from the Internet. In many respects, the weakness of these early solutions is that they do not address secure remote access.

To mitigate this issue, Citrix introduced a product into the market, in 2001, called **Citrix Secure Gateway** (**CSG**). This is still available today and is bundled with XenApp 6.5. This, much in the same way as CAG, is a remote access solution that can be used to provide remote users on the Internet connectivity to your internal resources, such as your XenApp or XenDesktop servers.

Without CAG or CSG, each Citrix XenApp server and/or each XenDesktop virtual machine would require a public IP address to be accessible from the outside world. Of course, this is not practical, especially when we look at XenDesktop; do you have 300 public IP addresses available for your virtual desktops or VDI environment?

Both the CSG and CAG can act as an ICA proxy to provide connectivity to your internal Citrix servers.

> ICA is the Citrix protocol for remote access. This can be listened on TCP port 1494 (for standard ICA connections) or TCP port 2598 (for session reliability). Session reliability tunnels ICA traffic through port 2598 to allow for momentary loss of connectivity, as would be experienced with mobile networks, and to allow seamless reconnection to the session.

So, if both devices can provide the ICA proxy functionality, why use CAG?

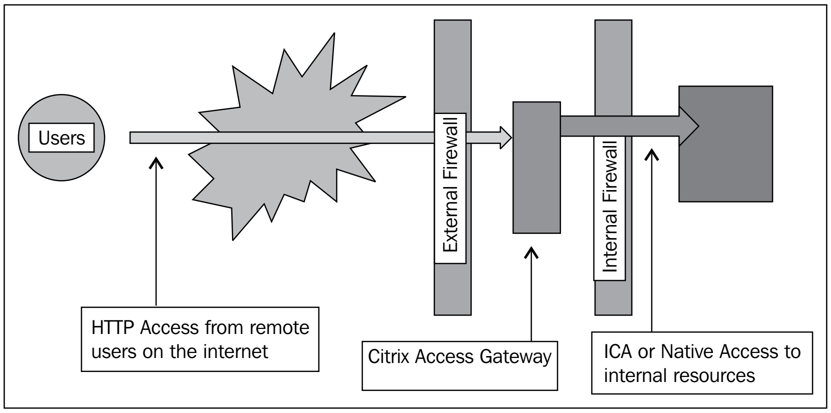
In 2005, Citrix systems acquired NetScaler, Inc. This gave them the NetScaler product range, and ultimately, Access Gateway. Quite simply, CAG is a secured system dedicated to remote access. It is supplied as either a hardware appliance or virtual appliance.

By "dedicated", it is meant that CAG has no other function, purpose, or unnecessary services. It is hardened or locked down for security at the time of production. CSG, on the other hand, is a software that installs onto a running operating system. We are, then, reliant on the OS that it is installed upon to be specifically hardened to provide the same level of security that you find out-of-the-box with CAG.

In addition to this, CAG can provide standard VPN connectivity into your private networks for remote users, not just connectivity to XenApp or XenDesktop. Choosing the appliance-based CAG includes support for additional applications and protocols. The software-based Secure Gateway is not only less secure but is also limited to supporting traffic directed to computers running XenApp or XenDesktop. Therefore, organizations that use the Secure Gateway might also have to deploy a remote access solution for other types of internal network resources, adding additional expense and management workload for already busy administrators.

CAG can handle your organization's remote access needs by securing traffic to applications hosted by Citrix XenApp and desktops hosted by Citrix XenDesktop as well as access to internal resources, such as e-mail, internal Web applications, and network file shares. In short, CAG is a secure remote access solution to provide VPN or ICA proxy access to internal resources to your mobile or remote workforce.

The following diagram illustrates that users connecting from the Internet pass through the external corporate firewall to the Access Gateway. From here, the incoming HTTPS is converted to an ICA stream targeting XenApp or XenDesktop servers. Possibly, even native protocols are converted to non-Citrix products when using a full VPN connection.


Users
External Firewall
Internal Firewall
HTTP Access from remote users on the internet
Citrix Access Gateway
ICA or Native Access to internal resources

Citrix Access Gateway hardware

CAG, as mentioned already, can run as a virtual appliance or on physical hardware. The physical hardware device is a dedicated Citrix NetScaler appliance and comes in various shapes and sizes. The CAG firmware is installed into the NetScaler appliance, which runs an embedded Linux operating system. The same firmware that is used to run CAG on the hardware appliance can be used on the VPX edition, for example, both the VPX appliance and NetScaler 2010 model run Access Gateway 5.x firmware.

NetScaler Model 2010 Appliance

Model 2010 Appliance represents entry-level dedicated hardware and supports Access Gateway 5.0 and Access Gateway Standard Edition. In this book we will focus on Access Gateway 5.0.4. You can install Model 2010 in the DMZ or the secure network. The preconfigured IP address of the Access Gateway is `10.20.30.40`. Citrix will tell you that you are able to change the IP address using a serial cable and a terminal emulation program such as Microsoft Windows Telnet Client, or you can connect Access Gateway using network cables and Access Gateway Management Console in Access Gateway 5. Usually, connecting via the network to change the IP address is the simplest method; just ensure you are plugged into a non-production environment when making the change, and then switch the appliance back into the DMZ. The following is a screenshot of NetScaler MPX 5500 Appliance model:

NetScaler Model MPX 5500 Appliance

This model boasts multiple processors, and from that, you can gain faster throughput and more concurrent connection support. Citrix provides Access Gateway in multiple forms to suit your organizational needs. This model supports Access Gateway Enterprise Edition. The preconfigured IP address of Access Gateway is `192.168.100.1` with a 16-bit or class B subnet mask. The IP address is changed in the same way as Model 2010.

Other hardware appliances are available to support the growing amount of concurrent connections that you may require.

You can install the Access Gateway Enterprise Edition appliances in the DMZ or the secure network as with Access Gateway 5.

The main difference between the models is their hardware specifications. The higher the specification of the hardware, the more users the appliance will support, and it will be quicker in those tasks. One of the first tasks in the planning of your appliance is to answer the question "how many concurrent connections do we need to support?" or, simply "how many users will be connected to the appliance at the same time?".

> If you are using VPX, the specifications can be managed by assigning fewer or less resources such a RAM and CPU to the virtual machine.

The following table conveniently lists each of the hardware appliances and their main specifications:

Appliance Specifications	**2010**	**5500**
Processors	1	1 dual core
RAM in GB	1	4
Power supplies	1	1

Appliance Specifications	2010	5500
Power in watts	250	300
Rack height	1U	1U
Weight	12 kg	13 kg
Heat output	950 BTU/hour	767 BTU/hour
PSU life	48,000 hours	108,000 hours
Concurrent users	500	5000
NICS	2	4 plus management and HA

Citrix Access Gateway versions

The very latest version of Access Gateway, as of June 2012, is Access Gateway 10, which is being introduced as a replacement for Access Gateway 9.3 Enterprise Edition.

Both the Access Gateway 9.x and 10.x models require NetScaler 5500 or higher as a hardware platform. The earlier editions of Access Gateway Version 4.x and 5.x can run on NetScaler 2010 or the virtual appliance. Many of the features are the same, but it is the enterprise class high availability of the premium models that sets them apart. Much of this high availability can be mirrored within your virtual host environment if you choose to use the VPX editions.

To gain an appreciation of where Citrix began on the Access Gateway product, we introduce to you the major milestones for the product under the ownership of Citrix Systems.

Access Gateway Milestones

Milestones of Access Gateway include:

- 2005 – Citrix acquires NetScaler
- 2005 – Citrix Access Gateway names product of the year by SearchNetworking
- 2006 – Citrix Access Gateway Enterprise Edition launches
- 2008 – MPX or multi-processor version of the Access Gateway hardware appliances (NetScaler) launches
- 2009 – Citrix launches Access Gateway VPX edition, a cost-effective replacement for CSG in 2009
- 2012 – CAG 10 introduces in 2012

Access Gateway 10

The latest and greatest offering from Citrix, Citrix NetScaler Access Gateway Version 10, offers support for:

- Clientless access for a receiver on the Web:
    - Connect to your internal resources with a secure VPN connection with just a web browser
- Multi-stream ICA that allows you to partition multiple ICA streams in the same session:

  Multi-stream ICA is a **quality of service** (**QoS**) enhancement developed in XenDesktop 5.5 and XenApp 6.5. When implemented, Multi-stream ICA uses four separate TCP connections to carry the ICA traffic between the client and the server. Each of these TCP connections will be associated with a different class of service. ICA traffic has always implemented multiple internal channels. These channels represent clipboard mapping, audio, drive mappings, and so on. With Multi-stream ICA, the four TCP connections are assigned a QoS priority, and each ICA stream is defined to work with one of these TCP connections inheriting the QoS.

    - Very high priority (for real-time channels, such as audio)
    - High priority (for interactive channels, such as graphics, keyboard, and mouse)
    - Medium priority (for bulk virtual channels, such as drive mapping, scanners)
    - Low priority (for background virtual channels, such as printing)
- Web socket protocol support that allows bi-directional communication between user devices and servers over HTTPS.

Organizational benefits of Access Gateway 10 include:

- Secure remote access for the most demanding and complex environments that require increased scalability and performance
- High availability of guaranteed access to resources and compliance with **Service-level agreements** (**SLA**s)
- Highest level of integration and control of remotely delivered Citrix XenApp applications, data through SmartAccess (endpoint analysis), and published desktops with Citrix XenDesktop

- Natural progression for existing XenApp customers who have used the Secure Gateway and wish to benefit from the added security and full VPN access
- Enterprise-class SSL VPN features, including client-side cache cleanup, detailed auditing, and policy-based access control for web and server applications
- Ability for remote users to work with files on shared network drives, access e-mail and intranet sites, and run applications as if they are working within your organization's firewall
- Support for the Access Gateway universal license. These licenses enable SmartAccess and can be purchased separately but are also bundled with XenApp Premium Edition

Access Gateway 9.3 Enterprise Edition

Access Gateway 9.3 Enterprise Edition is very commonly deployed and probably represents many of the enterprise class installations of Access Gateway, more so than version 10 as that is so very new. There were no new features in version 9.3 over those included in the predecessor, Access Gateway 9.2 EE; the enhancements in 9.3 relate more to security.

Access Gateway 9.2 Enterprise Edition

Access Gateway 9.2 Enterprise Edition offers the following benefits:

- Secure remote access for the most demanding and complex environments that require increased scalability and performance
- High availability for guaranteed access to resources and compliance with SLAs
- Highest level of integration and control of remotely delivered Citrix XenApp applications, data through SmartAccess, (endpoint analysis), and published desktops with Citrix XenDesktop
- Natural progression for existing XenApp customers who have used the Secure Gateway and wish to benefit from the added security and full VPN access
- Enterprise-class SSL VPN features, including client-side cache clean-up, detailed auditing, and policy-based access control for web and server applications
- Ability for remote users to work with files on shared network drives, access e-mail and intranet sites, and run applications as if they are working within your organization's firewall

- Support for the Access Gateway universal license; these licenses enable SmartAccess and can be purchased separately but are also bundled with XenApp Premium Edition

> Access Gateway 9.2 and 9.3 do not provide support for ICA Multi-stream. ICA Multi-stream is supported in Access Gateway 10, 5.03, and 5.04.

Earlier versions of Access Gateway Enterprise Edition exist, but these versions are enough to cater for what you will encounter in the current market.

Access Gateway 5.x

The Citrix Access Gateway can be used on NetScaler Model 2010 and the VPX Edition. The Gateway has two modes of operation, Standalone and Controller. Access Controller is an additional piece of software that is installed onto Windows Server 2008 R2 to allow access policies to be defined from within the standard XenApp Group Policies filters. The focus of this book is on Access Gateway in Standalone mode. The key features of Citrix Access Gateway are as follows:

- Authentication of users against LDAP directories or RADIUS
- Termination point for encrypted sessions
- Authorization of users to access resources
- Secure VPN through traffic relay for authorized users
- Support for multiple logon points that can allow for basic or SmartAccess endpoint analysis

Citrix Access Gateway VPX Edition

The purpose of this book is to specifically help you understand and deploy the VPX edition of Access Gateway. As organizations have increased their use of remote access solutions, Citrix has had to cater to that need with a diverse offering of systems. These solutions need to provide the same flexibility as the customer base is diverse. Access Gateway VPX is a virtual appliance delivering the same features and functionality as the Model 2010 physical appliance. Customers will find that Access Gateway VPX is ideal for:

- Natural progression for existing XenApp customers, who have used the Secure Gateway and wish to benefit from the added security and full VPN access. Access Gateway VPX supports Citrix Receiver and XenDesktop whereas Citrix Secure Gateway does not.

- Consolidation of physical resources where rack space may be limited.
- Meeting the needs of green IT by reducing cooling needs and power consumption within the data center.
- Minimizing downtime by utilizing the HA infrastructure that is already maintained with your virtual machine hosts, maximizing the investment that you have with Citrix XenServer or VMware.
- Multi-tenant solutions with the availability of multiple logon points.

In simple terms, the virtual appliance is an easy choice for organizations that already implement a virtual machine infrastructure. The high availability that is not provided in the VPX is maintained by XenServer or VMware. Performance can be optimized by assigning more RAM or VCPUs (virtual processors) to the Access Gateway virtual machine. Citrix suggests a maximum of 500 concurrent users on each virtual appliance.

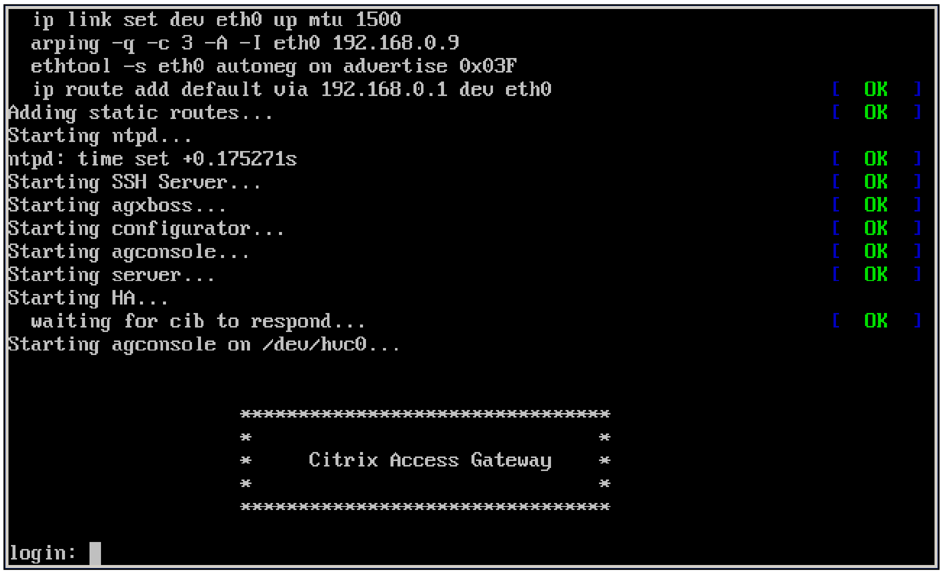
> The Citrix Access Gateway VPX Express is free but is limited to just five concurrent users.

The VPX is downloaded from the Citrix website. If you do not already have a MyCitrix login, you will be required to register for an account.

Virtual machine resources required by the Access Gateway VPX are as follows:

XenServer version	5.5 or Higher
VMware version	ESX/ESXi 4.0 or higher
Memory	1 to 4 GB RAM
Concurrent users	500
VCPU	1 to 4 VCPUs (2 recommended)
Virtual NICS	1 to 4 NICS
Disk space	12 GB minimum

The following screenshot shows the console screen from Citrix Access Gateway while running on XenServer:



```
  ip link set dev eth0 up mtu 1500
  arping -q -c 3 -A -I eth0 192.168.0.9
  ethtool -s eth0 autoneg on advertise 0x03F
  ip route add default via 192.168.0.1 dev eth0                 [  OK  ]
Adding static routes...                                         [  OK  ]
Starting ntpd...
ntpd: time set +0.175271s                                       [  OK  ]
Starting SSH Server...                                          [  OK  ]
Starting agxboss...                                             [  OK  ]
Starting configurator...                                        [  OK  ]
Starting agconsole...                                           [  OK  ]
Starting server...                                              [  OK  ]
Starting HA...
  waiting for cib to respond...                                 [  OK  ]
Starting agconsole on /dev/hvc0...


                    ********************************
                    *                              *
                    *     Citrix Access Gateway    *
                    *                              *
                    ********************************

login: 
```

Designing a secure Remote Access solution

So, now we understand a little of what the CAG models can provide for us and are clear that we can use hardware or virtual appliances. At this point, we can take the opportunity to review the security solutions provided with CAG and how to design a secure deployment.

Availability

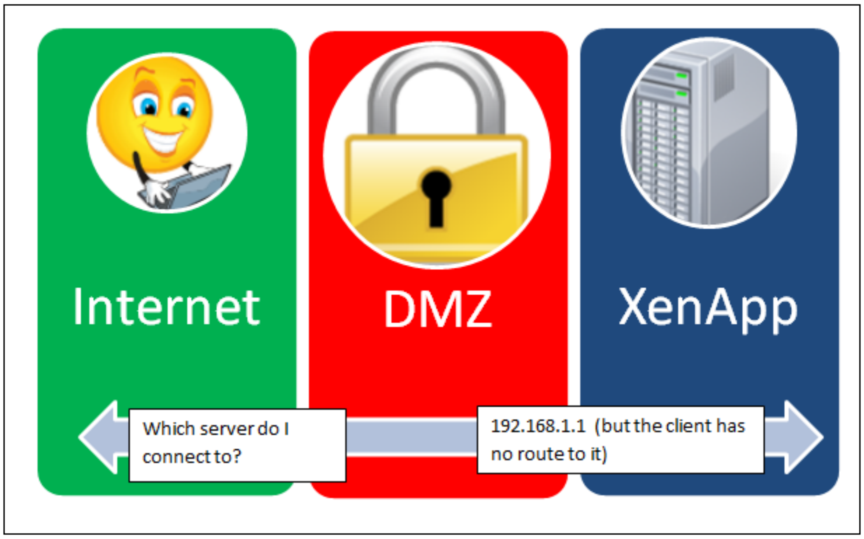
How many users do you need to support concurrently?

Part of a secure solution will be making sure the system maintains its presence. Partly, that involves not overloading the system. CAG maintains all incoming connections and passes all VPN traffic into and out of your LAN. Each Model 2010 appliance and VPX can support 500 users, the MPX can support 5500 users, and a massive can support 5000 users. If you're using the VPX, make sure you have enough appliances deployed and load-balanced.

Using ICA Proxy to access XenApp/ XenDesktop

When connecting from the Internet, your remote users are going to connect into your server farms and request a published application from XenApp or a virtual desktop from XenDesktop. The corresponding ICA file that is returned to the client will contain the IP address of the server that will accept the connection. This is usually a private IP Address and the client will have no route to the network.

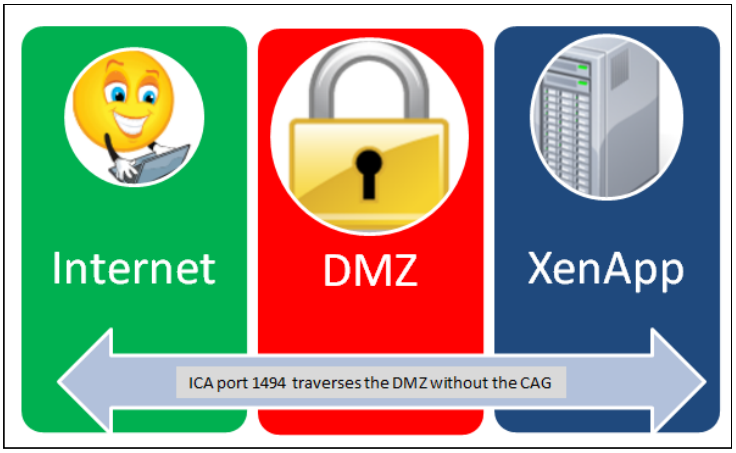
If remote users are presented with the internal address of the hosted applications or desktops, they will not be able to connect. Thus the need for ICA proxy.


Internet
DMZ
XenApp
Which server do I connect to?
192.168.1.1 (but the client has no route to it)

Ensuring there is no path for a single protocol to traverse the DMZ

From a security perspective, your network will be more secure if we can ensure that no single protocol can traverse from the external firewall of your DMS into the internal network hosting your private resources. Implementing an ICA proxy on CAG will allow users to connect via HTTPS to the gateway, and the Gateway to forward the connection into the private network using ICA.

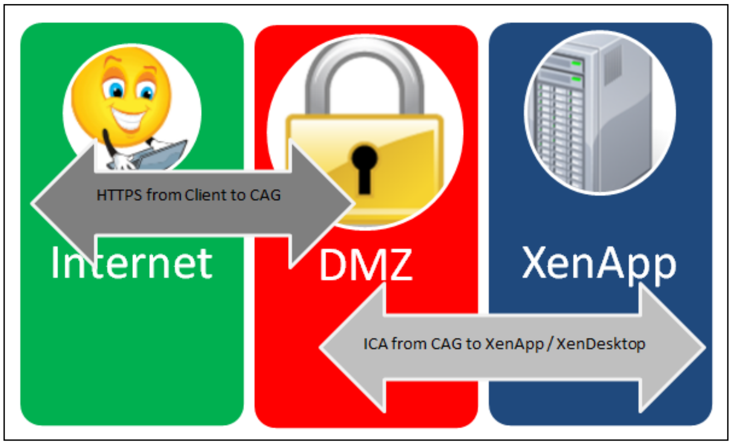
Without the Access Gateway ICA, traffic is unchallenged in the DMZ.



Resolving remote access issues using Citrix Access Gateway

In its simplest form, Access Gateway will proxy incoming requests— in this case, for ICA connections to XenApp/XenDesktop. As the client only ever connects to CAG, ICA traffic need not be allowed through the exterior firewall. Additionally, as the client never connects directly to the XenApp servers, they do not need public addresses and need only to be routable to CAG.

The following diagram shows that the client connects using HTTPS from their client to CAG within the DMZ and CAG connects using ICA to the internal resources of XenApp/XenDesktop:



If you need access to other resources, we have full VPN connections

CAG can additionally provide similar VPN access via SSL and to your internal resources using SmartAccess logon points. Multiple logon points can exist on single CAG to provide flexible access.

Authentication

To allow for secure remote access, authentication of your users should take place within the DMZ. In this way, users are authenticated without the need to connect them to internal resources. CAG addresses these issues by authenticating any user request before they are connected. In addition, your existing directory infrastructure can be used as the authentication source. CAG can connect with Microsoft Active Directory and Novell eDirectory as well as **Remote Authentication and Dial-In User Service** (**RADIUS**) and other LDAP providers.

PKI Certificates

The communication from the client to CAG is secured with SSL. When planning for your CAG deployment, you will need to consider the provision of **public-key infrastructure** (**PKI**) certificates for the appliance. The public key from the issuing authority and the server's own key pair must be added to the device.

Summary

In this chapter, we have become familiar with the CAG range and considered which model we require and how many appliances we will need to support our projected concurrent user load. We should also now be able to envision how the gateway will provide remote access solutions to both ICA-based resources, such as XenApp and traditional VPN access to file shares, reducing your reliance on multiple remote access products.

In the next chapter we will be looking at the licensing requirements for CAG and how we can cater to these.

2

Licensing the Citrix Access Gateway

Just contain your excitement for a little more time; we are not quite ready to install CAG. There is still a little infrastructural planning to complete in relation to correct licensing; yes, unfortunately, you are going to need licenses! The good news is that there is a free license for Access Gateway Express VPX, while other licenses may be bundled with your existing Citrix purchases. In this chapter we are going to get familiar with the licensing options for the Access Gateway VPX and install License Server.

- Overview of licensing CAG
- License Server options
- Obtaining licenses
- Deploying Microsoft Windows Server and VPX License Servers
- Importing licenses
- License Server Administration

Overview of licensing CAG

Once you have downloaded your CAG virtual machine, you will need a license to use it, and this includes the Citrix Access Gateway Express (free edition).

> All editions of CAG require licenses, including the VPX Express, VPX Access Gateway 5, Access Gateway 5 (NetScaler 2010), and Access Gateway 9 and 10 running on NetScaler MPX 5500.

As with all projects, the more the planning at the outset, the fewer the surprises we will encounter during the deployment. There are two license types for the CAG:

- Platform
- Universal

Either one, or both, of these licenses would normally be imported to License Server but can also be accessed directly from the CAG. This, however, would limit the use of licenses to just that single CAG. In many circumstances, License Server would already be implemented as other Citrix products, including XenServer, a possible VPX host, need Citrix licenses. For completeness, we will cover the licensing and the latest License Server version in this book.

License Grace Period

Initially, you have a 96-hour grace period after the gateway has started to add licenses. During this period, the CAG is issued a platform license and two universal licenses. After the first 96 hours, these licenses are revoked and an unlicensed CAG will not operate; other than allowing access to the management console. Once the CAG has connected with License Server that has valid CAG licenses, License Server can be unavailable for a maximum period of 30 days. Once contact is regained to License Server, this 30-day timer is reset. With this in mind, availability of License Server does not need to be placed high upon your agenda.

Platform License

Each concurrently running CAG requires a valid platform license. The licenses can be installed on the CAG or on a separate License Server. A platform license enables users to make connections through **basic logon points** and is only directed to the Citrix Web Interface Server. Users may log on using Citrix online plug-ins by means of their web browser or the Citrix Receiver. Basic logon points allow connections to XenApp servers to retrieve applications or to XenDesktop controllers to retrieve virtual desktops.

When you install the platform license, Access Gateway VPX allows the following types of connections:

- Connection from the user's web browser to a Citrix Web Interface site
- ICA and **Secure Sockets Layer** (**SSL**) connections to XenApp or XenDesktop initiated by Citrix online plug-ins

The platform license supports the following connection features:

- Authentication on the CAG or at the Citrix Web Interface
- Integration with Citrix Web Interface to broker connections to XenApp or XenDesktop
- Secure SSL relay of ICA session traffic

Universal License

Access Gateway Universal user licenses enable **SmartAccess logon points**:

- Full network-layer VPN tunnelling
- Endpoint analysis

When you install a universal license, users log on using the CAG plug-in, which can be deployed via the CAG or by other methods that suit your software distribution model.

Universal licenses are used for concurrent sessions in which users access SmartAccess logon points that enable access to internal resources other than XenApp or XenDesktop and can include endpoint analysis to determine the appropriate level of access for that session.

Concurrent connections

The platform license allows basic connections up to the maximum capacity of the appliance, five in the case of the Express Edition and 500 in the case of the full VPX version.

The universal license allows SmartAccess connections up to the number of purchased licenses; Universal licenses also are bundled within the Platinum editions of XenApp and XenDesktop. With careful planning on your initial product purchase, large savings may be made with effective licensing options.

Citrix Access Gateway Express

This is a free edition of the CAG; however, although free, it is still required to be licensed. The license is an expiring license that is valid for a single year, effectively making this a one-year trial version.

This edition allows for some testing and proofing of the concept of your deployment. The limitation of five connections does effectively limit a full pilot, though. If you have been using the Express license, you can later add a platform (and universal licenses if required) later without losing any of your gateway configuration.

The following table summarizes the licenses available for the CAG:

License Types	Smart Access Logon Points	Basic Logon Points
First 96-hours grace period	Two sessions	
Expired grace period	Disallow	
Platform license only	Disallow	500
Platform and universal	Allow up to concurrent purchased user count	500
Express license	Five sessions for one year only	

From 5.04 onwards, the initial grace period has increased from 48 to 96 hours, while in previous versions, this was limited to 48 hours.

License Server options

All versions of the CAG require licenses. These licenses can be retrieved locally from the CAG. Perhaps, for very small deployments, this may be an option; however, it would be more standard to deploy Citrix License Server. This may be by means of an MSI installer onto Windows Server or utilizing the License Server VPX downloaded from Citrix (`http://citrix.com/downloads/licensing.html`). Using either method, the License Server software is free to use. Once deployed, License Server can provide licenses across the complete range of Citrix products that you utilize. Licenses are imported into License Server as they are purchased and required. Citrix recommend that a single server can provide licenses for a maximum of 200 product servers.

Using EdgeSight from Citrix, you can monitor historical license usage to ensure you have correct license numbers to support logon peak times. For more information on monitoring your systems with Citrix Edgesight, visit the Citrix eDOCS site at `http://support.citrix.com/proddocs/topic/technologies/edgesight-wrapper.html`.

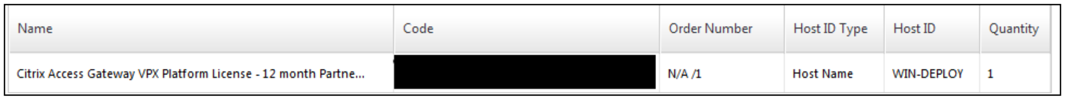
The MSI installer for the License Server software is provided on many of the product DVDs, such as XenApp and XenDesktop. Alternatively, you can download the latest version from the Citrix website, `http://citrix.com/downloads/licensing.html`. The latest version will work with all products, but if you are using an earlier version, you will need to check that it is compatible with the version of the CAG you are using or other Citrix products you wish to use.

> Best practice is to keep License Server version up-to-date so that it will work with the latest updates of the CAG and other Citrix products.

Obtaining licenses

Licenses from Citrix products are downloaded from the MyCitrix website, `https://www.citrix.com/English/mycitrix`. You allocate your purchased licenses to License Server. If you are working in an organisation, they will add you as a license administrator and your personal ID will be able to download and manage corporate licenses. The hostname of License Server is case sensitive and you have to assign the licenses to the correct name and correct case of your server.

Note that the host ID is case sensitive and matches the hostname of License Server.



Name	Code	Order Number	Host ID Type	Host ID	Quantity
Citrix Access Gateway VPX Platform License - 12 month Partne...	[redacted]	N/A /1	Host Name	WIN-DEPLOY	1

The license is then downloaded and will need to be imported into License Server or CAG. If using the CAG as License Server, the CAG name must be in the **HOST ID** field.

Deploying Microsoft Windows Server and VPX License Server

License Server can be installed on Windows, which we will look at first or installed as a virtual appliance in your virtual infrastructure servers, which we will look at later. It does not matter which type you use; I use the virtual appliance in the book.

Installing License Server 11.10

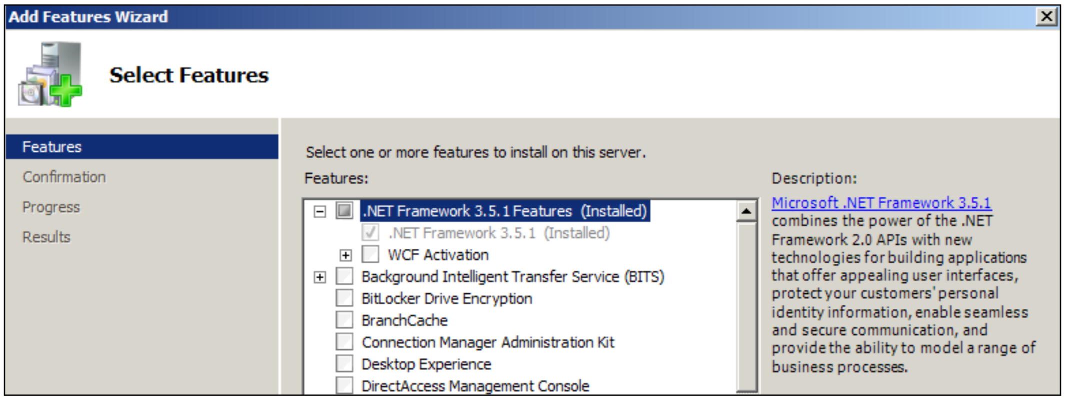
Citrix License Server can be installed on to the following Windows Platforms:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows 7

50 MB of free disk space is required for the installation; you may read from this that, in itself, License Server does not require many resources to run.

Windows .NET 3.5 Framework is required to be installed prior to License Server. If you are using Server 2008 R2 or Windows 7, .NET 3.5 can be added directly from the OS as a feature.

.NET 3.5.x is a Server 2008 R2 and a Windows 7 feature and can be installed easily using the **Programs and Features** tool in Control Panel.



Add Features Wizard

Select Features

Features
Confirmation
Progress
Results

Select one or more features to install on this server.

Features:

- ▣ .NET Framework 3.5.1 Features (Installed)
  - ☑ .NET Framework 3.5.1 (Installed)
  - □ WCF Activation
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BranchCache
- □ Connection Manager Administration Kit
- □ Desktop Experience
- □ DirectAccess Management Console

Description:

Microsoft .NET Framework 3.5.1 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

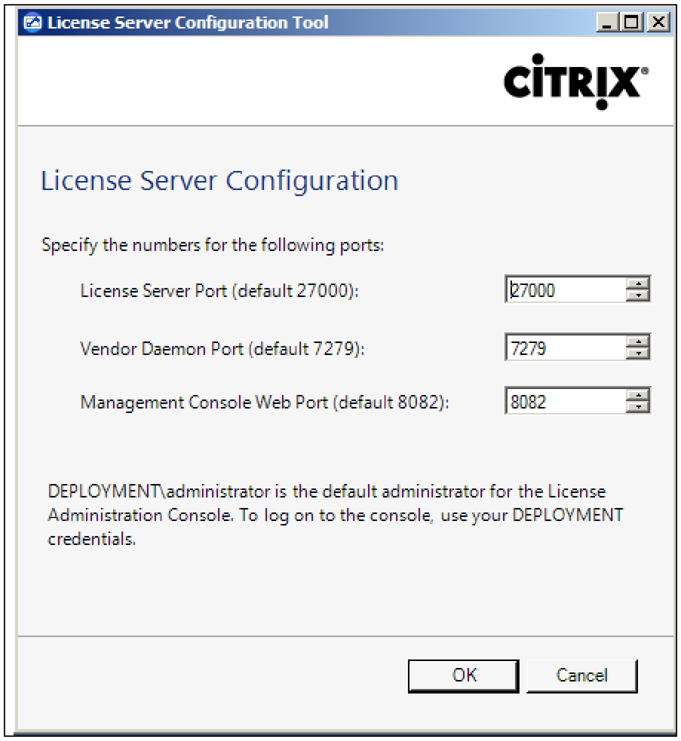
With .NET installed, you can install Citrix License Server. The current version as of this writing is 11.10.

> With Version 11.10 installed onto a Windows domain-joined server, you have the added benefit of being able to use domain accounts as License Server administrators.

To begin the installation, double-click on the License Server installation file, **CTX_Licensing.msi**. Once the system checks have completed, you will be prompted to accept the End User License Agreement. Click on **Accept** and continue the installation, and you soon will be prompted for the installation directory. On 64-bit systems, this defaults to `c:\Program Files (x86)\Citrix`.

Choose **Install** to continue. This is not a large install. Remember, just 50 MB of free disk space is required. Soon, you will be presented with the configuration pane.

With Version 11.10, the currently logged-in Windows user becomes the license administrator. In the following screenshot, we see that the account **DEPLOYMENT\Administrator** has been added as the server admin.



License Server Configuration

Specify the numbers for the following ports:

License Server Port (default 27000): 27000

Vendor Daemon Port (default 7279): 7279

Management Console Web Port (default 8082): 8082

DEPLOYMENT\administrator is the default administrator for the License Administration Console. To log on to the console, use your DEPLOYMENT credentials.

On a server that is not domain-joined, you would have to add a local administration account to manage License Server. Here though, we see that the current user has been added in as the license administrator. Additionally, as you can see, the default ports are listed on this screen. Upon CAG start-up, License Server will be polled on port **27000**. Platform and universal licenses are checked out as required on port **7279**. Port **8082** is used by License Management Console, which is a web-based interface.

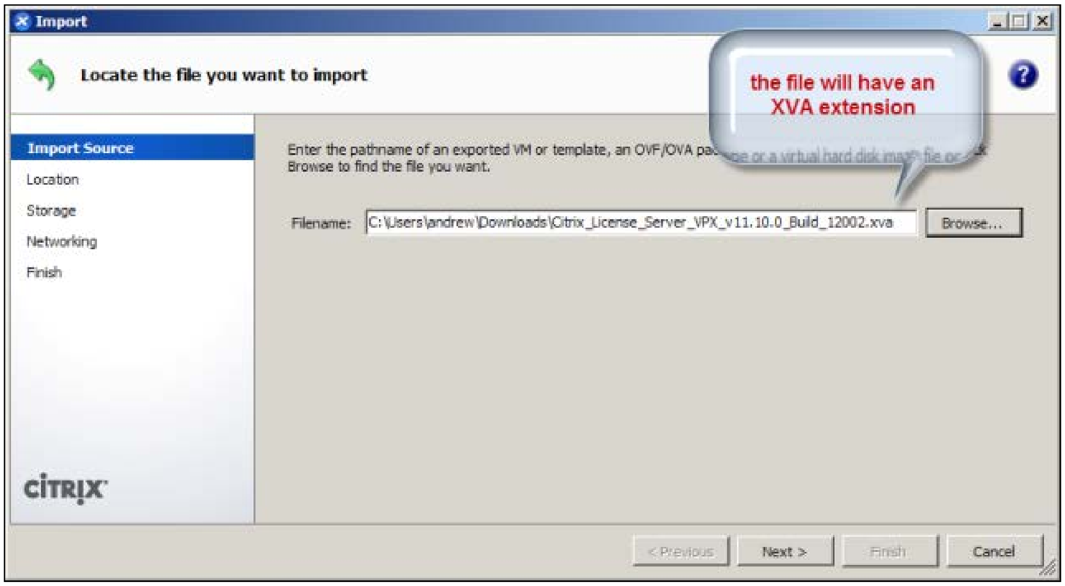
Importing License Server VPX into Citrix XenServer

With this method (importing License Server into Citrix XenServer), the License Server software is supplied along with the operating system in a virtual machine optimized for VMW are ESX or Citrix XenServer. This does save you one of your Windows Servers and possibly an additional Windows license if the server would be dedicated to this role. The only downside of this is that you lose the ability to manage License Server with a domain account as only local accounts are used on License Server. Using domain accounts is new to Version 11.10 of License Server and is only available on domain-joined Windows Servers.

Using the VPX edition of CAG will require a virtual machine infrastructure to host CAG or CAGs, so this makes it an obvious choice as License Server in our environment. The VPX is a free download from Citrix and is quite resource-friendly in as much as it needs just 256 MB of RAM and 8 GB of disk space to run in a VMware or XenServer environment.

Once downloaded using XenCenter, we can import the VPX appliance into our XenServer environment. From XenCenter, choose **File** | **Import**.

Importing the Citrix License Server VPX from XenCenter is shown in the following screenshot:



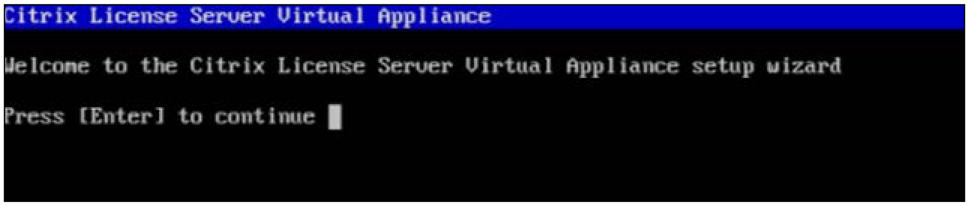
Enter the pathname of an exported VM or template, an OVF/OVA pa... ge or a virtual hard disk ima... file or ...k Browse to find the file you want.

Filename: C:\Users\andrew\Downloads\Citrix_License_Server_VPX_v11.10.0_Build_12002.xva

As the wizard continues, you will need to choose **Home Server** from the location page of the wizard. This is the server that the appliance should start on. We will then need to select the disk storage repository to use, and finally, the network to connect to. License Server by default will start after the import and will be labeled **Citrix License Server Virtual Appliance**. This is just a label in XenServer and not the name of the host, which will be named from the License Server command-line wizard.

Once started, we will need to connect to the virtual machine console in XenCenter to finalize the import.

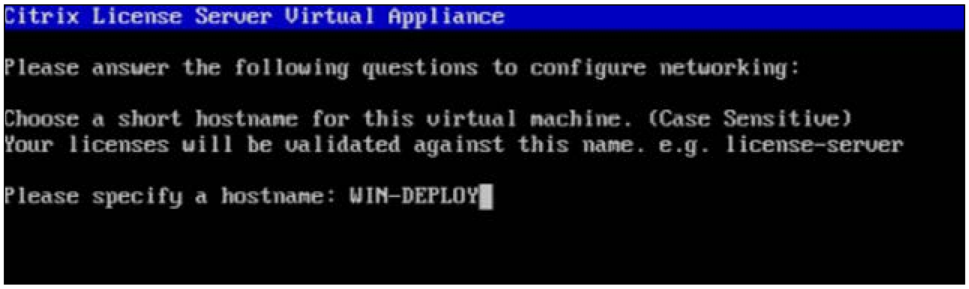
Accessing the virtual appliance console in XenCenter console will allow you to access the setup wizard for Citrix License Server.



```
Citrix License Server Virtual Appliance

Welcome to the Citrix License Server Virtual Appliance setup wizard

Press [Enter] to continue
```

To proceed with the configuration, we can use the *Enter* key from the console. First, we are prompted for the root user password. We create this secure password and enter it twice to validate our typing skills. Then, we are prompted for the License Server hostname. This is very important as this is the name that we issue licenses to. Previously, we assigned the CAG license to **WIN-DEPLOY** in uppercase, so we will name this License Server `WIN-DEPLOY`.

The License Server name is used when assigning licenses and is case sensitive; make sure the name of the server that we configure matches the name we issued the licenses to.

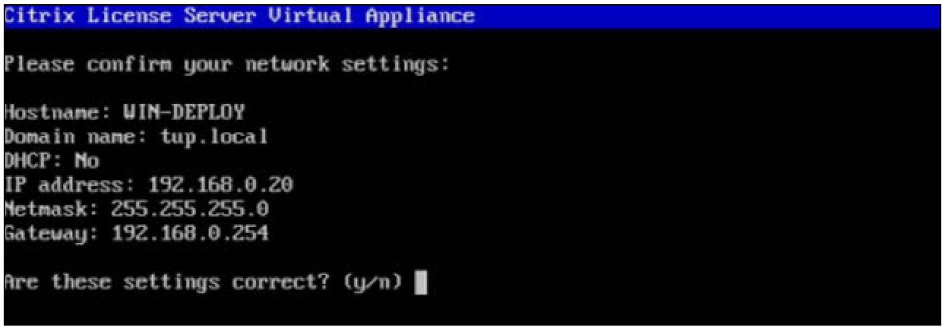


```
Citrix License Server Virtual Appliance

Please answer the following questions to configure networking:

Choose a short hostname for this virtual machine. (Case Sensitive)
Your licenses will be validated against this name. e.g. license-server

Please specify a hostname: WIN-DEPLOY
```

As the wizard continues, we are prompted for:

- Domain name
- IP configuration

Finalize the settings by confirming with the letter `y`.



```
Citrix License Server Virtual Appliance

Please confirm your network settings:

Hostname: WIN-DEPLOY
Domain name: tup.local
DHCP: No
IP address: 192.168.0.20
Netmask: 255.255.255.0
Gateway: 192.168.0.254

Are these settings correct? (y/n) █
```

On confirming the settings, the final stage is to configure the license administrator, unlike the Windows version, in which we do not integrate with Active Directory and use a local account called admin. The password should be different from the root user account. The admin account is used to access the web console, which you access via `http://<yourserver.yourdomain>:8082`.

If we ever need to change the configuration, we can run a script called `/usr/local/bin/resetsettings.sh`.

This script is in the `PATH` statement, so just typing `resetsettings.sh` at the command prompt is all that needs to be done. This script does reset the configuration, but if licenses have been imported, these are retained on the server.

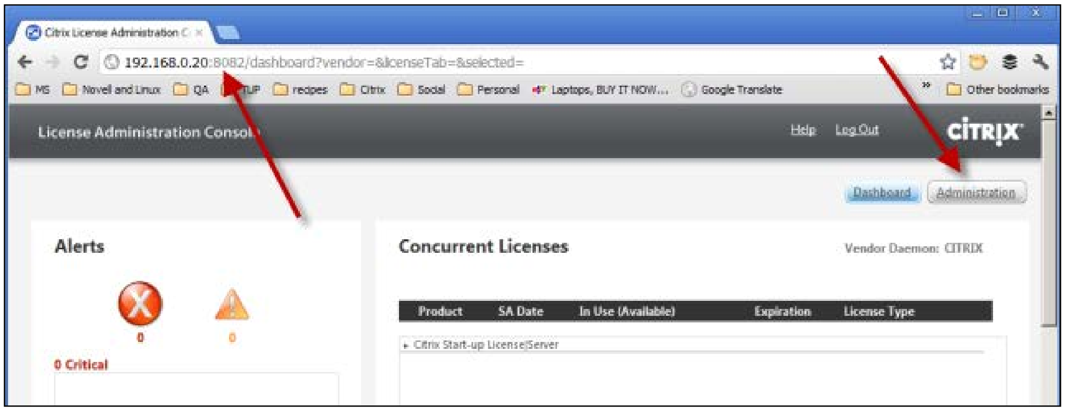
Importing licenses and management

As we have now completed the initial setup of either the Windows or VPX version of the License Server, we can import the Citrix licenses to it. This is managed through the web-based console of License Server listening on port **8082**, by default. Citrix supports the following browsers to manage License Server 11.10:

- Internet Explorer Version 6.0 to Version 9.0 (use IE 8 and 9 in compatibility mode)
- Mozilla Firefox 3.0 – 8.0
- Chrome 12.0 – 15.0
- Safari 5.1

As always, other browsers may work, but these are supported and known to work.

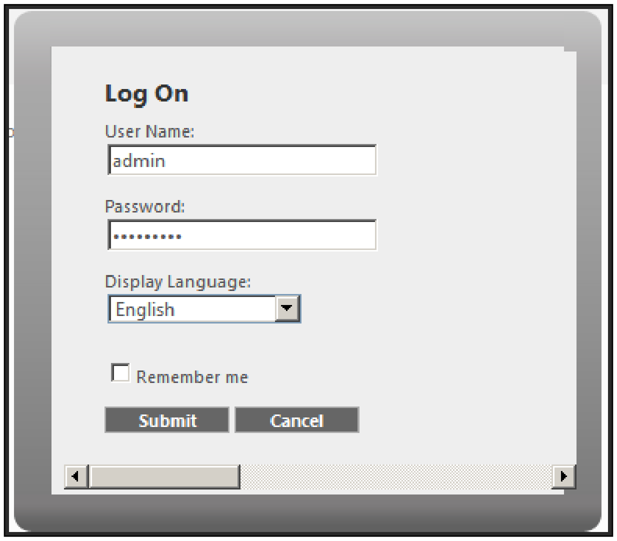
The following is a screenshot of License Server console:



192.168.0.20:8082/dashboard?vendor=&licenseTab=&selected=

Product	SA Date	In Use (Available)	Expiration	License Type
Citrix Start-up License Server				

From the web page, you can see that port **8082** is used to access the server and the administration button is used to log on with administrative credentials. Here, we are using the VPX version, so will use the `admin` account. The following is a screenshot of the administration console login:



Log On

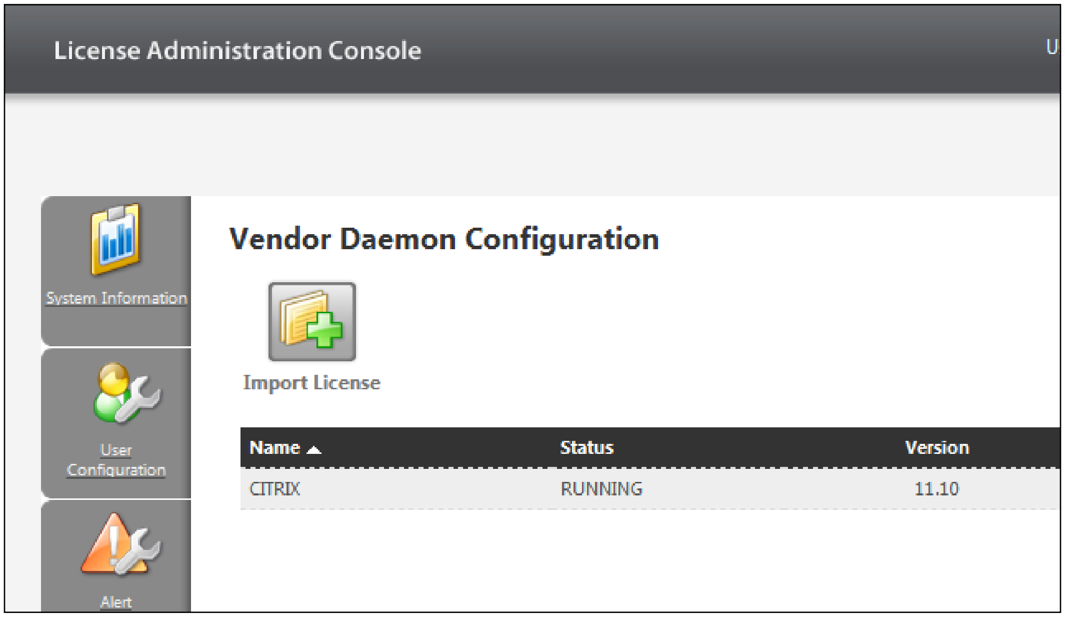
User Name: admin

Password: •••••••••

Display Language: English

□ Remember me

To import the license, we click on the **Vendor Daemon Configuration** button on the left-hand side of the **Administration System Information** page. From here, we should not miss the big **Import License** button. The following is a screenshot of the **Vendor Daemon Configuration** window:



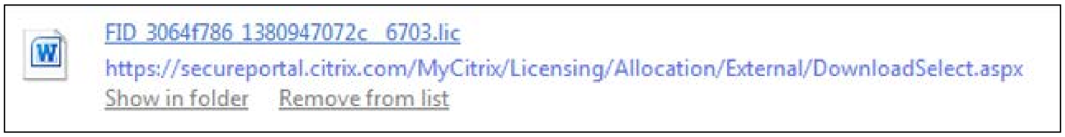
Vendor Daemon Configuration

Name ▲	Status	Version
CITRIX	RUNNING	11.10

Using the **Import License** button, we can then browse through to where we have saved the license and upload it to the server. The license is now stored on the server and is available to CAGs that connect to the server.

> Note that we should keep the originals as backups, and renaming the file makes sense as it will then be easier to manage them in the backup file system.

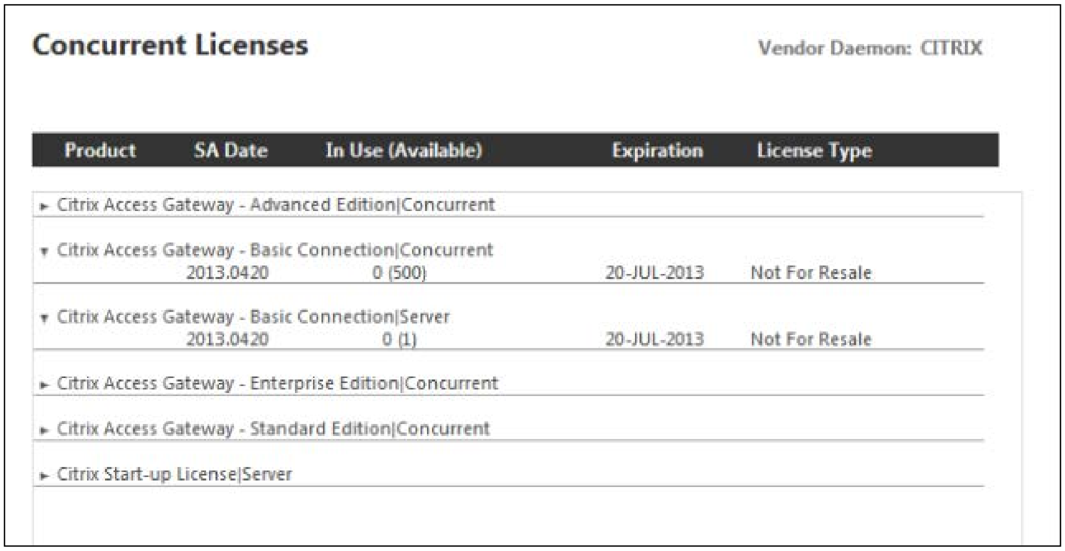
Downloaded licenses have obscure names; rename them to simplify your backup and ensure that you can identify them later.



FID_3064f786_1380947072c__6703.lic
https://secureportal.citrix.com/MyCitrix/Licensing/Allocation/External/DownloadSelect.aspx

Once the license is imported, License Server will require a reboot. Upon restarting, we would advise you to check the availability of the license from the dashboard on the License Server console. By default, you do not need to log in to see this, but this behavior can be adjusted in **Server Configuration**.

The dashboard of License Server shows one Platform License and 500 basic connections available with the CAG VPX 5.



Concurrent Licenses

Vendor Daemon: CITRIX

Product	SA Date	In Use (Available)	Expiration	License Type
▸ Citrix Access Gateway - Advanced Edition|Concurrent				
▾ Citrix Access Gateway - Basic Connection|Concurrent	2013.0420	0 (500)	20-JUL-2013	Not For Resale
▾ Citrix Access Gateway - Basic Connection|Server	2013.0420	0 (1)	20-JUL-2013	Not For Resale
▸ Citrix Access Gateway - Enterprise Edition|Concurrent				
▸ Citrix Access Gateway - Standard Edition|Concurrent				
▸ Citrix Start-up License|Server				

We have added just the CAG VPX platform license, which supports one concurrently running CAG with a maximum of 500 connections to basic logon points. The dashboard confirms this. As this is new License Server, we have no other product licenses. We do not have universal licenses or SmartAccess licenses to support full VPN access; initially, we will continue with just the platform license and move on to add universal licenses later.

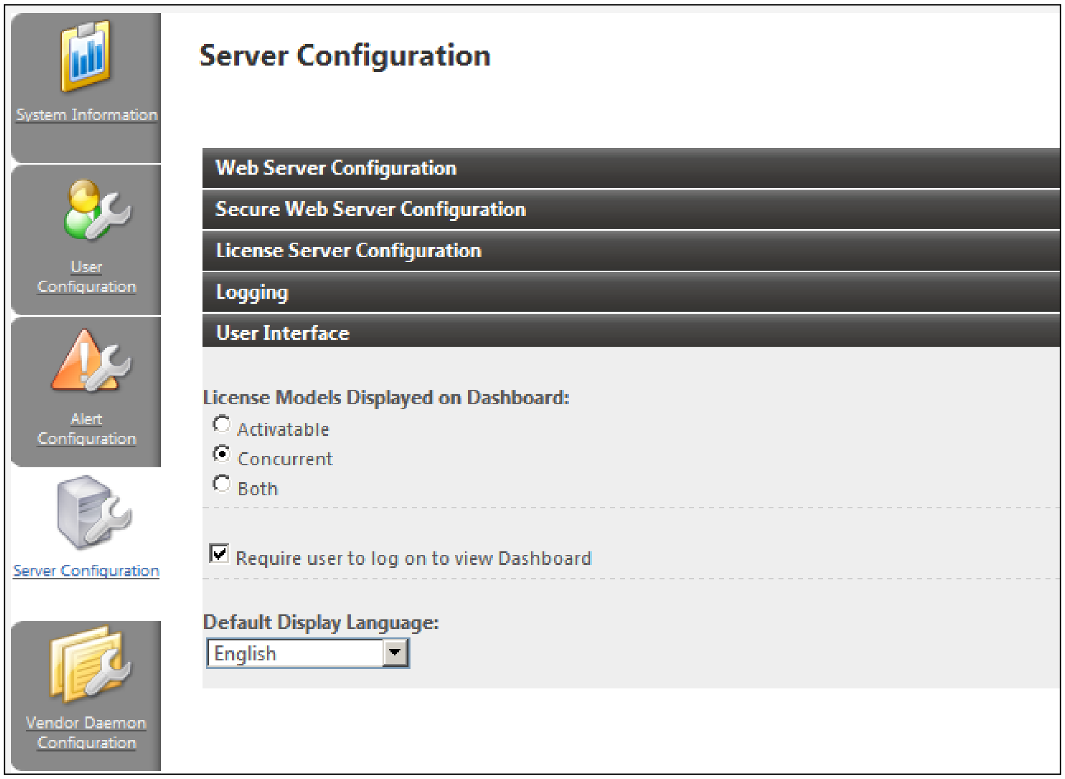
License Server Administration

Having licenses on License Server is one thing, but adequately managing the server is something else entirely. There is not much additional management to do; after all, License Server is quite simple. However, I would suggest securing the dashboard and using HTTPS to access the server.

Securing the dashboard

As we have seen from accessing the License Server console, we are not required to authenticate when accessing the dashboard (the first page on the web console); we are only prompted for credentials when we choose **Administration**. Potentially, access to the dashboard exposes information about the products that you have in use and how many users access these resources.

You may choose to require authentication when connecting to the dashboard, as shown in the following screenshot:



Server Configuration

License Models Displayed on Dashboard:

○ Activatable
● Concurrent
○ Both

☑ Require user to log on to view Dashboard

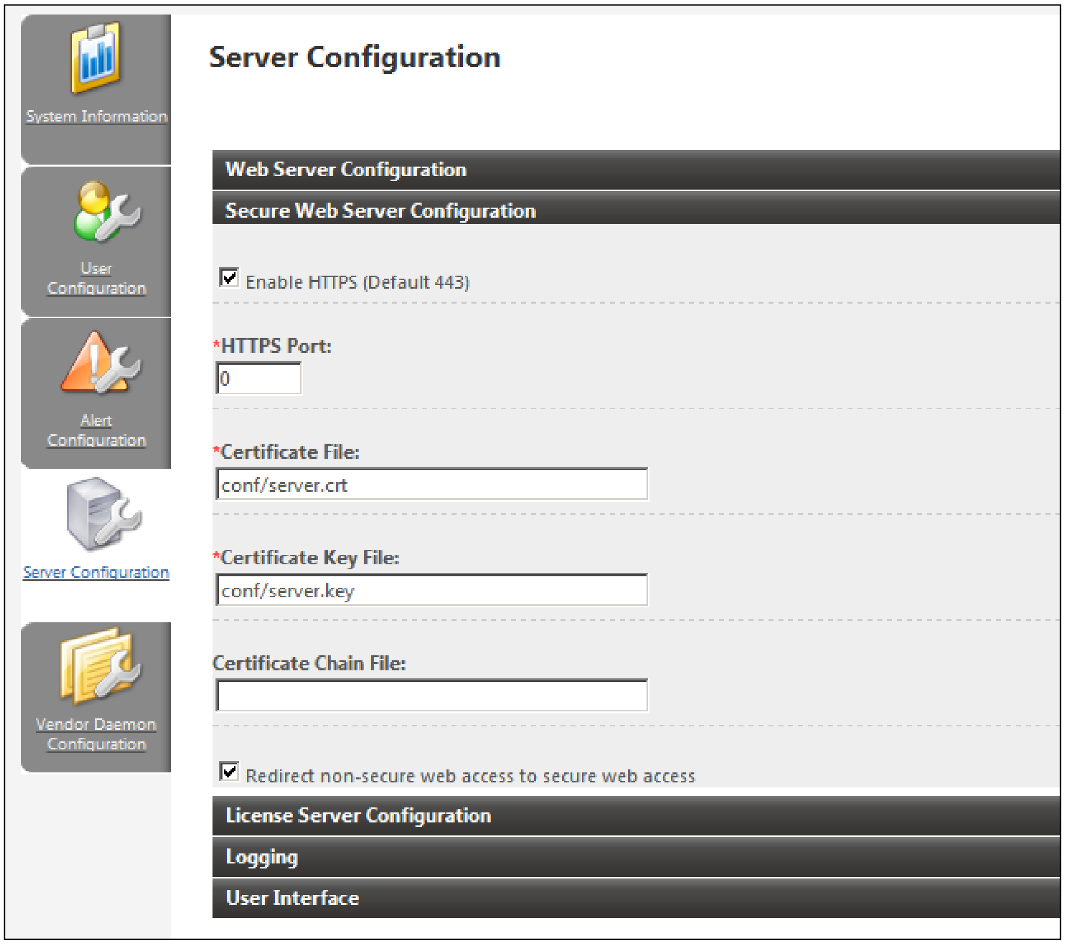
Default Display Language:

English

This can be set from the **Administration** console, choosing **Server Configuration** | **User Interface** | **Require user to log on the view Dashboard**.

Securing License Server with HTTPS

Especially if you integrate your License Server administrators with Active Directory accounts, you probably will want to ensure that HTTPS is used to fully encrypt user logon on the console. The configuration can be made by navigating **Server Configuration | User Interface | Secure Web Server Communication**.



☑ Enable HTTPS (Default 443)

*HTTPS Port: 0

*Certificate File: conf/server.crt

*Certificate Key File: conf/server.key

Certificate Chain File:

☑ Redirect non-secure web access to secure web access

The paths to the certificate file are `conf/server.crt` and `conf/server.key`.

The full path would relate to:

- Linux: `/opt/citrix/licensing/LS/conf`
- Windows: `%PROGRAMFILES%\citrix\licensing\LS\conf`

Just add your own certificates and the trusted root public key into this directory and adjust the filenames to match those that you have added. If you are unfamiliar with generating SSL certificates, the simple choice is not to use SSL. If you are familiar with PKI and SSL certificates, the mechanism that you currently use to generate certificates will be just fine for License Server. If you are using Active Directory, a certificate server is provided as a role service that you can add. When we come to install and configure CAG, a little more detail is given on creating certificates.

Summary

In this chapter, we have become familiar with the CAG range and have begun to make plans with regards to which model we require and how many appliances we will need to support our projected concurrent user load. We should also now be able to envision how the gateway will provide remote access solutions to both ICA-based resources, XenApp and traditional VPN access to file shares, reducing your reliance on multiple remote access products.

In the next chapter we will be looking at the licensing requirements for CAG and how we can cater for these.

3
The Citrix Access Gateway Initial Setup

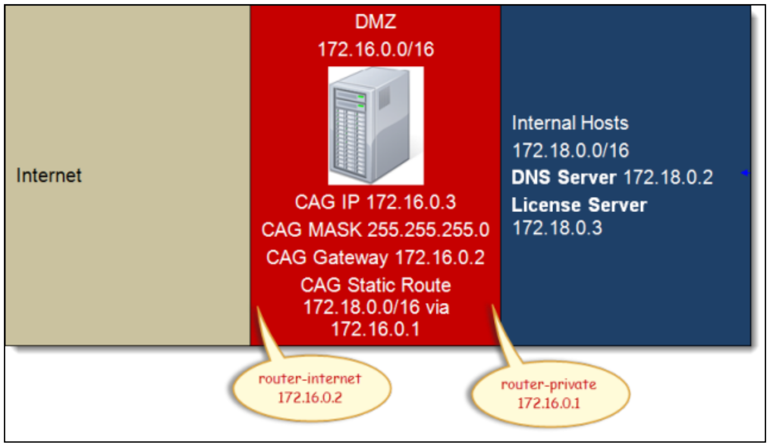
Now we are able to look forward, in this chapter, to using CAG, as we are licensed and ready to download and import the Access Gateway VPX into our virtualization environment. By the end of the module, we will have a working gateway ready and awaiting logon points. So, of course, this will include us having to download and run the initial configuration of CAG, which includes setting its IP address and adding PKI certificates. CAG only works with incoming HTTPS connections. In more detail, this setup includes:

- Understanding the network architecture
- Downloading the VPX import file
- Importing into VMWare ESX/Citrix XenServer
- Initializing the setup from the command line
- Completing the initial configuration from the web portal
- Adding SSL certificates
- Monitoring CAG

Understanding the network architecture

Firstly, we should know the network segment on which we are to attach CAG. There is always the curse of the Internet and its hidden threats, but it is totally necessary; we want to keep this traffic away from our internal hosts, protecting them from malicious intent. CAG will act as an intermediary between the Internet and internal hosts and, as such, should be placed in a secured subnet or DMZ. CAG will act as our gatekeeper and validate any external visitors to the precious resources within the corporate network.

The following table illustrates the network topology used throughout the book:



The external router facing the Internet (router Internet) is not configured with a route into the private internal network, `172.18.0.0/16`. This should always be the case as external hosts are prevented from talking directly to your internal servers, unless it is by way of the VPN or ICA proxy created on CAG. CAG is configured with its default route facing hosts on the Internet. This makes absolute sense as it is easy to define routes to your own network, but not to all hosts on the Internet. A static route to the internal network is added to CAG using the router-private gateway. Internals hosts have their default gateway directed to the router private, so that they can access hosts in the DMZ but have no route into the Internet.

When planning CAG deployment, your XenServer or VMware hosts have to be able to present a network structure similar to the earlier structure.

Downloading the virtual appliance from Citrix

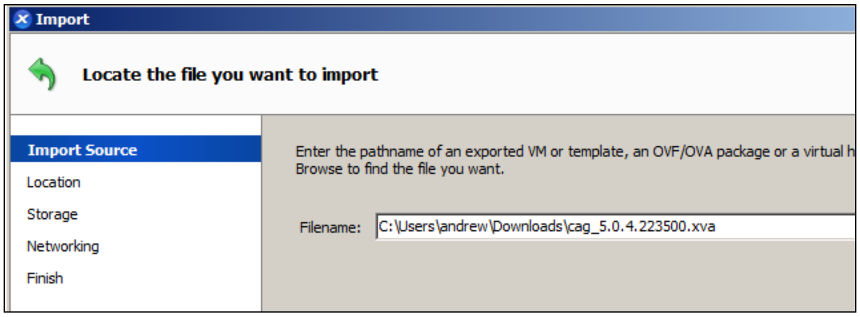
The VPX edition of CAG can be downloaded as a trial version from the Citrix site, `http://citrix.com/downloads/netscaler-access-gateway/product-software/access-gateway-504.html`. You can run the gateway without a license for up to 96 hours; however, if you wish to test further before your purchase, a 90-day trial license can be made available by Citrix. To use the trial license, navigate to the **Products** page and choose the **Try It** button, and go to `http://citrix.com/products/netscaler-access-gateway/overview.html?ntref=prod_cat`. Trial licenses are available only for the current products, as the new gateway versions become available and the trial licenses will be issued for those products.

Importing the Citrix Access Gateway into VMware

CAG for VMware is available as an **Open Virtual Format** file, (**OVA**). Once downloaded, you can import this into VMware using your VSphere Client, going to **File** | **Deploy OVF Template** | **Browse** | **OK**, and following the import wizard.

Importing the Citrix Access Gateway into XenServer

This process is very similar to the way in which we imported the License Server VPX. From XenCenter, we can choose **File** | **Import** and then browse to CAG that we have downloaded. The Citrix download has a `.XVA` extension. In this book, we use Version 5.04 of CAG to import in XenServer. Then the import wizard takes you through the storage location and the networks to connect to the VM. Remember that this should be connected to the DMZ or secure subnet between your private network and the Internet. Using the Citrix XenCenter tool, we can import the Citrix Access Gateway VPX from the XVA file.



Enter the pathname of an exported VM or template, an OVF/OVA package or a virtual h
Browse to find the file you want.

Filename: C:\Users\andrew\Downloads\cag_5.0.4.223500.xva

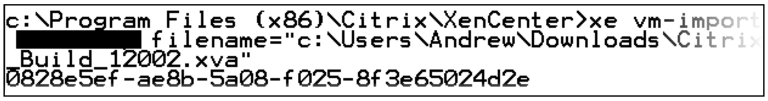
It is also possible to import virtual machines from the command line of your Windows machine that has XenCenter installed and CAG download available. `XE.EXE` is the command to use; this though, is not in the `PATH` statement and as such will necessitate your running XE from `%PROGRAMFILES%\Citrix\XenCenter` on a 32-bit host and `%PROGRAMFILES (x86)%\Citrix\XenCenter` on a 64-bit host. An example of a 32-bit Windows host would be:

```
cd %PROGRAMFILES%\Citrix\Xencenter
xe vm-import -s 192.168.0.12 -u root -pw Password1 filename="c:\tmp\
cag_5.0.4.223500.xva
```

The `xe` command is written as a single line, including the filename argument that has been wrapped in this book.

Depending on the speed of your disk subsystem, network, and processors, the import can take up to an hour to complete. If using the command line, once the import has completed, you will be presented with the unique ID or UUID of the imported machine.

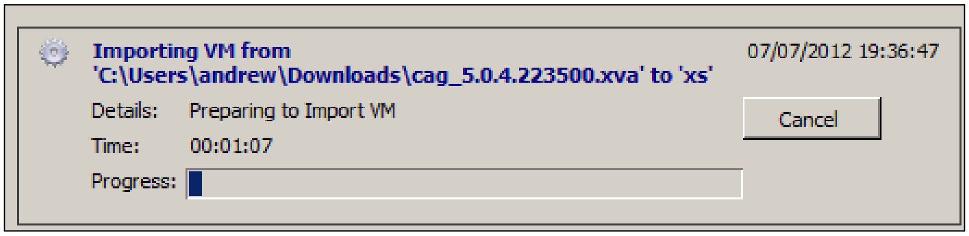
If you use the `xe` command from the command line for the import, the virtual machine's UUID is displayed on completion of the import.



```
c:\Program Files (x86)\Citrix\XenCenter>xe vm-import
 [redacted] filename="c:\Users\Andrew\Downloads\Citrix
_Build_12002.xva"
0828e5ef-ae8b-5a08-f025-8f3e65024d2e
```

If you are using the XenCenter graphical tool, you can follow the progress on the **Logs** tab of the virtual machine being imported. These logs are displayed in XenCenter in all cases, even if the import was initiated from the command line.

If you are using XenCenter for the import, the import progress can be seen from the **Logs** tab in XenCenter.



Importing VM from 'C:\Users\andrew\Downloads\cag_5.0.4.223500.xva' to 'xs'

07/07/2012 19:36:47

Details: Preparing to Import VM

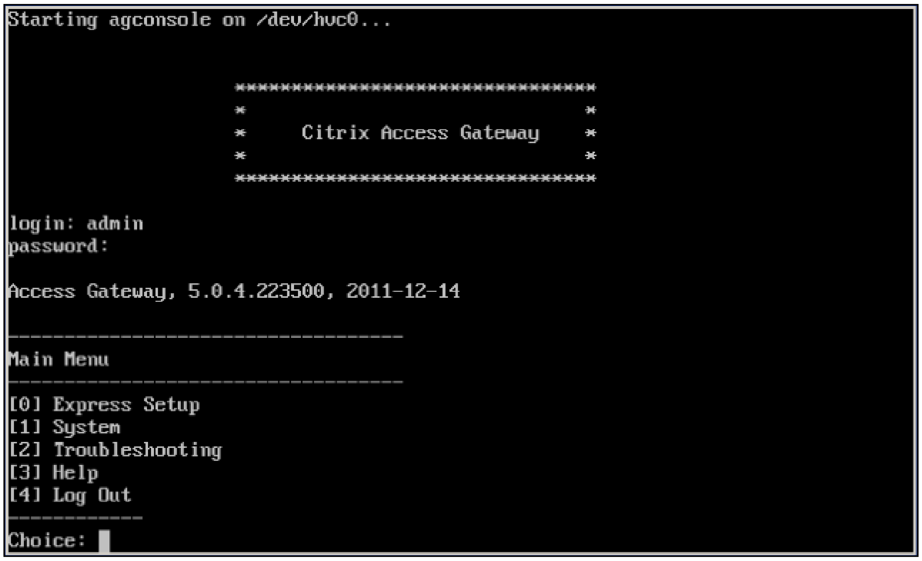
Time: 00:01:07

Progress:

Initiating the Access Gateway setup from the command line

Before starting CAG, make sure that its pre-configured IP address will not conflict with anything else on the DMZ, that is, `10.20.30.40/24`.

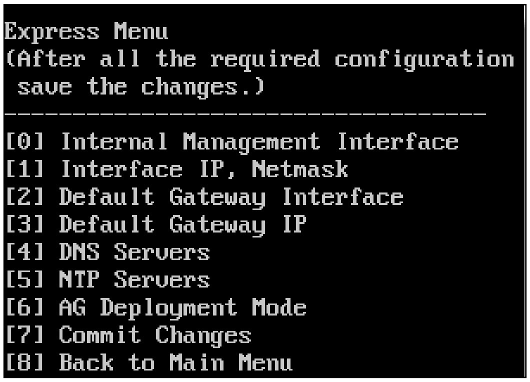
We will change the IP address of CAG once it has started, but we need to make sure that the pre-configured address will not conflict with anything on your DMZ. Once CAG has started, you can log in with the default username and password – `admin` and `admin`. CAG is designed to be hosted on a secure operating system; part of this security within CAG is to restrict access to the command prompt. As such, even as the user admin, we are restricted to what we can run from the system-supplied menu, rather than having direct access to the command line itself. Once the login process is complete, you will be presented with the main menu from where we can access the Express Setup, where the fun can begin. The following is the screenshot of the console's main menu:



```
Starting agconsole on /dev/hvc0...

                    ********************************
                    *                              *
                    *     Citrix Access Gateway    *
                    *                              *
                    ********************************

login: admin
password:

Access Gateway, 5.0.4.223500, 2011-12-14

-----------------------------------
Main Menu
-----------------------------------
[0] Express Setup
[1] System
[2] Troubleshooting
[3] Help
[4] Log Out
------------
Choice: 
```

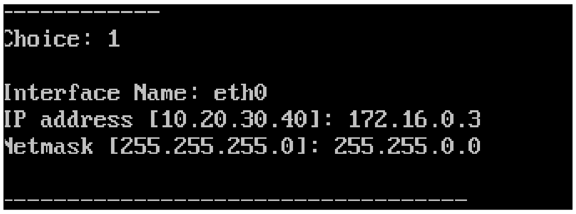
We will start by choosing option `[0]` for the `Express Setup` command and then select option `[1]` from the Express Menu to configure the IP address. Note that option `[0]` from the Express Menu is chosen if we want a separate interface to use for management of CAG. In this book, we use the single interface for both data and management.

The Express Menu allows you to quickly configure networking on CAG, as shown in the following screenshot:



```
Express Menu
(After all the required configuration
 save the changes.)
-----------------------------------
[0] Internal Management Interface
[1] Interface IP, Netmask
[2] Default Gateway Interface
[3] Default Gateway IP
[4] DNS Servers
[5] NTP Servers
[6] AG Deployment Mode
[7] Commit Changes
[8] Back to Main Menu
```

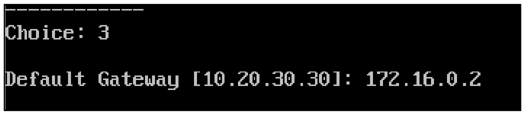
In the previous screenshot, option `[1]` from the `Express Setup` allows the IP address and subnet mask to be set:



```
------------
Choice: 1

Interface Name: eth0
IP address [10.20.30.40]: 172.16.0.3
Netmask [255.255.255.0]: 255.255.0.0

-----------------------------------
```

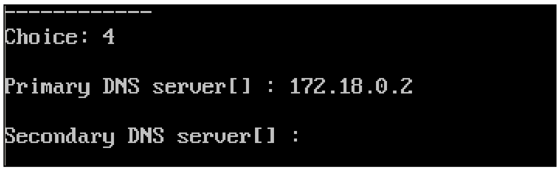
Continuing, we can select option `[2]` for the `Default Gateway Interface` command, `eth0`, the interface to access the default gateway, and then we can select option `[3]` to set the `Default Gateway IP` command. This should be set to the Internet-facing router of the DMZ. Based on the earlier network map, for our setup, we can see where we need to configure `172.16.0.2`.

When configuring the `Default Gateway IP` command with option `[3]`, ensure that it is configured as the Internet-facing router.



```
------------
Choice: 3

Default Gateway [10.20.30.30]: 172.16.0.2
```

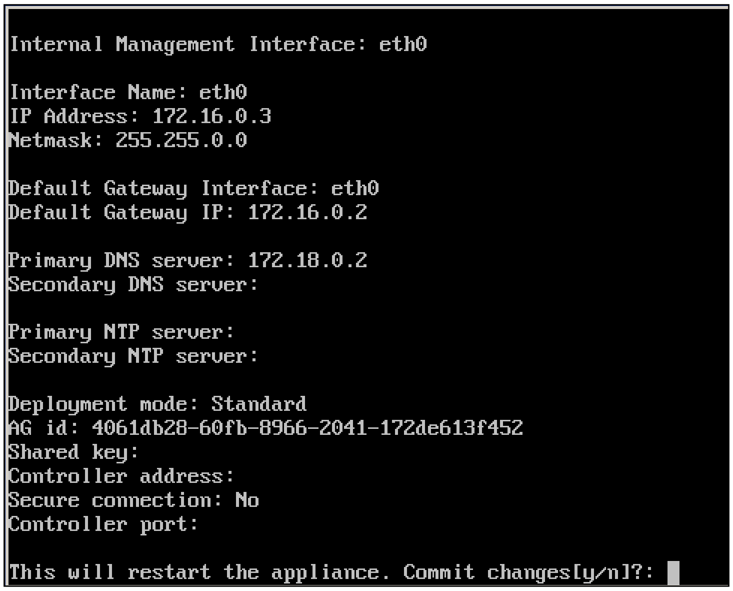
To configure the DNS, we can choose option `[4]` and in this case, we set `172.18.0.2` as our DNS server. We do not currently have a route to the `172.18.0.0/16` network, the private network; however, we will add a static route in later using the web-based management console of CAG.



```
------------
Choice: 4

Primary DNS server[] : 172.18.0.2

Secondary DNS server[] :
```

We would normally set the NTP server, but in this case we will leave it. The time will be synchronized to the XenServer host in any case and all our VMs are on a single machine. We would, though, recommend setting a time server to ensure accurate time, especially for agile virtual machines that move from the virtualization host to VM host.

Choosing option `[7]` allows us to commit the changes and will force a reboot of CAG after displaying a summary page. If we had selected option `[6]`, this would allow us to select the `Controller Deployment` mode, which is used as a policy filter within XenApp and XenDesktop; we will not be deploying the access controller. The following screenshot shows that the option `[7]` saves the changes and displays the summary:



```
Internal Management Interface: eth0

Interface Name: eth0
IP Address: 172.16.0.3
Netmask: 255.255.0.0

Default Gateway Interface: eth0
Default Gateway IP: 172.16.0.2

Primary DNS server: 172.18.0.2
Secondary DNS server:

Primary NTP server:
Secondary NTP server:

Deployment mode: Standard
AG id: 4061db28-60fb-8966-2041-172de613f452
Shared key:
Controller address:
Secure connection: No
Controller port:

This will restart the appliance. Commit changes[y/n]?:
```

While CAG is rebooting, we can summarize our selections:

- `[0]` for `Express Setup`
- `[1]` to set the IP Address and subnet
- `[3]` to set the default gateway
- `[4]` to configure the DNS
- `[7]` to save our changes and reboot

> The IP addresses detailed here match the lab environment used to develop this book. Don't forget that you will use addresses appropriate for your own networks.

Now we are ready to complete the initial setup using the web console.

Completing the initial configuration from the web portal

We will use CAG's web console to complete the initial configuration. For this, we will use a PC with Internet connection for our lab. In your own environment, you may choose to deploy CAG with a management interface connected to your private network. This would effectively restrict access to the console to hosts on the internal network.

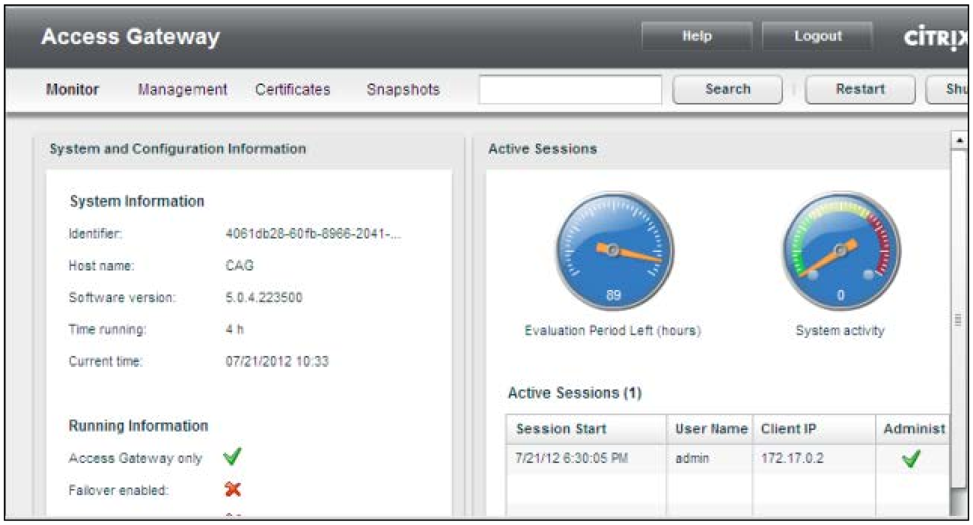
> Adobe Flash is required in the browser to manage CAG.

To access the management console, go to `https://ag.example.com/lp/adminlogonpoint`.

You would, of course, replace the address with the address of your own server.

CAG can only be accessed using HTTPS connections. To facilitate initial configuration, a self-signed certificate is installed. This, naturally, is not trusted by your browser, so for the moment, we will accept the certificate warnings as we access the site. We can log on with the same credentials we used before – `admin` as the username and `admin` as the password. As we have not licensed the server yet, we will receive a warning about the trial license and the number of hours remaining. The dashboard acts as a welcome page for the gateway and we can monitor its health from this page.

We are taken to the dashboard when first accessing the web console of CAG:



System Information

Identifier:	4061db28-60fb-8966-2041-...
Host name:	CAG
Software version:	5.0.4.223500
Time running:	4 h
Current time:	07/21/2012 10:33

Running Information

Access Gateway only	✓
Failover enabled:	✗

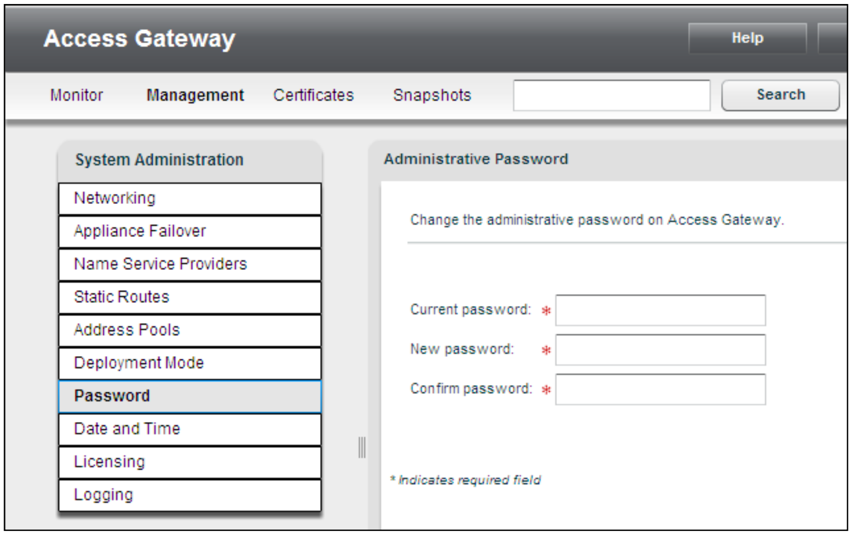
Active Sessions (1)

Session Start	User Name	Client IP	Administ
7/21/12 6:30:05 PM	admin	172.17.0.2	✓

Setting the admin password

Our first calling point should be to change the admin password, replacing the default password to something a little more secure. This is especially true if the management console is available on the Internet; although, I would not be surprised to find many gateways out there with a password of admin. From the **Management** tab, we can then choose **Password**. The new password must meet the following security complexity:

- Between 6-128 characters in length
- At least one uppercase and one lowercase letter
- At least one number
- And at least one non-alpha-numeric character, such as a question mark or hyphen



Administrative Password

Change the administrative password on Access Gateway.

Current password: *

New password: *

Confirm password: *

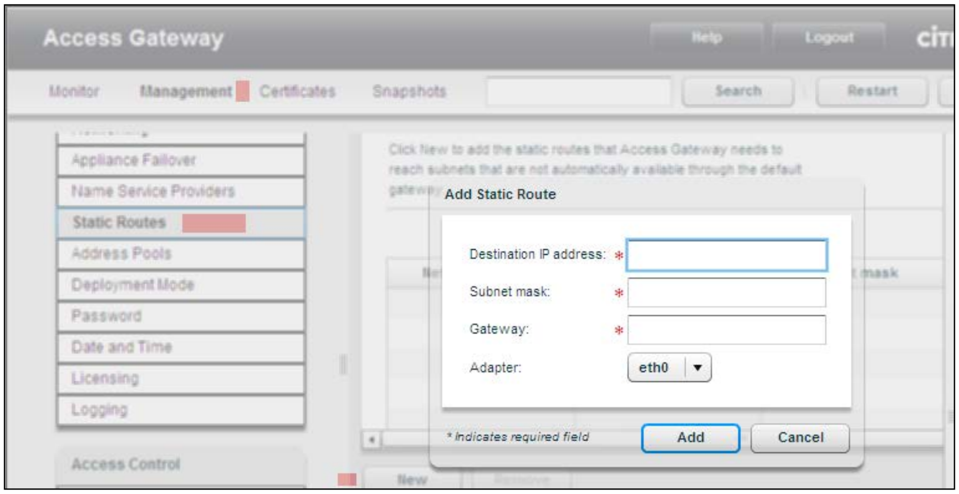
* Indicates required field

Setting your admin password, as seen from the web console, is shown in the previous screenshot.

Add a static route to a private network

The next step that we shall take is to add a route to CAG to enable connections to internal hosts on our private network. This is necessary because the default gateway that we point to is the Internet-facing router, which does not have an entirely correct route to the internal network. We want to ensure that access to the internal network is available only via CAG. We need to configure the route at this stage, as License Server is located on the private, internal network.

Again, using the **Management** tab, we can access **Static Routes** | **New** and then complete the details prior to clicking the **Add** button.



Click New to add the static routes that Access Gateway needs to reach subnets that are not automatically available through the default gateway.

Add Static Route

Destination IP address: *

Subnet mask: *

Gateway: *

Adapter: eth0

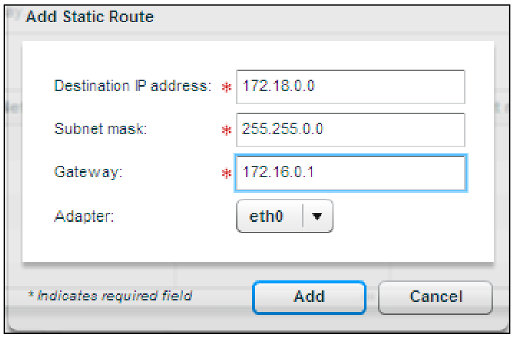
* Indicates required field

Adding a static route to the private network is required in most cases.

We will add in the following configuration to match the lab environment we are using for this book:

- Destination IP address: `172.18.0.0`
- Subnet mask: `255.255.0.0`
- Gateway: `172.16.0.1`
- Adapter: `eth0`

The dialog box then should appear as shown in the following screenshot; use the **Add** button and then the **Save** button when you are satisfied with the entered data. The following is the screenshot of **Adding Static Route**:



Add Static Route

Destination IP address: * 172.18.0.0

Subnet mask: * 255.255.0.0

Gateway: * 172.16.0.1

Adapter: eth0

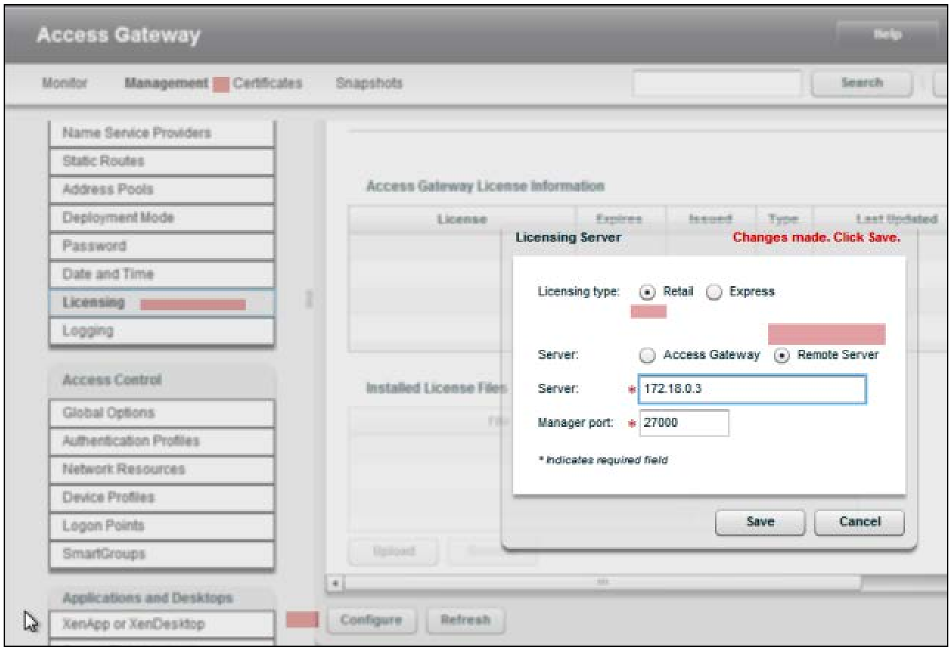
* Indicates required field

To verify the connectivity into the private network, we can access the console of CAG. By logging in with `admin` and our new password, we can:

- Select option `[2]` from the menu for troubleshooting
- Select option `[0]` for Network Utilities
- Select option `[1]`, which will display the routing table
- Select option `[3]` to ping another device, such as License Server; in our case, `172.18.0.3`

Licensing the Citrix Access Gateway

Having added in the static route to the private network, we now have connectivity from CAG through to License Server. We shall now add in the connection details to License Server. We start again on the **Management** tab and this time we choose **Licensing**. From the bottom-middle of the web page, we can then click the **Configure** button. From here, we choose **Retail** for the type of license, Remote Server for the server, and then add in the server IP address or DNS name. The dialog should look similar to that shown in the following screenshot:



Licensing Server

Changes made. Click Save.

Licensing type: ● Retail ○ Express

Server: ○ Access Gateway ● Remote Server

Server: * 172.18.0.3

Manager port: * 27000

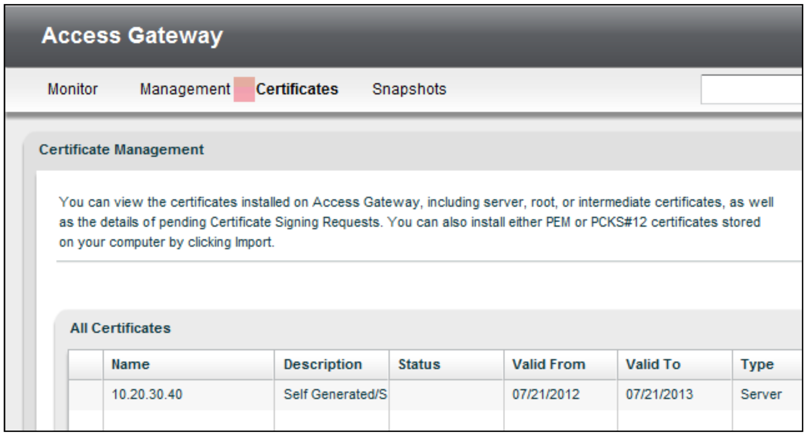
* indicates required field

Once completed, you can use the **Save** button; the page will then refresh for a few seconds and the license details will be displayed. At this stage, we are able to use CAG, but we really should add a certificate correctly issued to CAG DNS name and signed with a trusted certificate. This will prevent the warnings that we have received in the browser so far.

Adding SSL certificates

You will have noticed the certificate warnings in the browser. As a user, we can override these warnings as we understand what is happening. However, automated processes may not be as forgiving as we might be. We need to add in signed SSL certificates issued to CAG's DNS name; in the case of the lab server, this is `ag.example.com`. We will look at how we can use CAG management console to create a certificate ready for signing. This will be submitted to our certificate authority as a **certificate signing request** (**CSR**). This will be imported back into the console, along with the trusted root certificate of the **certificate authority** (**CA**). In this book, we will use a Microsoft Active Directory CA, as you may also, however, always consider the use of an external signing authority when access from machines on the Internet is required. This ensures that no matter who owns the device, the trusted root certificate will be present. This may not be the case with internal corporate CAs.

From CAG management console, we will need to access the **Certificates** tab. From here, we can see the internal certificate that ships with the appliance. This is issued to the IP address and not signed by a CA. Hence, it is of little use for authentication of the server, although it still provides effective encryption. Following is the screenshot of **Certificate Management**:

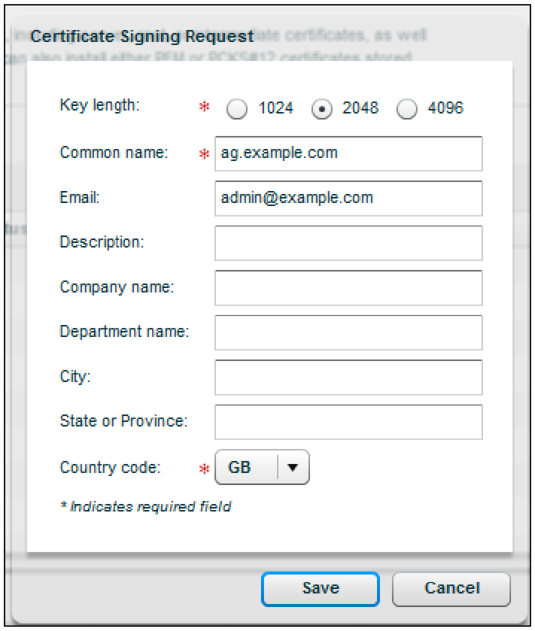


You can view the certificates installed on Access Gateway, including server, root, or intermediate certificates, as well as the details of pending Certificate Signing Requests. You can also install either PEM or PCKS#12 certificates stored on your computer by clicking Import.

All Certificates

Name	Description	Status	Valid From	Valid To	Type
10.20.30.40	Self Generated/S		07/21/2012	07/21/2013	Server

Using the **New** button on the right-hand side of the page, we can create a new signing request to submit to the CA. Make sure that the **Common name** field exactly matches the fully-qualified DNS name used to access CAG, and double-check the spelling. Part of the SSL authentication will check the DNS name in the entered URL against the **Common name** field in the certificate, so they have to match. The following is the screenshot of **Certificate Signing Request**:



Certificate Signing Request

Key length: * ○ 1024 ● 2048 ○ 4096

Common name: * ag.example.com

Email: admin@example.com

Description:

Company name:

Department name:

City:

State or Province:

Country code: * GB ▾

* Indicates required field

On clicking the **Save** button, we will be presented with the certificate to paste into the signing request on the CA. Use the **Copy** button to copy the certificate straight to our paste buffer.

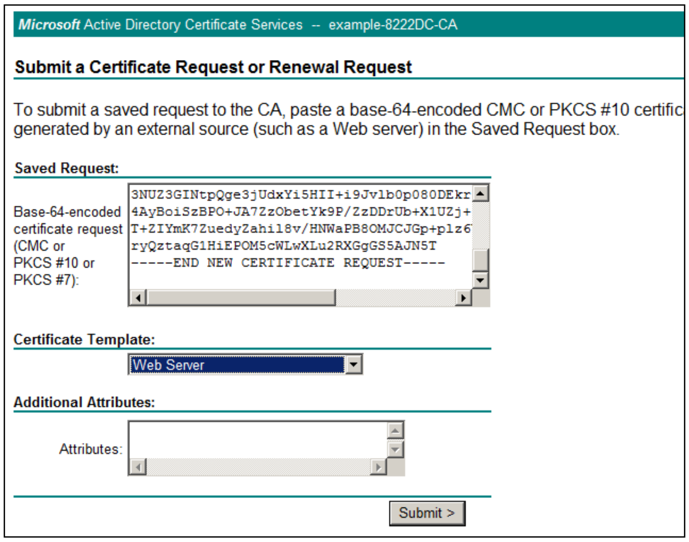
For this book, we use the Certificate Server integrated with Active Directory on Microsoft Windows Server. To access the CA via the web browser, enter the following URL:

```
https://8222DC.example.com/certsrv
```

Once on the CA web page, we choose:

Request a Certificate | **Advanced Certificate Request** | **Submit a request**.

Paste the contents of the paste buffer into the **Saved Request** field and select **Web Server** as the **Certificate Template** listbox. Following is the screenshot of the certificate signing request on the CA:



Microsoft Active Directory Certificate Services -- example-8222DC-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certific generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
3NUZ3GINtpQge3jUdxYi5HII+i9Jvlb0p080DEkr
4AyBoiSzBPO+JA7ZzObetYk9P/ZzDDrUb+X1UZj+
T+ZIYmK7ZuedyZahil8v/HNWaPB8OMJCJGp+plz6
ryQztaqG1HiEPOM5cWLwXLu2RXGgGS5AJN5T
-----END NEW CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

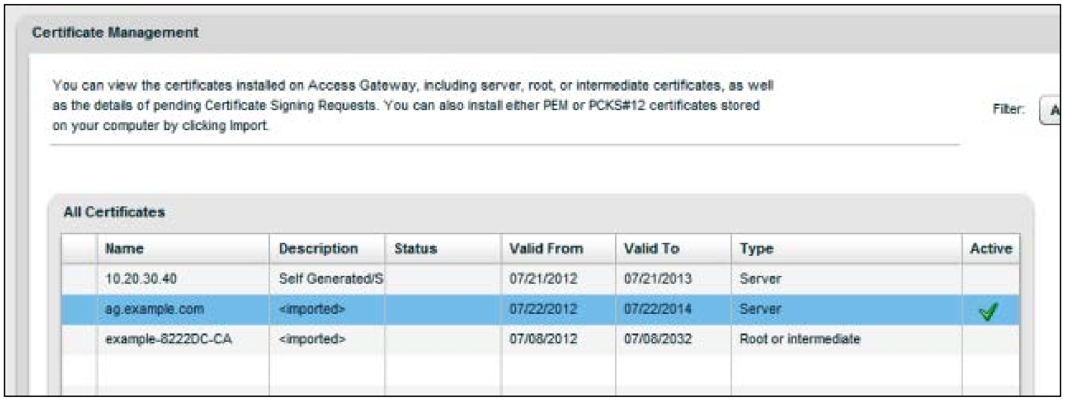
Attributes:

Click on the **Submit** button to jump to the download page. We need to download the certificate as a base-64 file. Now we return to CAG web console and choose **Import** | **Server .pem** from the **Certificates** page. We will be prompted for a password, but no password is assigned to the private key we generated on CAG. Proceed, leaving the **Password** field blank and click on **OK**.

The final part of the certificate setup is to install the CA's public key onto CAG. This is required if CAG needs to connect to the XenApp Web Interface server using SSL; just like a client browser, the CA's key is required for trusting certificates that it has issued. From the certificate server's welcome page, choose **Download a CA key** | **base64 + Download CA certificate**. Again, save this and import into CAG.

From CAG web console, choose **Import** | **Trusted .pem** from the **Certificates** page and click on **OK**.

Just one small job left, and that is to make the certificate active for the newly issued server certificate. In our case, we will click the `ag.example.com` certificate and then choose **Make Active** towards the right of the page. Once active it will be marked with a green checkmark. Making the certificate that we imported active is shown in the following screenshot:



Certificate Management

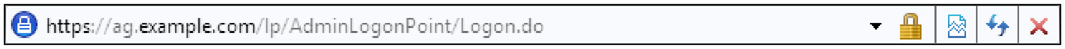
You can view the certificates installed on Access Gateway, including server, root, or intermediate certificates, as well as the details of pending Certificate Signing Requests. You can also install either PEM or PCKS#12 certificates stored on your computer by clicking Import.

All Certificates

	Name	Description	Status	Valid From	Valid To	Type	Active
	10.20.30.40	Self Generated/S		07/21/2012	07/21/2013	Server	
	ag.example.com	<imported>		07/22/2012	07/22/2014	Server	✓
	example-8222DC-CA	<imported>		07/08/2012	07/08/2032	Root or intermediate	

Now that we have completed the certificate setup on the server, we just have to make sure that the CA key is distributed to clients; remember our discussion about the external signing authority. Distribution of the CA certificate, though, is made very easy in a Microsoft Windows domain environment using group policies.

With the certificate process complete, we are able to log on to the management console of CAG without the certificate errors we encountered earlier.



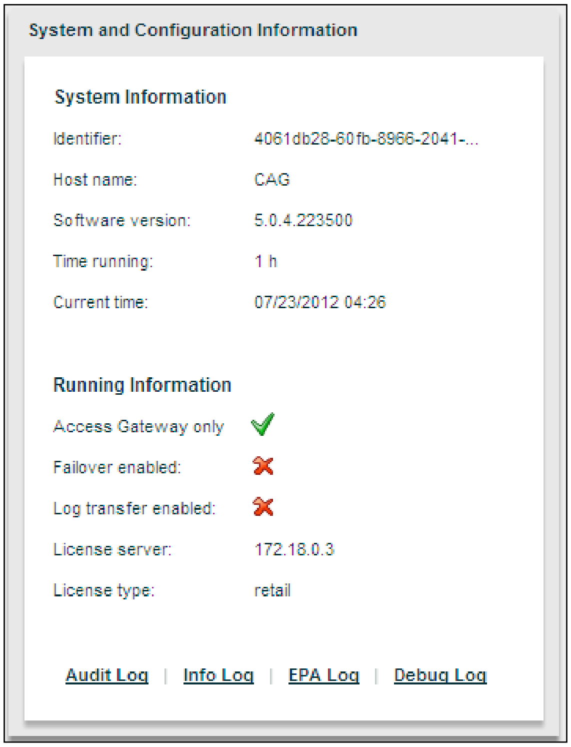
https://ag.example.com/lp/AdminLogonPoint/Logon.do

Notice the error-free access via HTTPS; certificates are now installed and configured correctly on CAG.

Monitoring the Citrix Access Gateway

Having completed the initial setup on CAG, we can now become a little more familiar with the **Monitor** tab of the management console we have been using on CAG.

From the **Monitor** tab, the first column we see on the left-hand side is **System and Configuration Information** column. From here, we can see the version of CAG, which is also known as the firmware; remember that this firmware can run on the Model 2010 NetScaler hardware appliance. The current time displayed is always in the Pacific Time zone. On our server, we see that we have not enabled Appliance Failover nor do we have Log Transfer, which is denoted by the big red X. These are optional and we will look at this setup later in the book. Links to the logs are displayed at the bottom of this column. The system and configuration column is detailed in the following screenshot:



System and Configuration Information

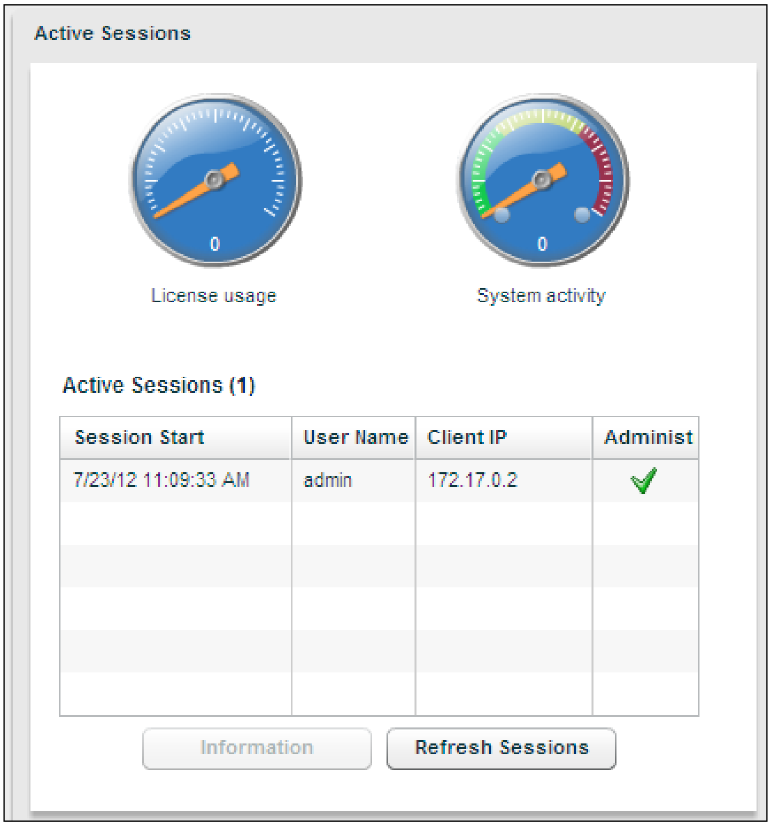
System Information

Identifier:	4061db28-60fb-8966-2041-...
Host name:	CAG
Software version:	5.0.4.223500
Time running:	1 h
Current time:	07/23/2012 04:26

Running Information

Access Gateway only	✓
Failover enabled:	✗
Log transfer enabled:	✗
License server:	172.18.0.3
License type:	retail

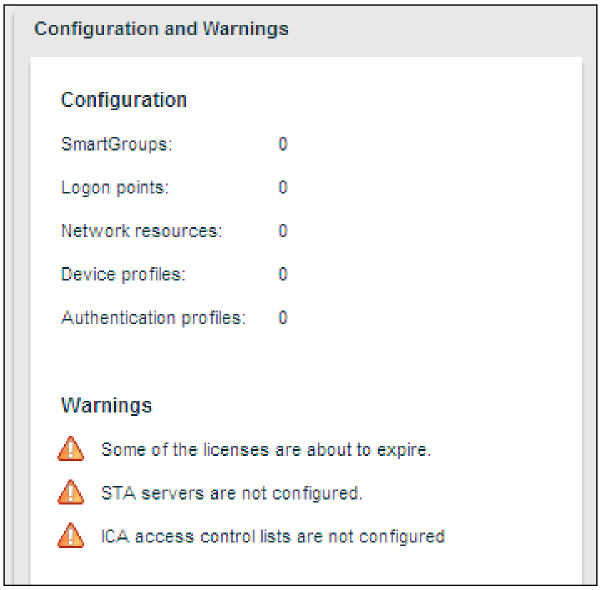
From the **Active Sessions** column, we can view, as you have guessed it – active sessions; not only this, the dials display **License usage** and **System activity**. Note that the left-most dial has changed from **Evaluation period left (hours)** to **License usage**. We can also drop down to the active sessions and once we have selected a session, we can click the **Information** button to view logon information and the client IP address. The following is the screenshot of **Active Sessions**:



Active Sessions (1)

Session Start	User Name	Client IP	Administ
7/23/12 11:09:33 AM	admin	172.17.0.2	✓

Finally we can view the **Monitor** tab's **Configuration** and **Warnings**. From here, we can view the amount of logon points we have created and items such as **SmartGroups** and **Device profiles**; below this, we see warnings. The licenses I have added have expiry dates, so I am warned about this as well as the fact that we have not set up the ICA access control list or **secure ticket authorities** (**STA**s). This is expected at this stage, as we have not set up any of this (but will do when we configure access to XenApp and XenDesktop in the next chapter). The following is the screenshot of **Configurations** and **Warnings**:



Configuration and Warnings

Configuration

SmartGroups:	0
Logon points:	0
Network resources:	0
Device profiles:	0
Authentication profiles:	0

Warnings

⚠ Some of the licenses are about to expire.

⚠ STA servers are not configured.

⚠ ICA access control lists are not configured

Summary

In this chapter, we have completed the initial setup of CAG. This involved downloading and importing CAG into XenServer. Once CAG has started from the command line, we can log in as `admin` with the password `admin`. We are presented with the menu and start the Express Setup. Once this is complete, we can continue the setup by changing the password, adding in static routes, and adding the licenses and server certificates via the management web console. With this complete, we are ready to move on to the next chapter, where we will get started with basic logon points to XenDesktop and XenApp.

4

Configuring a Basic Logon Point for XenApp/XenDesktop

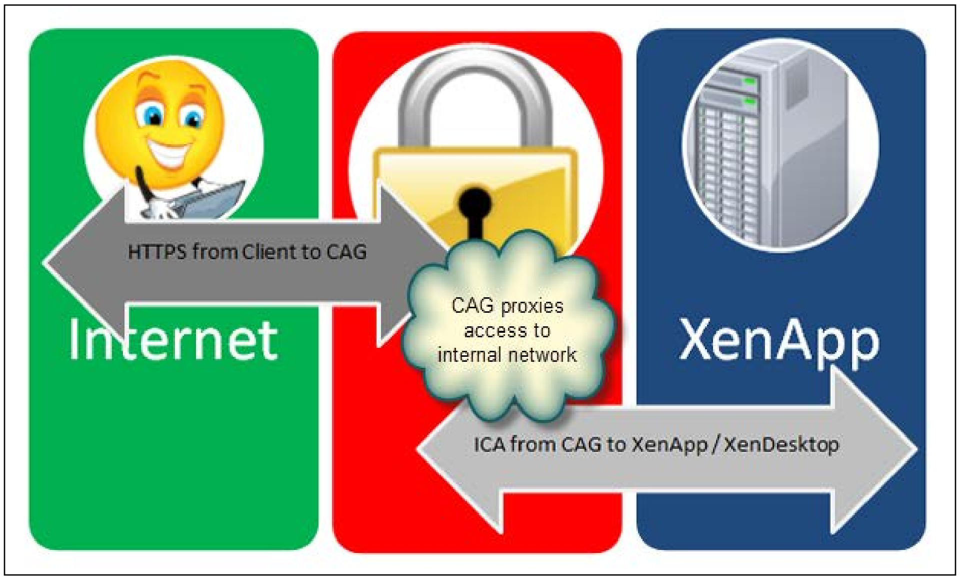
The ability for system administrators to provision remote access to users who are away from the office is becoming an absolute necessity; the headache is to keep this access secure. We have seen from our network layout in the previous chapter that we are prohibiting access from the big wide world (the Internet) to anything on our private network. Access, therefore, must be obtained through CAG. One of the most commonly used functions of the gateway will be to provide secure access to Citrix XenApp and XenDesktop hosts located on the internal, private network. By the end of this chapter, we will have created basic logon points, so remote users will be able to use these resources easily and securely, along with other internal web resources, such as:

- Identifying the need for using CAG for remote access to XenApp/XenDesktop
- Configuring a Citrix Web Interface site for use with the CAG
- Configuring a CAG basic logon point
- Accessing the server farms securely using the CAG
- Editing the logon point to allow access to any internal web resource
- Auditing access to the CAG

Identifying the need for using CAG as a remote access solution

As in the case of the lab environment that we are using throughout this book, it is quite normal to use private address ranges for our internal servers. Our XenApp application server is on the private network `172.18.0.0` and is not accessible from the Internet. Even though connections to the XenApp server will work correctly from internally based hosts on the private network, they will not work for remote users on the Internet. It is possible using static **NAT** (**network address translation**) to map public addresses on a router, though, to the private addresses on your internal network. The NAT table can be maintained on the NAT router or by using the `ALTADDR` command on the XenApp server. However, as your server farm grows, you will need more and more public addresses; this really is not scalable, especially to desktop virtualization with XenDesktop. The solution lies with the proxy service provided by the CAG. Using this method, CAG requires a public address but not the resources they connect to.

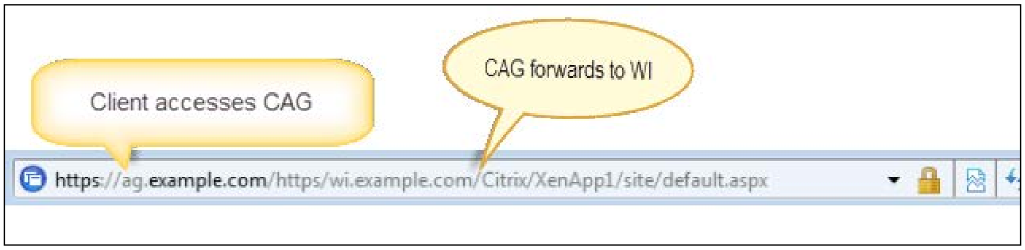
The CAG requires a public address, but the private resources can remain with just private IP addresses and are accessible only via CAG.


HTTPS from Client to CAG
Internet
CAG proxies access to internal network
XenApp
ICA from CAG to XenApp / XenDesktop

Our remote clients will have access to the CAG, and as we saw in the previous section, CAG will have a static route added to allow it to connect to the internal resources. The CAG will then receive and forward the initial requests to the Citrix **Web Interface** (**WI**) and display XenApp and XenDesktop resources to the user. Once a resource is selected, CAG will proxy the ICA requests directly to the XenApp server or virtual desktop.

Additionally, with CAG 5.04 firmware, we will see that the CAG can act as a reverse proxy, using just the platform license to other web-based resources on our internal network.

The CAG forwards requests initially to the WI, as shown in the following screenshot:



https://ag.example.com/https/wi.example.com/Citrix/XenApp1/site/default.aspx

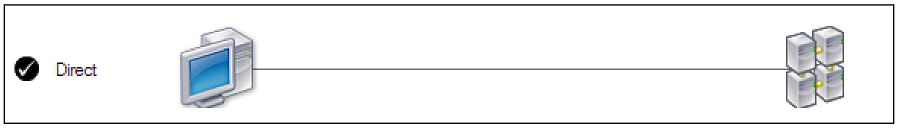
In short, using the CAG will allow for secure remote access to internal resources without the use of additional IP addresses or opening up ports other than HTTPS/443 through the Internet-facing firewalls.

Configuring a Citrix Web Interface site for use with the Citrix Access Gateway

When remote users connect from the Internet, they are directed to the CAG and from there onto the Web Interface server. All connections to Citrix XenApp servers and XenDesktop virtual desktops must pass through the WI; this is true even if connections are not made through CAG. The WI will connect into the server farms and locate resources for the user. Once available resources have been located, an ICA file with the path to the resource will be supplied back to the user. In the case of local users, they can connect directly to the XenApp or XenDesktop resource.

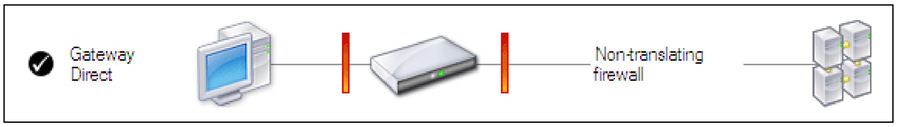
This is not possible for remote users, so we must create a website specifically for them that will instruct these users to proxy their connection via the CAG.

The WI, if left at the defaults, will use direct connections to internal resources from client devices.



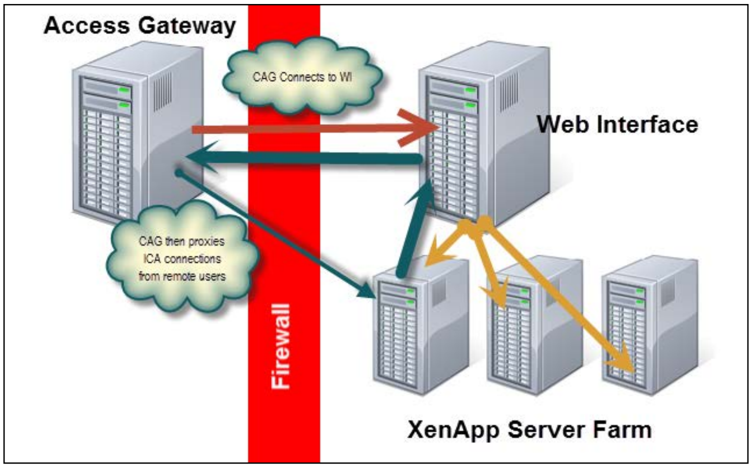
Configuring our WI site for connections using CAG will ensure that the clients connect to internal resources via the CAG. The WI will create ICA files for client connections that specify the requirement to connect through the CAG.

Remote connections will be made via CAG, as shown in the WI when modified.



Web Interface placement

It will be possible to place the WI server in the DMZ, and this would be the recommendation if authentication needs to take place at the WI. However, there really does not seem to be a strong argument to have authentication occur at the WI; CAG is able to and should authenticate the users. In this way, authentication occurs at the first point of contact for the users rather than forwarding unauthenticated traffic to the WI. Placing the WI on the internal network would also allow the device to provide access for both internal and remote users. Internal users would not be able to connect to the WI if it were to be placed in the DMZ.



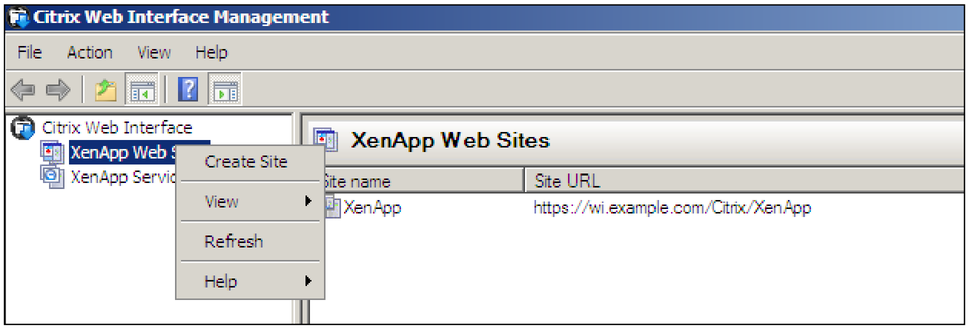
Placing the WI on the internal network offers the most security, as it is not exposed to external threats, and the single WI can be used by internal and external connections.

Configuring a website for remote users

Now that we understand a little about the physical placement of the Citrix WI server, we will begin to investigate the steps in configuring a website, specifically, for our remote workers. The remote users will connect transparently to the WI site; they need visibility and knowledge of the CAG logon point, but not of its target (the WI). The WI is managed using the **Citrix Web Interface Management** console, usually installed on the WI server, along with the web service itself. From the management console, we navigate to **XenApp Web Sites**, and by right-clicking on it, we choose **Create Site**.

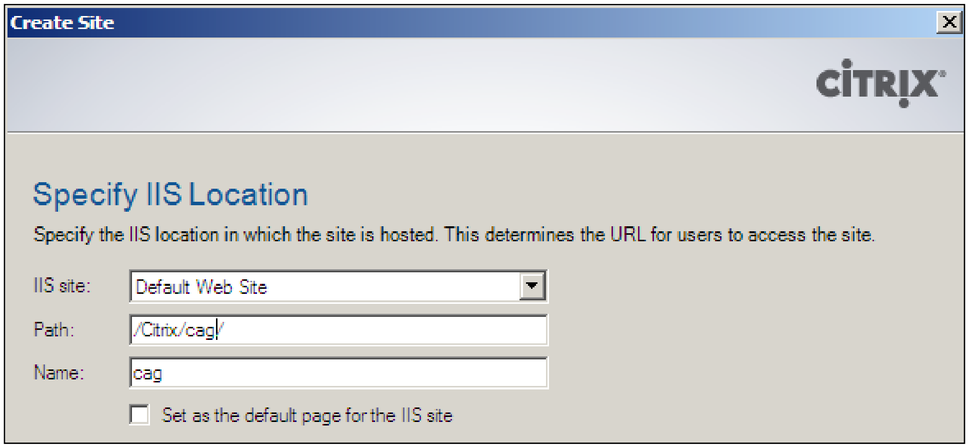
> Remember, the CAG will provide connections to the websites in the WI and do not use service sites. Service sites are for native connections with the Citrix Receiver.

The first step in creating a new website from within the **Citrix Web Interface Management** console is shown in the following screenshot:



Site name	Site URL
XenApp	https://wi.example.com/Citrix/XenApp

From the **Create Site** dialog, we just need to set a path and name. If we are using the default IIS website, then the path we type will be relative to `c:\inetpub\wwwroot`. So in our case, the full path to the website for our remote users will be `c:\inetpub\wwwroot\Citrix\cag`, as shown in the following screenshot:



Specify IIS Location

Specify the IIS location in which the site is hosted. This determines the URL for users to access the site.

IIS site: Default Web Site

Path: /Citrix/cag/

Name: cag

☐ Set as the default page for the IIS site

Once we have completed this first page of the wizard, the following page will ask us for the point of authentication. We will leave this set to the WI initially, allowing us to expand on this later, and include authentication profiles on CAG. These will allow authentication to take place on the CAG itself. We will continue past the summary page to create the new site. We can configure the site straight away or postpone until later; at this stage though, our site is created using default values. As a minimum, we will need to set the following:

- The server farm or farms to connect to
- The connection type
- The authentication type

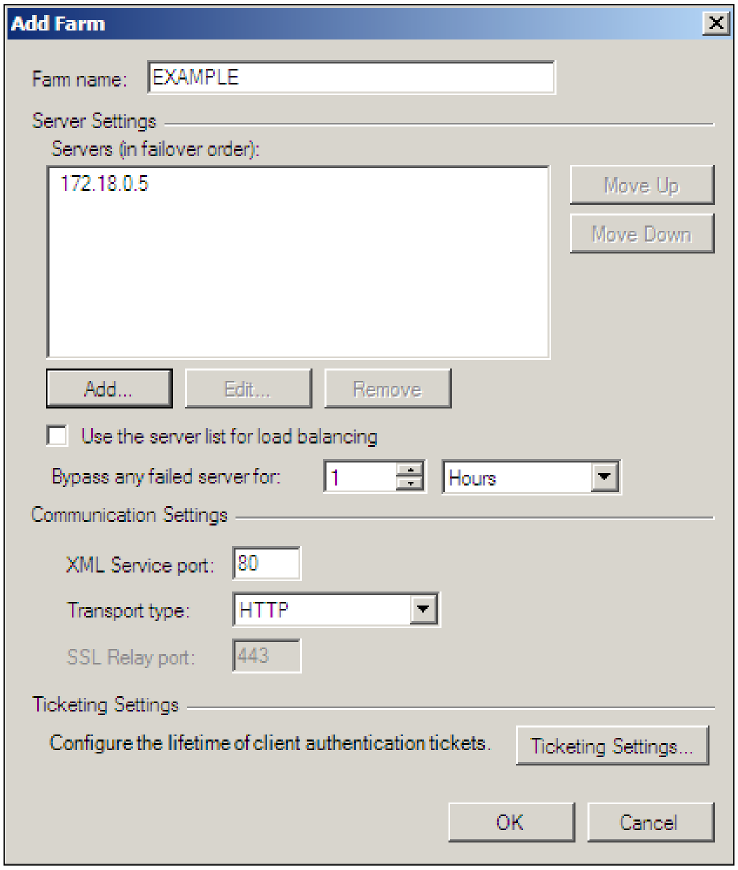
These settings are saved to the file:

```
c:\inetpub\wwwroot\Citrix\<nameofsite>\conf\webinterface.conf
```

Changes can be made directly to the file, but are more often configured through the GUI management console.

Firstly, within the WI management console, we will add in the server farm that we need to connect with; this could be a XenApp farm so that users can access hosted and streamed applications or XenDesktop to support desktop virtualization. We will connect to a XenApp farm from this website. Navigating to the website that we will use for the CAG, we can right-click on the site and select **Server Farms**. From here, we can add a list of XenApp servers for the WI server to connect to in order to obtain a list of applications associated with our remote user. Remove any existing server (this normally includes the local host and is not valid).

Adding connections to your server farm from the WI console is shown in the following screenshot:



Add Farm

Farm name: EXAMPLE

Server Settings

Servers (in failover order):

172.18.0.5

☐ Use the server list for load balancing

Bypass any failed server for: 1 Hours

Communication Settings

XML Service port: 80

Transport type: HTTP

SSL Relay port: 443

Ticketing Settings

Configure the lifetime of client authentication tickets.

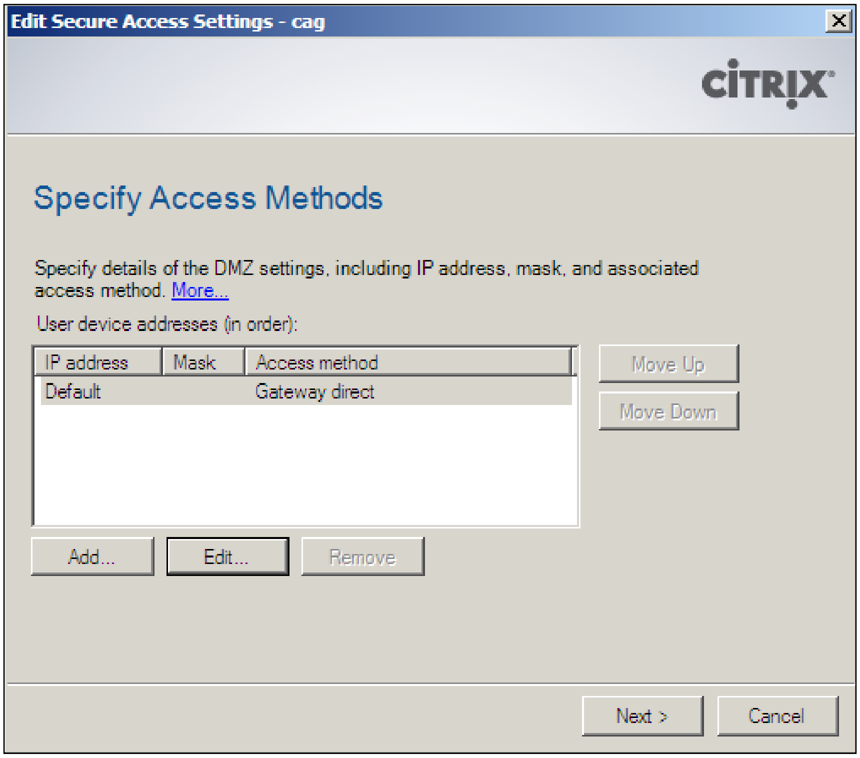
As we can see from the previous screenshot, we have added just one server; if more servers existed, these too would be added. However, there is certainly no need to add all the servers that exist in the farm, providing more than one will offer redundancy. We can use DNS names or the IP addresses of the servers that we add to the server list.

Changing the Secure Access method

With this set, we move on to the connection type. We know that we need to proxy the connections and as such, we will change the default setting of **Direct**, indicating that the clients connect directly to the XenApp server, to **Gateway direct**, used when remote users have their connections made via the CAG.

By right-clicking on the menu, on the website, we should now select **Secure Access**. From the next page, we will edit the existing connection type from **Direct** to **Gateway direct**.

Editing the exiting connection type to enable **Gateway direct** connections is shown in the following screenshot:



Edit Secure Access Settings - cag

Specify Access Methods

Specify details of the DMZ settings, including IP address, mask, and associated access method. More...

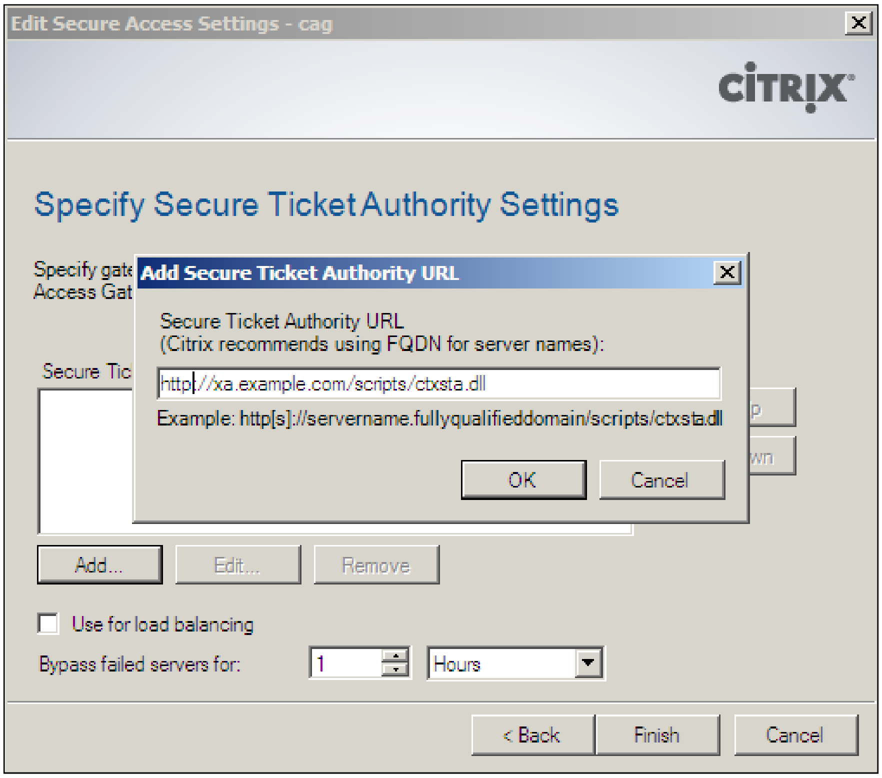
User device addresses (in order):

IP address	Mask	Access method
Default		Gateway direct

We continue with this wizard by selecting the **Next** button, as we are required to complete details of the CAG. In our case, we enter `ag.example.com` as the address of the gateway. Here we have to use the DNS name, so we can match the common name issued in the certificate. The WI server should have the public key of the CA in its certificate store in order to be able to authenticate CAG. Distribution of the CA certificate is normally managed with group policies and this is already in place for the `example.com` domain.

The final configuration page will require us to set the address of the XenApp servers, or **Secure Ticket Authorities** (**STA**s) to connect to. These would normally be the same servers that we listed for the server farm. Unless we are using HTTPS, we can use the IP address or DNS name. The XenApp servers do not have certificates, so we use HTTP. The STAs provide access tokens or tickets that CAG will duplicate to the remote user, maintaining a copy itself. The ticket identifies the user's session to CAG and from CAG to the XenApp servers. Each session will have its own unique ticket.

Adding the STA completes the **Edit Secure Access Settings - cag** wizard, as shown in the following screenshot:



Edit Secure Access Settings - cag

Specify Secure Ticket Authority Settings

Specify gate
Access Gat

Secure Tic

Add Secure Ticket Authority URL

Secure Ticket Authority URL
(Citrix recommends using FQDN for server names):

http://xa.example.com/scripts/ctxsta.dll

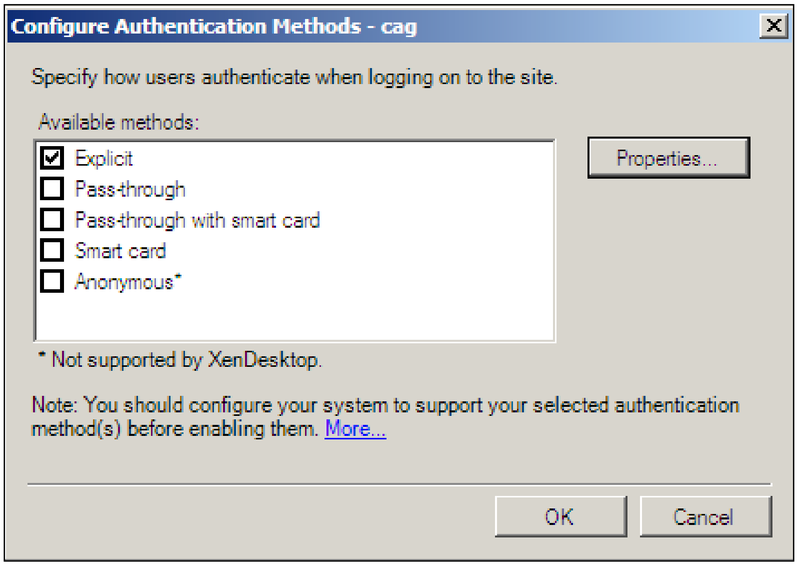
Example: http[s]://servername.fullyqualifieddomain/scripts/ctxsta.dll

□ Use for load balancing

Bypass failed servers for: 1 Hours

Finally, for the website configuration, we will configure the authentication type. This we will set as **Explicit**. As we expand the complexity of the configuration later in the book, we will reset this to **Pass-through**. With **Explicit**, the user will type in the username, password, and possibly domain. This fits the scenario where our users are remote and authenticating at the WI. **Pass-through** would take the user's current credentials and use these to access the server farm. To access authentication settings, we can again right-click on its menu and click on **Authentication Methods**. **Explicit** should be the default, but it never hurts to double-check.

Check that **Explicit** authentication is enabled when authenticating remote users at the WI, as shown in the following screenshot:



Configure Authentication Methods - cag

Specify how users authenticate when logging on to the site.

Available methods:

☑ Explicit
☐ Pass-through
☐ Pass-through with smart card
☐ Smart card
☐ Anonymous*

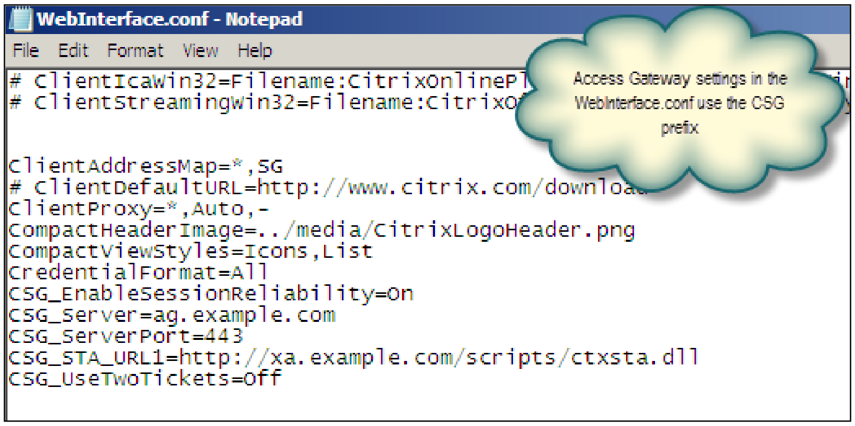
* Not supported by XenDesktop.

Note: You should configure your system to support your selected authentication method(s) before enabling them. More...

We have implemented these changes through the GUI management console; you may recall that these settings could also be achieved by writing to the `webinterface.conf`. References to the CAG in this file use the CSG prefix from the earlier Citrix Secure Gateway product. Once the configuration is complete, do not forget to back up this file: `c:\inetpub\wwwroot\Citrix\<nameofsite>\conf\webinterface.conf`

> It is also possible to use this file as a template for creating additional sites, even if those sites exist on different Web Interface servers.

Changes can be implemented via the GUI or the `webinterface.conf` file, as shown in the following screenshot:



```
# ClientIcaWin32=Filename:CitrixOnlineP
# ClientStreamingWin32=Filename:CitrixO


ClientAddressMap=*,SG
# ClientDefaultURL=http://www.citrix.com/downloa
ClientProxy=*,Auto,-
CompactHeaderImage=../media/CitrixLogoHeader.png
CompactViewStyles=Icons,List
CredentialFormat=All
CSG_EnableSessionReliability=On
CSG_Server=ag.example.com
CSG_ServerPort=443
CSG_STA_URL1=http://xa.example.com/scripts/ctxsta.dll
CSG_UseTwoTickets=Off
```

Access Gateway settings in the WebInterface.conf use the CSG prefix

The Citrix WI website is now complete and we are ready to turn our attention to the creation of our first basic logon point on the CAG, which will forward incoming client requests to this website.

Configuring an Access Gateway basic logon point

With the WI configuration implemented and the assumption that the XenApp and XenDesktop farms are already in place, we will create a CAG basic logon point to provide secure remote access to these and other web resources. To make use of a basic logon point, we must be in the initial grace period or have a valid platform license. We should remember that the platform license provides for 500 concurrent connections through the CAG into our server farms. We have already licensed our server, so we will drop straight back into CAG's web-based management console to create our first logon point.

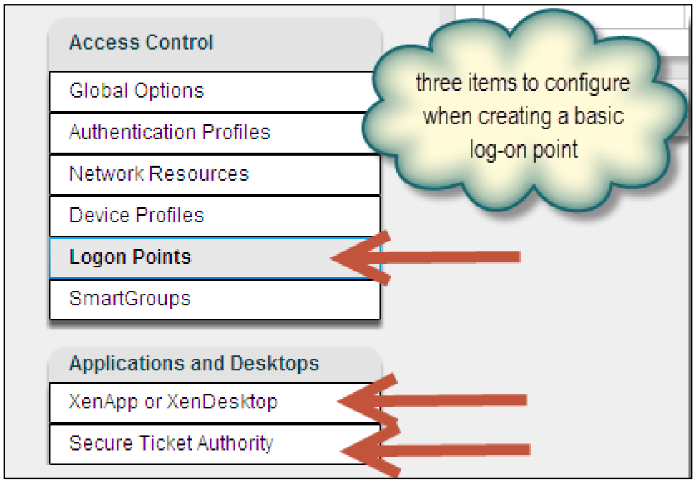
Go to `https://ag.example.com/lp/adminlogonpoint`.

We create logon points from the **Management** tab in the web-based management tool. There are three items to configure:

- **Logon Points**
- **XenApp or XenDesktop**
- **Secure Ticket Authority**

If we need to authenticate at the CAG, we are also required to create an authentication profile. For the moment, we can be happy to continue with the minimum requirements for the logon point.

We need to make three configurations for a basic logon point, as shown in the following screenshot:

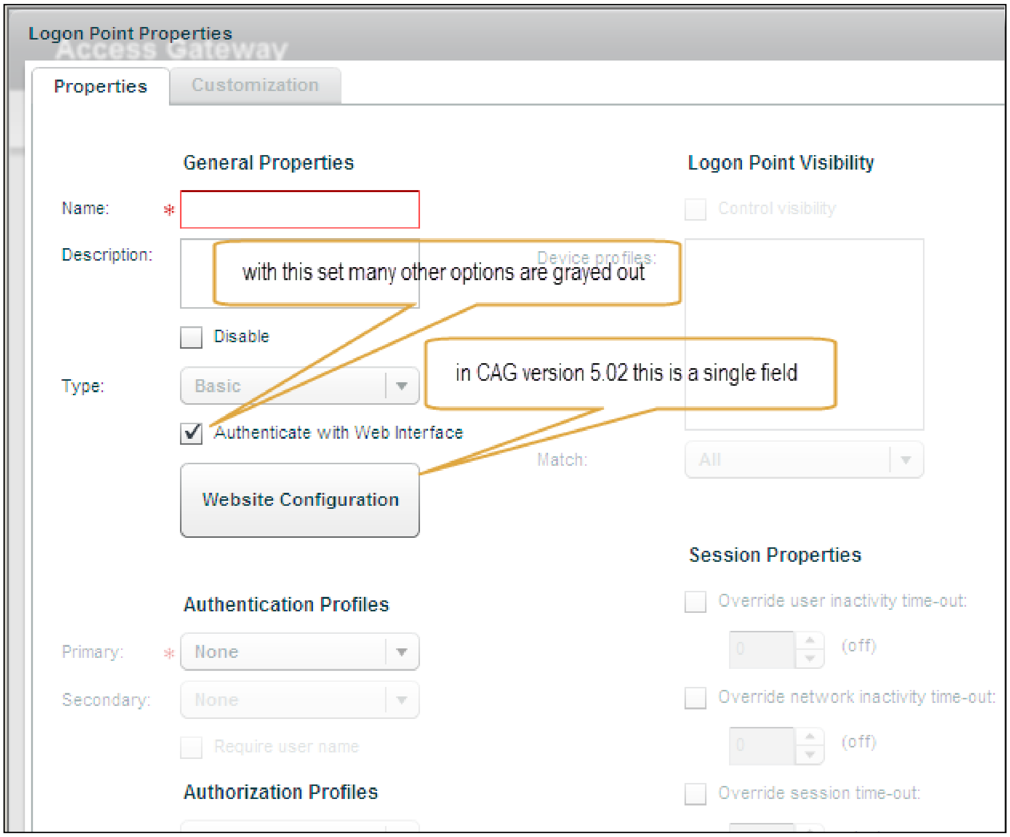


Logon point

When creating a new logon point, we choose between SmartAccess and basic. In this instance, we will be creating a basic logon point. Once we have selected the basic option from the logon point type drop-down, we will choose to authenticate with the WI. These options combine to reduce the options that are available to be configured (more options in SmartAccess).

> SmartAccess logon points allow full VPN access and basic access to ICA-Proxy, and, if we can recall; basic logon points use the platform licenses and SmartAccess additional universal licenses.

All we are required to do with this configuration (for a basic logon point) is to add the address of the WI server; however, in Version 5.04 of CAG that we are using for this book, multiple web servers can be included. The previous version only allowed for a single server to be added to a logon point. The following is the screenshot of the **Logon Point Properties** wizard:



with this set many other options are grayed out

in CAG version 5.02 this is a single field

We will set a logon point name; it is always good practice to keep logon points to a similar case (uppercase or lowercase and not both), as this will be used as part of the URL when accessing the logon point. A simple name of `cag` will suffice for our example. This would create the following URL:

```
https://ag.example.com/lp/cag
```

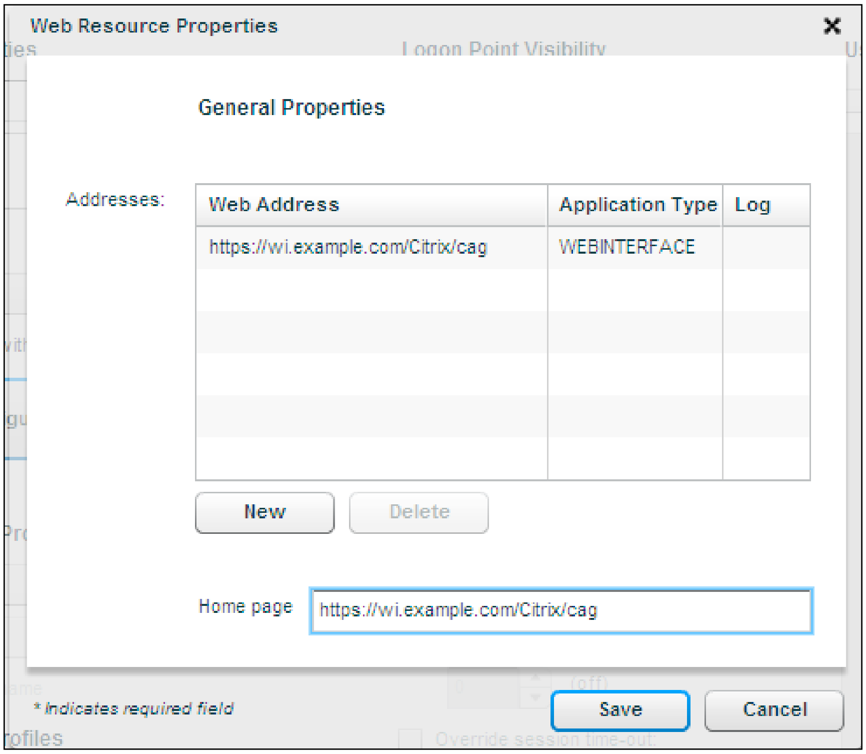
Moving on to the **Website Configuration** button, new to 5.04, we can add URLs for the WI site or sites we wish to use. Additionally, these web resources allow functionality for previously reserved SmartAccess logon points, allowing access to any website accessible to the CAG. These web pages could include the following:

- Intranet sites
- E-mail websites such as Outlook Web Access
- Citrix License Server

The importance of authenticating at CAG becomes heightened when accessing private resources on the internal network, without having been pre-authenticated by the CAG.

For the moment, we will keep the configuration simple and use the single URL for our WI website. Later in this chapter, we will add additional web resources.

The website URL needs to be entered twice – once as a web address and then as the home page. This instructs CAG to use the site as the default page for the logon point. Any web address added to the home page field must also have been added as a web address in the uppermost field. The following screenshot shows Website Configuration with a single WI site (using firmware 5.04):



Addresses:

Web Address	Application Type	Log
https://wi.example.com/Citrix/cag	WEBINTERFACE	

Home page: https://wi.example.com/Citrix/cag

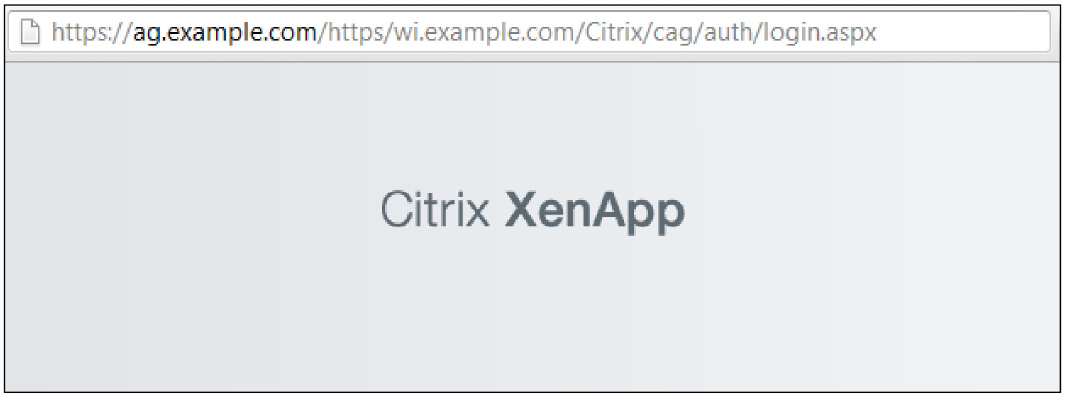
* Indicates required field

On saving the log point configuration, we will be warned that we have not, as yet, added any STAs. This we will complete very soon. With that said, and not wanting to disagree with Citrix, we can access the WI site at this stage, and just not authenticate beyond. So, at this point, let's pause and test the configuration so far, and prove that we do indeed have remote access to resources that are not normally accessible to Internet hosts. We will need to enter the full URL of the logon point on the CAG (we have not, as yet, configured a default site). Using our example site, we will use our web browser on the Internet to access the URL:

```
https://ag.example.com/lp/cag
```

We should then be directed to the Citrix WI site we configured earlier.

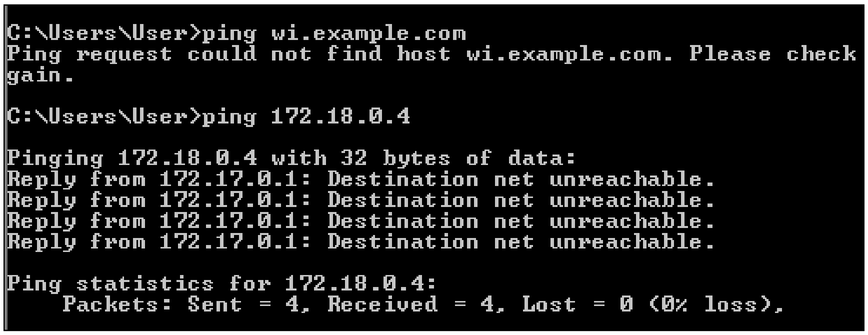
Access to the basic logon point will direct us to the configured WI site, as shown in the following screenshot:



https://ag.example.com/https/wi.example.com/Citrix/cag/auth/login.aspx

At this stage, we will not be able to authenticate, but we have proved the validity of the configuration so far. You may also like to access the WI website without using the CAG. The Citrix WI server is located on our private network and there is no route to it using either its DNS name or IP address. Access can only be achieved by using the CAG.

Accessing internal resources from the Internet is not possible without using CAG, as Internet hosts do not have routes to the private resources, as shown in the following screenshot:



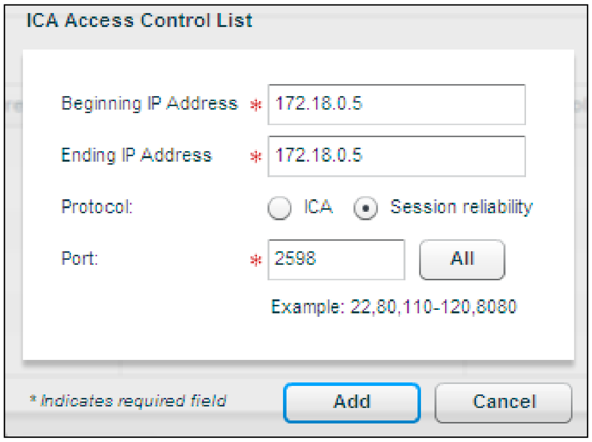
```
C:\Users\User>ping wi.example.com
Ping request could not find host wi.example.com. Please check
gain.

C:\Users\User>ping 172.18.0.4

Pinging 172.18.0.4 with 32 bytes of data:
Reply from 172.17.0.1: Destination net unreachable.
Reply from 172.17.0.1: Destination net unreachable.
Reply from 172.17.0.1: Destination net unreachable.
Reply from 172.17.0.1: Destination net unreachable.

Ping statistics for 172.18.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

XenApp and or XenDesktop access controls

You may remember that we had three configurations to make – the logon point, XenApp/Desktop access controls, and the STAs. Following the order in which they appear on the Management Console, we will now set the access control lists. In doing so, we will specify XenApp and XenDesktop machines that we will allow access to via this CAG. Clicking on XenApp or XenDesktop on the **Management** tab (**Applications and Desktops** section), we can add in destination IP addresses or address ranges that we would like to permit access to via the CAG connections. The addresses should include all the virtual desktops and XenApp servers that will be required for remote connections. This is simple in our example so far, as we only need to add in the single IP address for the XenApp server. We also need to select **Session Reliability** and port **2598**. This is not the default setting in the CAG, but session reliability is enabled by default in XenApp server farms.

Session Reliability was introduced with Citrix Presentation Server 4 and allows for auto-reconnection of sessions in the event of momentary network outages, such as those associated with cellular networking with mobile connections.

Adding the IP address or address ranges for your XenApp Servers is shown in the following screenshot:



ICA Access Control List

Beginning IP Address * 172.18.0.5

Ending IP Address * 172.18.0.5

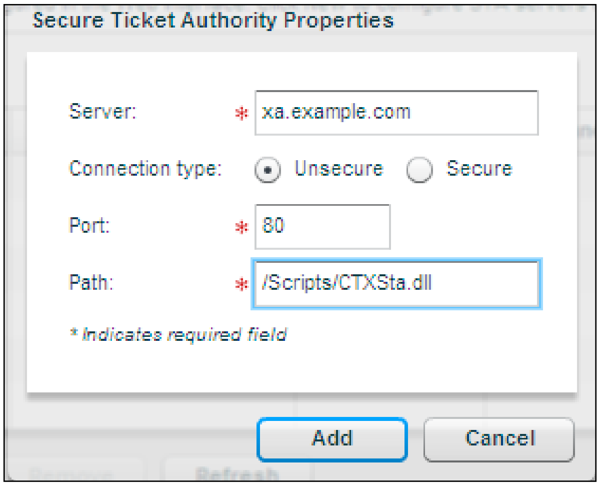
Protocol: ○ ICA ● Session reliability

Port: * 2598

Example: 22,80,110-120,8080

Secure Ticket Authority

When accessing a published application on XenApp servers or published desktops with XenDesktop users, both local and remote, are issued with access tokens, or as Citrix names them, secure tickets. These validate the authenticity of the connection and the resulting tickets exist for the duration of the user's session. The list of STAs, the issuing authorities, must match the list configured on the Citrix WI. In our example, we add just the single XenApp server and the connection type will be insecure, HTTP, as we have not configured certificates for the XenApp servers. The STA configuration is shown in the following screenshot:



Secure Ticket Authority Properties

Server: * xa.example.com

Connection type: ● Unsecure ○ Secure

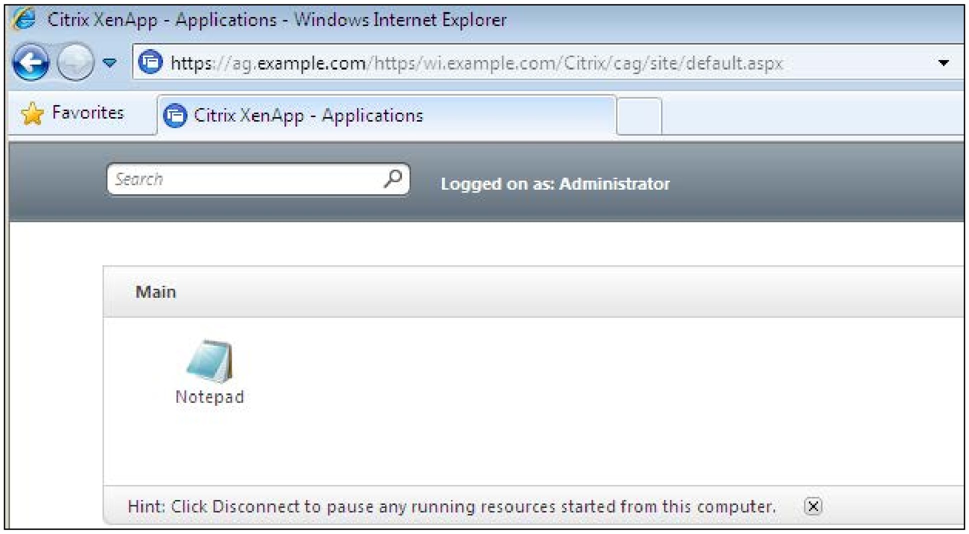
Port: * 80

Path: * /Scripts/CTXSta.dll

Accessing XenApp Server farms securely with the Citrix Access Gateway

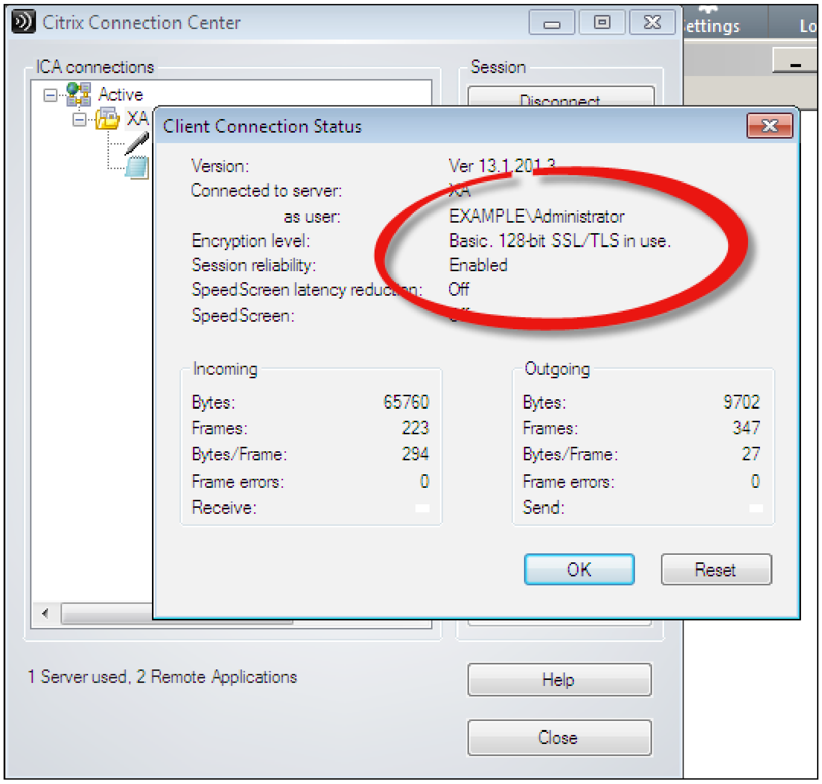
This completes the initial configuration of the basic logon point and we should now be free to connect into our published applications from the XenApp server farm. We will use the same URL and logon point as before, but we can now complete the logon process to see the published applications. You will see in the **EXAMPLE** farm that we have a notepad available as a published application (**Notepad**). I know it is a little like "Hello World", but you must allow me an easy life at times.

The view of published applications for XenApp when accessed through CAG from the Internet host is shown in the following screenshot:



Citrix XenApp - Applications - Windows Internet Explorer
https://ag.example.com/https/wi.example.com/Citrix/cag/site/default.aspx
Favorites
Citrix XenApp - Applications
Search
Logged on as: Administrator
Main
Notepad
Hint: Click Disconnect to pause any running resources started from this computer.

Moreover, we said that these would be secure connections. Passing through the CAG, we maintain SSL-encrypted traffic to and from CAG. This ensures the integrity of your data and applications as they pass through the Internet. Once we have initiated a connection to the published application, Citrix Receiver on the client PC will display the application and relay updates and keystrokes in the same way as a connection on local network to XenApp. The only difference is that these connections are passed through CAG. Using the Citrix connection center running from the client, we can view the properties of the connection once an application starts running. From here, we can see that the connection is protected with SSL and 128-bit encryption. The following is the screenshot of **Client Connection Status**:



Version: Ver 13.1.201.3
Connected to server: XA
as user: EXAMPLE\Administrator
Encryption level: Basic. 128-bit SSL/TLS in use.
Session reliability: Enabled
SpeedScreen latency reduction: Off
SpeedScreen: Off

Incoming		Outgoing	
Bytes:	65760	Bytes:	9702
Frames:	223	Frames:	347
Bytes/Frame:	294	Bytes/Frame:	27
Frame errors:	0	Frame errors:	0
Receive:		Send:	

Extending the basic logon point to access other internal web-based resources

We have achieved so much already in this chapter, but we do not want to finish just yet. The additional features of the CAG 5.04 enable us to connect to other website resources and not just to those of the WI server. These sites can allow, as already mentioned, access to internal webmail sites, License Server, and other intranet sites. In this next sub-section, we will add additional web resources to this basic logon point and utilize the cost-effective platform licenses to extend VPN access to internally-based HTTP/HTTPS resources.

We will start by returning to CAG web management console and edit the existing basic logon point, `cag`, and add web resources to the Website Configuration. Initially, we will add a welcome page to act as an intranet site and the URL for Citrix License Server, which you may remember, has its own web console listening on port 8082. Only web pages we add into the logon point can be accessed through CAG; so, importantly, we are not opening a hornet's nest of insecurity here. We will demonstrate the point by adding an additional link into the intranet site that points to the Certificate Authority running on our Windows domain controller. Access will fail until we allow access through the logon point configuration.

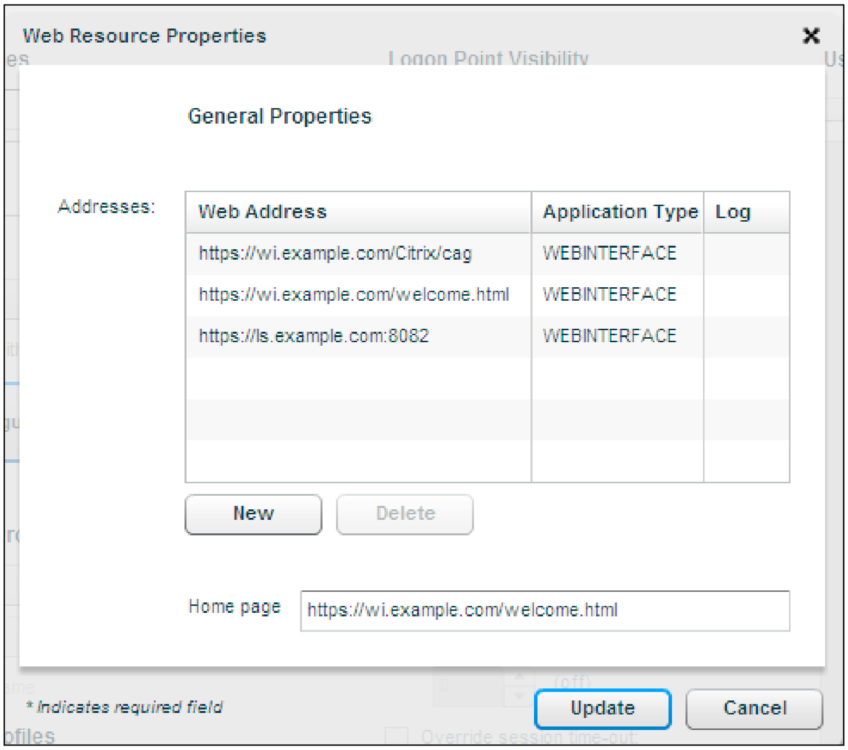
We will add a welcome page to the WI server by adding in an HTML page to the path `c:\inetpub\wwwroot`. This directory acts as a Windows IIS server default site. The page will be basic but will contain anchor links to our WI website, License Server, and CA. The example of HTML code is given to help understand the processes in place here:

```
<h1>Welcome to Example</h1>
<a href = https://wi.example.com/Citrix/cag>XenApp</a>
<a href = http://ls.example.com:8082>License</a>
<a href = https://8222dc.example.com/certsrv>CA</a>
```

So a very basic web page links to three resources; initially, we will not permit access to the CA, which is the bottom link on the page. The Website Configuration in the CAG 5.04 logon point will be edited to look similar to this page, excluding access to the Certificate Server.

> Note that the home page is now set to `welcome.html`, which is the intranet site we created on the WI server.

The updated Website Configuration, which is now excluding the CA website, is shown in the following screenshot:



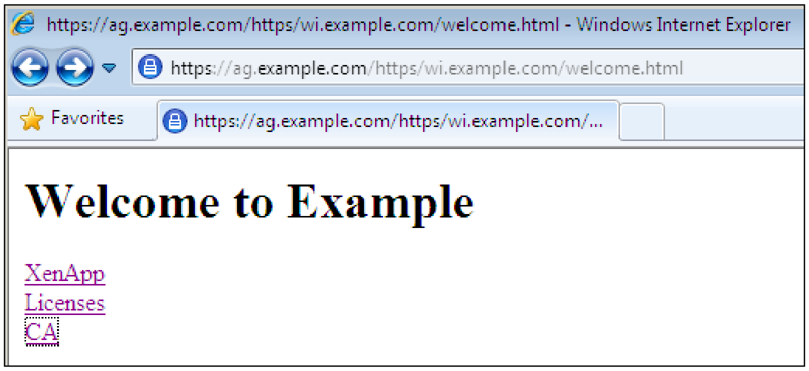
Addresses:

Web Address	Application Type	Log
https://wi.example.com/Citrix/cag	WEBINTERFACE	
https://wi.example.com/welcome.html	WEBINTERFACE	
https://ls.example.com:8082	WEBINTERFACE	

Home page: https://wi.example.com/welcome.html

As we have not allowed, as yet, access to the CA, we will be able to access all the links, except the CA, on the welcome page. Once the logon point is updated, we can access the original URL for the logon point; this does not change, only its targets have changed.

Accessing the updated basic logon point will now display the welcome page, as shown in the following screenshot:

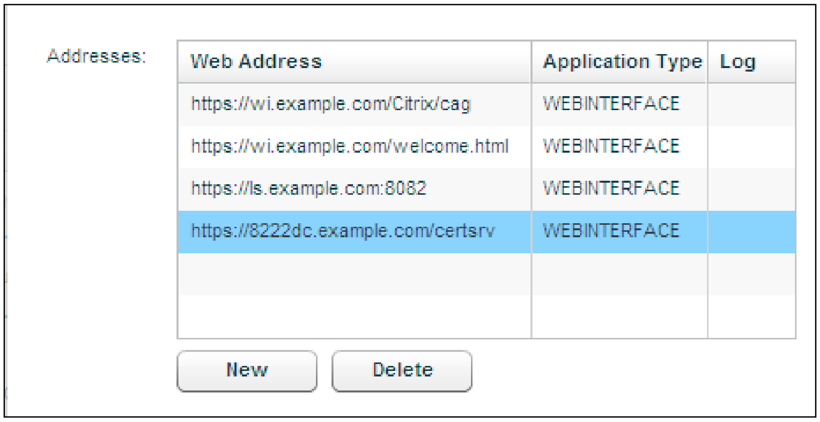

https://ag.example.com/https/wi.example.com/welcome.html - Windows Internet Explorer
https://ag.example.com/https/wi.example.com/welcome.html
Favorites
https://ag.example.com/https/wi.example.com/...

Welcome to Example

XenApp
Licenses
CA

When attempting to access the CA link, the browser will return standard messages saying that the website or domain could not be contacted. Having validated the security provided by excluding the site, we can return to the **Website Configuration** option within our logon point and add in the CA web resource, allowing access to this resource.

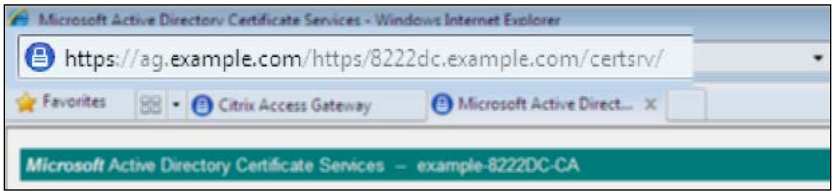
Now we add the CA site and we can see how the basic logon point should currently appear, as shown in the following screenshot:


Addresses:

Web Address	Application Type	Log
https://wi.example.com/Citrix/cag	WEBINTERFACE	
https://wi.example.com/welcome.html	WEBINTERFACE	
https://ls.example.com:8082	WEBINTERFACE	
https://8222dc.example.com/certsrv	WEBINTERFACE	

The final check to confirm the behavior of the basic logon point web proxy will be to ensure we have updated the logon point. The button is labeled as **Update**, but perhaps it would be more accurately labeled as save, as that is what it does. From the Internet client, we will access the logon point again, and this time we will have access to all the links on the welcome page.

With security in place, we can now access the CA through CAG, as shown in the following screenshot:


Microsoft Active Directory Certificate Services - Windows Internet Explorer
Favorites
Citrix Access Gateway
Microsoft Active Direct...

https://ag.example.com/https/8222dc.example.com/certsrv/

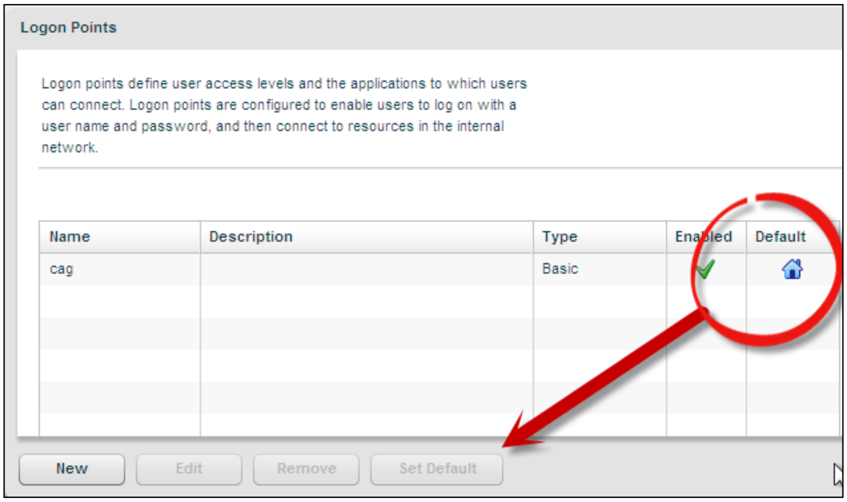
Microsoft Active Directory Certificate Services – example-8222DC-CA

Keeping your users happy

This is really important. I can imagine how ecstatic you are just now having configured this phenomenal remote access solution, but your users will be less happy. The logon point URL? Is that a 1p or an lp, ("one p" or "el p")? How many times have you told them that it is lp (lp for logon point)! User acceptance is so important in IT now. We have to mold IT around the users rather than molding our users around the IT infrastructure. So we should set a default logon point for the CAG; rather than accessing `https://ag.example.com/lp/cag`, we would simply enter `https://ag.example.com`.

We now have the user's euphoria to match our own happiness. This state is easily met by setting the logon point to be the default in the web console of CAG. Navigate back to the **Management** tab, and then down to **Logon Points**. Select the logon point, and then, with the logon point selected, choose **Set Default**.

Setting a logon point as default simplifies the URL. The configuration is shown in the following screenshot:



Logon points define user access levels and the applications to which users can connect. Logon points are configured to enable users to log on with a user name and password, and then connect to resources in the internal network.

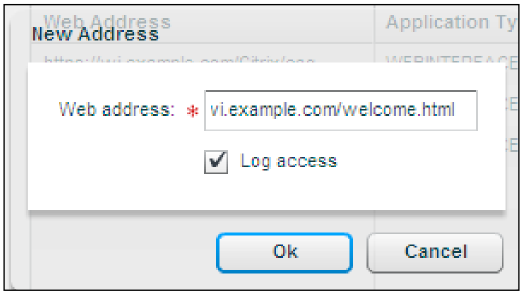
Name	Description	Type	Enabled	Default
cag		Basic	✓	⌂

So we have nirvana for our users, help desk calls are down, and we are in for a pay rise. Please take this moment to pat yourself on the back. There is one final task we must complete to keep the men in black happy (your security guys) and that is audit or log access to the CAG.

Auditing access to the Citrix Access Gateway

Yes, we can understand their point of view. If we sold this on the concept that CAG was a secure access system, it would then be reasonable to expect to be able to state which IP addresses and, possibly, which users have accessed the system. For each basic logon point—web resource that we create—at the time of creation, we can tick the **Log access** checkbox. This will then record the access in the **Audit Log**, accessible from the **Monitor** tab.

Enable logging for a web resource if you would like to audit access, as shown in the following screenshot:

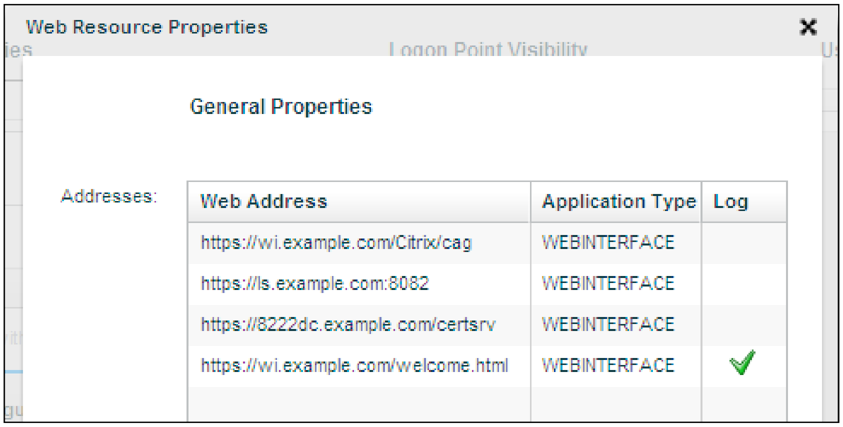


Web address: * vi.example.com/welcome.html

☑ Log access

Once this has been set, we can identify which resources have been enabled for logging as they are marked with a big green tick. We have chosen to log access just to the entry page – `welcome.html`. To view these logs, navigate to the **Monitor** tab and **Audit Log** hyperlink at the bottom of the page.

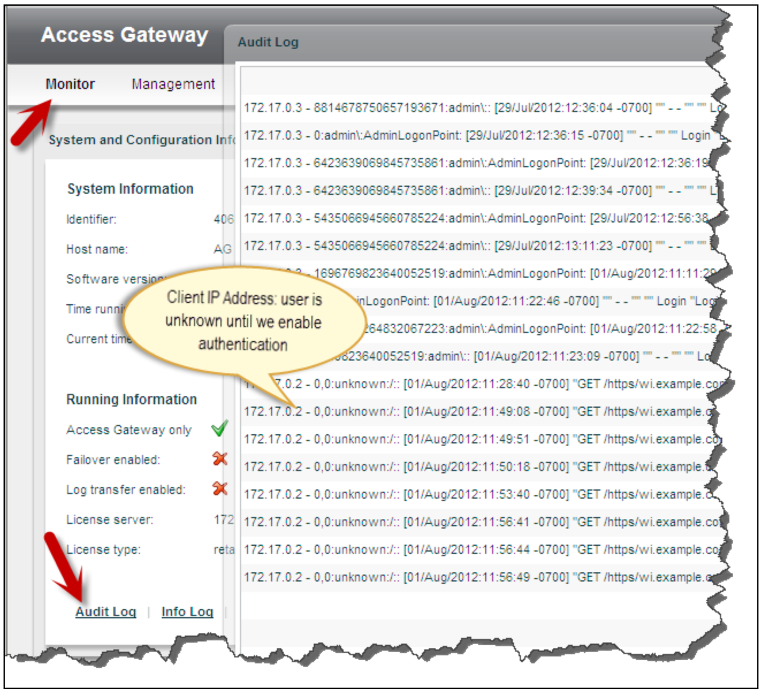
Once logging is set, we can see that the resource is marked with a tick, so we can easily note that access to this resource is audited.



Addresses:

Web Address	Application Type	Log
https://wi.example.com/Citrix/cag	WEBINTERFACE	
https://ls.example.com:8082	WEBINTERFACE	
https://8222dc.example.com/certsrv	WEBINTERFACE	
https://wi.example.com/welcome.html	WEBINTERFACE	✓

Viewing the logs from the **Audit Log** hyperlink will enable us to see the IP address of the user devices that accessed logged resources. Also, adding user authentication will allow for the username to show. This has not yet been enabled, but will be in later chapters; for now, we can view the graphic and notice that access was made from the client with the IP address of `172.17.0.2`:



Access Gateway
Audit Log
Monitor
Management
System and Configuration Info
Client IP Address: user is unknown until we enable authentication
Audit Log
Info Log

System Information
Identifier: 406
Host name: AG
Software version
Time runni
Current time

Running Information
Access Gateway only ✓
Failover enabled: ✗
Log transfer enabled: ✗
License server: 172
License type: reta

```
172.17.0.3 - 8814678750657193671:admin\:: [29/Jul/2012:12:36:04 -0700] "" - - "" "" Lo
172.17.0.3 - 0:admin\:AdminLogonPoint: [29/Jul/2012:12:36:15 -0700] "" - - "" "" Login
172.17.0.3 - 6423639069845735861:admin\:AdminLogonPoint: [29/Jul/2012:12:36:19
172.17.0.3 - 6423639069845735861:admin\:: [29/Jul/2012:12:39:34 -0700] "" - - "" "" L
172.17.0.3 - 5435066945660785224:admin\:AdminLogonPoint: [29/Jul/2012:12:56:38
172.17.0.3 - 5435066945660785224:admin\:: [29/Jul/2012:13:11:23 -0700] "" - - "" ""
         - 1696769823640052519:admin\:AdminLogonPoint: [01/Aug/2012:11:11:29
                    inLogonPoint: [01/Aug/2012:11:22:46 -0700] "" - - "" "" Login "Log
                    264832067223:admin\:AdminLogonPoint: [01/Aug/2012:11:22:58
                    9823640052519:admin\:: [01/Aug/2012:11:23:09 -0700] "" - - "" "" Lo
17  7.0.2 - 0,0:unknown:/:: [01/Aug/2012:11:28:40 -0700] "GET /https/wi.example.co
172.17.0.2 - 0,0:unknown:/:: [01/Aug/2012:11:49:08 -0700] "GET /https/wi.example.c
172.17.0.2 - 0,0:unknown:/:: [01/Aug/2012:11:49:51 -0700] "GET /https/wi.example.co
172.17.0.2 - 0,0:unknown:/:: [01/Aug/2012:11:50:18 -0700] "GET /https/wi.example.
172.17.0.2 - 0,0:unknown:/:: [01/Aug/2012:11:53:40 -0700] "GET /https/wi.example.c
172.17.0.2 - 0,0:unknown:/:: [01/Aug/2012:11:56:41 -0700] "GET /https/wi.example.co
172.17.0.2 - 0,0:unknown:/:: [01/Aug/2012:11:56:44 -0700] "GET /https/wi.example.co
172.17.0.2 - 0,0:unknown:/:: [01/Aug/2012:11:56:49 -0700] "GET /https/wi.example.c
```

Summary

In this chapter, we have created a basic logon point to allow secure access to remote users, enabling access to web resources, and XenApp/XenDesktop farms. You have been introduced to Secure Ticket Authorities, XenApp, and XenDesktop Access control lists, as well as the basic logon point. These are all configured on CAG, but we have to make sure we have configured the WI site to work correctly with CAG and ICA proxy.

One of the weaknesses in the deployment so far is the reliance on the WI server for authentication. This is certainly sub-optimal. In order to correct this, the next chapter will show the use in adding authentication profiles to allow users to be authenticated directly on the CAG.

5
Creating Authentication Profiles

We learnt in the previous chapter that deploying CAG and authenticating at the Web Interface was a weak security option, especially when deployed to a basic logon point that accesses multiple internal web pages. I don't know about you, but that criticism is still stinging me and we have to resolve this. In this chapter, we will require traffic to be authenticated at CAG, before passing it through to our private internal network. We will look at the following topics:

- Authentication profiles
- Creating RADIUS authentication profiles
- Creating RSA SecurID authentication profiles
- Creating LDAP authentication profiles in Microsoft Active Directory
- Using Windows authentication with just the username
- Using the userPrincipalName for multi-tenant Windows systems
- Creating LDAP authentication profiles in Novell eDirectory
- Creating LDAP authentication profiles in Linux openLDAP
- Customizing the CAG logon page
- Allowing users to reset their passwords using CAG
- Implementing two-factor authentication

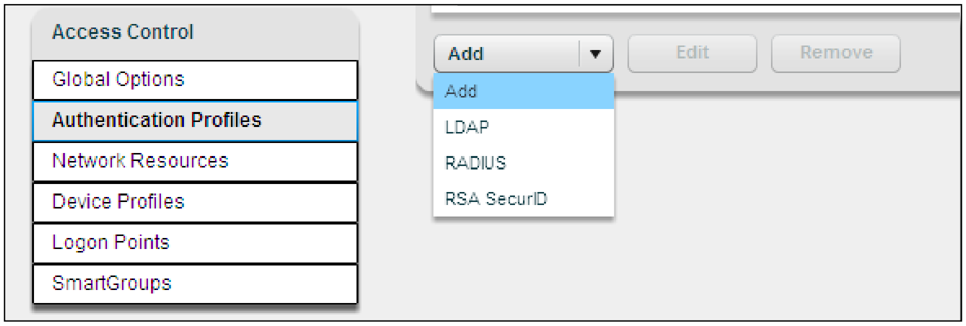
Authentication profiles

Authentication profiles on CAG reference our user sources or identity vaults and allow for authentication to take place at CAG itself, thus protecting against unauthenticated traffic passing onto our resource hosts. The following authentication profiles are flexible to meet your organizational needs that are being able to authenticate:

- **LDAP**
- **RADIUS**
- **RSA SecurID**

Of course, **LDAP** allows further access to common directory services such as Microsoft's Active Directory and Novell's eDirectory.

Authentication profiles can be created to suit your organizational needs, as shown in the following screenshot:



Authentication can be singled to two factors; using one or two profiles. With two-factor authentication, we may need to authenticate to an **LDAP** profile and then enter an **RSA SecurID** pin. The added security with two-factor authentication makes for a popular choice in many organizations.

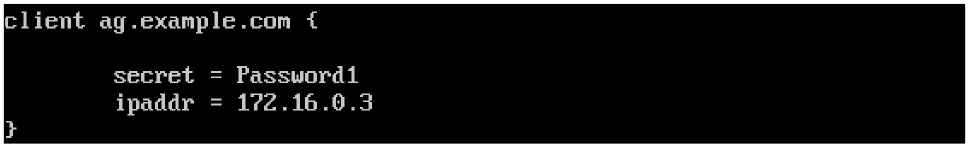
Creating a RADIUS authentication profile

Perhaps we should start off with one of the original remote authentication protocols, **Remote Access Dial In User Service** (**RADIUS**). You may have started with this, decades ago; perhaps at the same time you were resetting user passwords. You can implement the RADIUS server as an independent hardware appliance or as a software service for Microsoft Windows 2003, 2008 server, or Linux. For the purpose of this book, we will look at utilizing the Open Source and free version of FreeRadius, installing this on an openSUSE Linux. Linux can be free, secure, and does not always need to consume the resources that other operating systems may require. FreeRadius is available for many Linux distributions. We will use openSUSE, but the configuration options remain consistent, as they are product-specific and not distribution-specific. On openSUSE, we can install FreeRadius from the command line with the following command:

```
zypper in freeradius-server
```

On other distributions, the `zypper` command may be yum or apt-get; this just being the command used to access the software installation repositories or stores.

Once installed, we can make some basic configuration settings. Firstly, we add CAG as an authorized client to the RADIUS server. This is in the `/etc/raddb/clients.conf` file. The following is the screenshot of a sample entry for `clients.conf`:



```
client ag.example.com {

        secret = Password1
        ipaddr = 172.16.0.3
}
```

From the sample in the screenshot, we can add an entry similar to the following to allow access to the RADIUS server from CAG. We restrict access to the IP address used by CAG and the secret represents the common pass-phrase or shared-secret that must be entered both here, on the RADIUS server, and in the configuration of the CAG authentication profile. One would hope that the length of your shared-secret is more complex and longer than the demonstration used here:

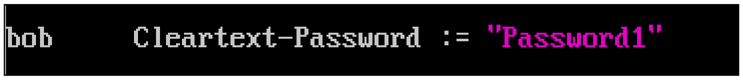
```
client ag.example.com {
  secret = Password1
  ipaddress = 172.16.0.3
}
```

This entry in the `clients.conf` command defines the parameters used by CAG when accessing the RADIUS server.

Next, still on the RADIUS server, we add user entries. These represent users who are allowed to authenticate to this RADIUS server and in the simplest form have just the username and password. These are added to the `/etc/raddb/users` file.

```
bob  Cleartext-Password := Password1
```

The previous entry would create a user account named `bob` with the password of `Password1`. Following is the screenshot of a sample `/etc/raddb/users` entry for the user `bob`:



```
bob     Cleartext-Password := "Password1"
```

Once the configurations are in place, we need to start the service and make sure that the service will auto-start on booting the Linux server:

```
service freeradius start
chkconfig -a freeradius
```

With this complete, we are ready on to move to the CAG configurations, but let's make sure we are happy with the RADIUS configuration:

- `/etc/raddb/clients.conf` – authorizes CAG
- `/etc/raddb/users` – configures users access

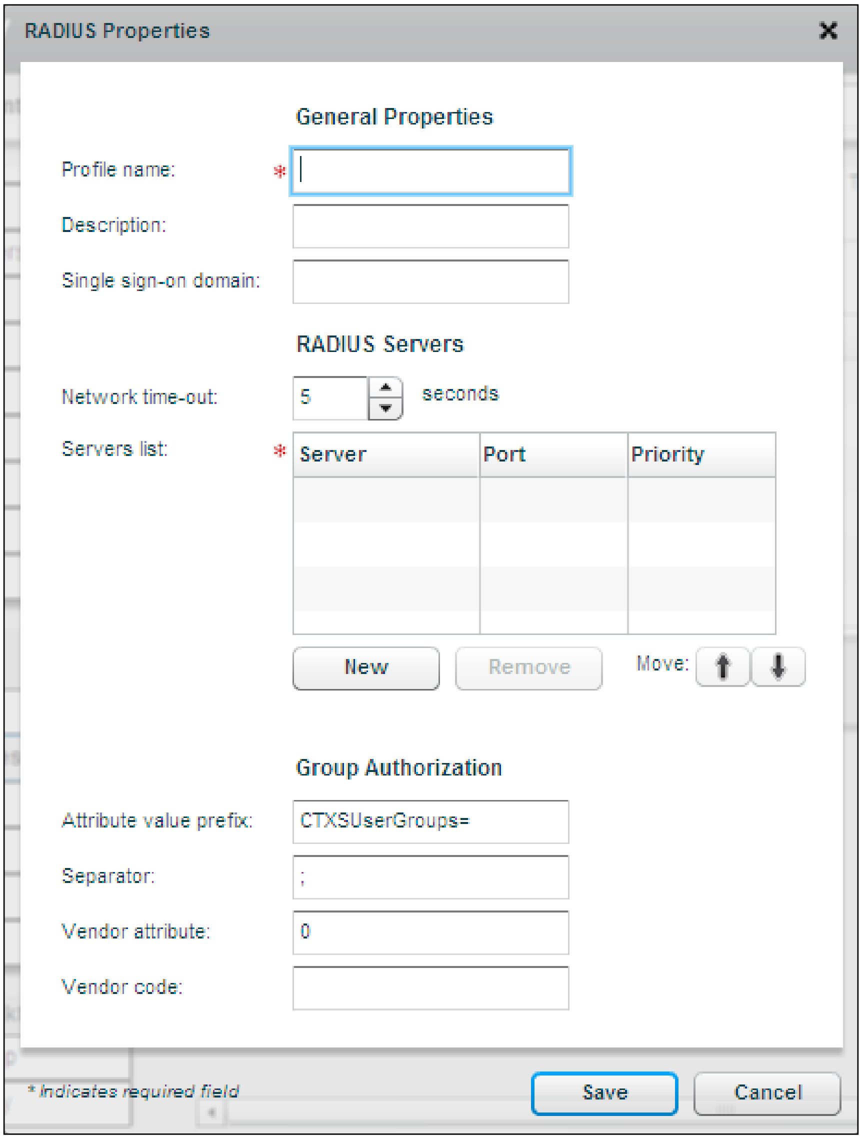
> RADIUS uses port 1812 over UDP or TCP to make sure these are accessible through the firewall from the DMZ.

Without any further delay, we shall move onto the configuration of the authentication profile using the web-based management console of CAG.

From the usual location of the **Management** tab, we can navigate to **Access Control** and **Authentication Profiles**. From the **Add** drop-down list, we can see that it is possible to create the three profile types:

- **LDAP**
- **RADIUS**
- **SecurID**

We will choose **RADIUS**. The **RADIUS Properties** page will now open and from here we can define the connection to the user source, as shown in the following screenshot:



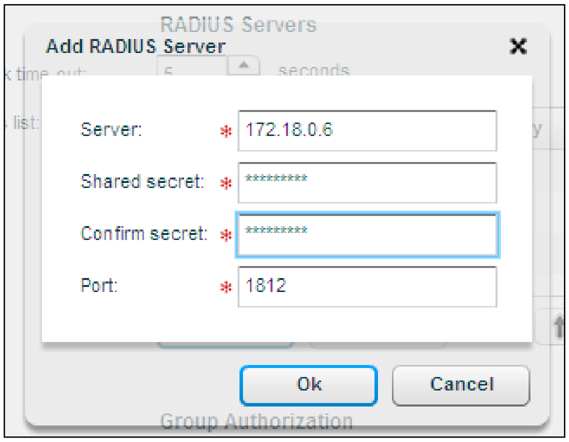
Network time-out: 5 seconds

Attribute value prefix: CTXSUserGroups=

Separator: ;

Vendor attribute: 0

The **Profile name** and **Description** textboxes should be self-explanatory; we do not have to fill in the single-sign on domain field, but we would need to if we needed our users to authenticate at CAG and have those credentials used to access the Web Interface server. We will set this to **EXAMPLE**, the Active Directory domain we use for the book. We will add our **FreeRadius** server into the server list. The following is the screenshot of **Add RADIUS Server**:



Add RADIUS Server

Server: * 172.18.0.6

Shared secret: * *********

Confirm secret: * *********

Port: * 1812

For each **RADIUS** profile that you use for authentication, you can configure up to three RADIUS servers. If the primary RADIUS server is unavailable, CAG attempts to authenticate against the other RADIUS servers for that profile in the order in which they appear in the list.

If you are using Gemalto Protiva or SafeWord servers for authentication, you configure these servers using RADIUS.

Configuring Gemalto Protiva

Protiva is a strong authentication platform that Gemalto developed to use the strengths of Gemalto's smart card authentication. With Protiva, users log on with a username, password and a one-time password that the Protiva device generates. Similar to RSA SecurID, the authentication request is sent to the Protiva authentication service and the server validates the password. You can use the following guidelines when configuring Protiva:

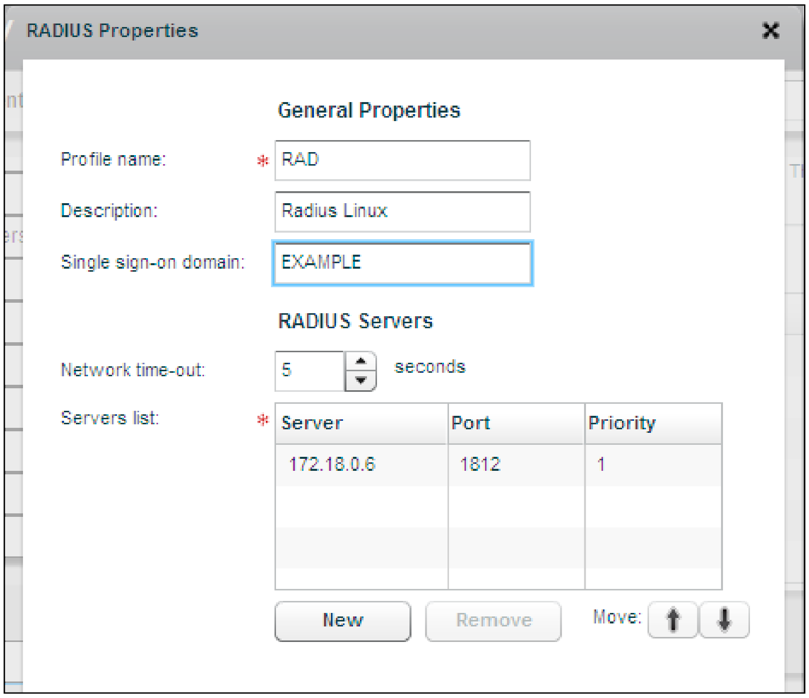
- Install the Protiva server
- Install the Protiva SAS Agent Software; this extends the functionality of the Microsoft IAS and RADIUS server
- Configure a RADIUS authentication profile on CAG and enter the settings of your Protiva server

Configuring SafeWord

The SafeWord product line provides secure authentication using a token-based passcode. After the user enters the passcode, SafeWord immediately invalidates the passcode and it cannot be used again. When you configure the SafeWord server, you need the following information:

- The IP address of CAG
- A shared secret as with any RADIUS server
- The IP address and port of the SafeWord server; the default port number is the standard RADIUS port – 1812

For our current configuration, we do not look at group authorization; this would require SmartAccess logon points, which we will cover later in this book in *Chapter 10, SmartAcess logon points*. Our executed properties for the Linux RADIUS authentication profile should be similar to this once ready. The following is the screenshot of **RADIUS Properties**:



General Properties

Profile name: * RAD

Description: Radius Linux

Single sign-on domain: EXAMPLE

RADIUS Servers

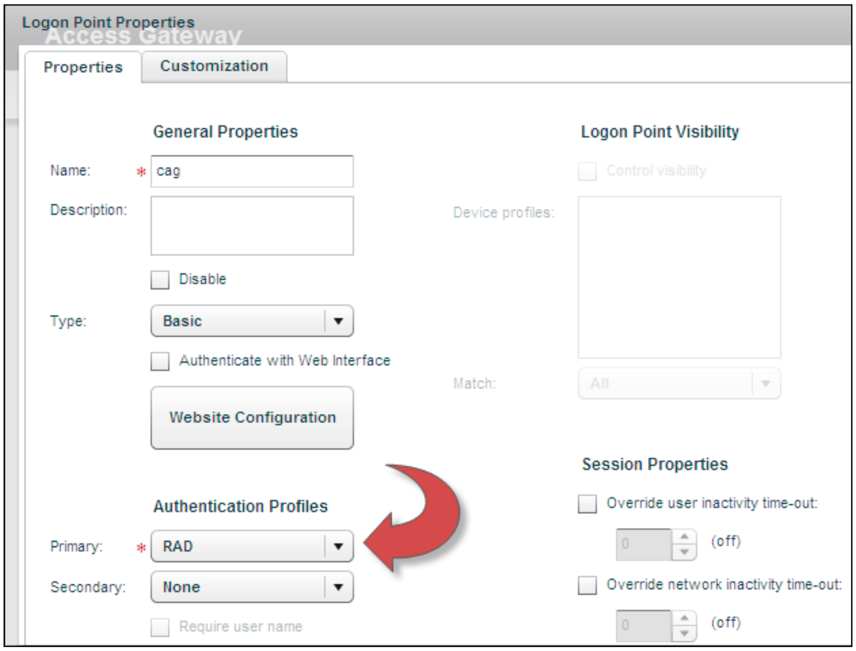
Network time-out: 5 seconds

Servers list: *

Server	Port	Priority
172.18.0.6	1812	1

Now we have an authentication profile that we can reference from our logon point. Authentication then takes place before we are directed to the welcome page or whichever other web resource we wish to point to. We can add in two authentication profiles – primary and secondary. If we add a secondary profile, we then have two-factor authentication.

We can see in the following screenshot that our basic logon point now includes authentication at CAG:



Name: * cag

Description:

□ Disable

Type: Basic

□ Authenticate with Web Interface

Primary: * RAD

Secondary: None

□ Require user name

□ Control visibility

Match: All

□ Override user inactivity time-out: 0 (off)

□ Override network inactivity time-out: 0 (off)

Creating RSA SecurID authentication profiles

Now that we have the RADIUS profile done and dusted, things should be pretty easy from now on; just more of the same. If your organization uses RSA ACE/Server or RSA Authentication Manager and RSA SecurID for authentication, you will configure the CAG to authenticate user access with the RSA server. The CAG acts as an RSA Agent Host, authenticating our users.

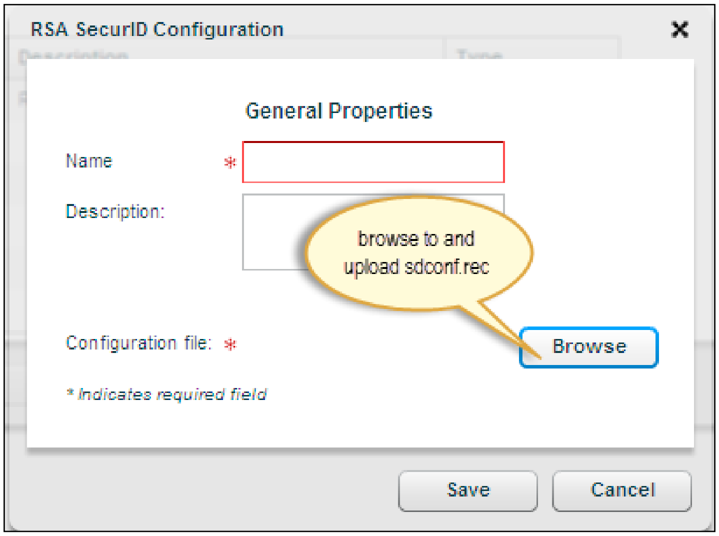
CAG supports the following versions of RSA servers:

- RSA ACE/Server Version 5.2 and higher
- RSA Authentication Manager Versions 6.1 and 7.1

The only configuration needed for the RSA SecurID authentication profile is to generate and upload a file called `sdconf.re`. When generating this file, use the following guidelines:

1. Create an Agent Host of type UNIX.
2. Configure Net OS Agent to identify the CAG. If the gateway has two interfaces, use the internal IP address.
3. If you configure two CAG appliances for appliance failover, use the internal virtual IP address.
4. When you are creating the Agent Host, make sure that the **Node Secret Created** checkbox on the RSA server is cleared. The RSA server sends the Node Secret to CAG the first time that the software authenticates a request from CAG. After that, the **Node Secret Created** checkbox is selected. By clearing the checkbox and generating and uploading a new configuration file you can force the RSA server to send a new Node Secret to CAG.
5. You can indicate which users can be authenticated through CAG in the following ways:
   1. Configure CAG as an open Agent Host that is open to all locally known users.
   2. Select the users to be authenticated by editing the Agent Host and selecting the users to be activated.

From the following screenshot, we can see that we need to browse to and upload the `sdconf.rec` file to the CAG:

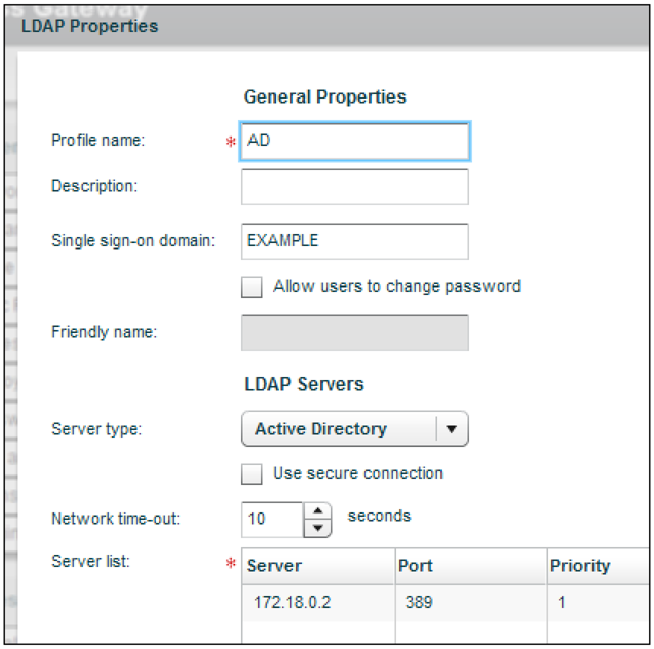

RSA SecurID Configuration
General Properties
Name *
Description:
browse to and upload sdconf.rec
Configuration file: *
Browse
* Indicates required field
Save
Cancel

Creating LDAP authentication profiles in Microsoft's Active Directory

Of course, many of us will work in organizations that use Microsoft's Active Directory as their identity solution. The AD is an LDAP-based directory and we can connect using secure LDAPS on TCP port 636, or less secure connections using the default LDAP and TCP port 389. We have not set up LDAPS, so we will use LDAP connections in our corporate AD for the time being; however, if we want users to change their passwords using CAG, LDAPS is required. LDAPS is not enabled in the Active Directory by default; however, we can enable it using the Certificate MMC on a Domain Controller and running through a certificate request wizard. We will enable this later in this chapter.

- **LDAP**: TCP port 389
- **LDAPS**: TCP port 636

The following is the screenshot of the Active Directory authentication profile:



LDAP Properties

General Properties

Profile name: * AD

Description:

Single sign-on domain: EXAMPLE

□ Allow users to change password

Friendly name:

LDAP Servers

Server type: Active Directory

□ Use secure connection

Network time-out: 10 seconds

Server list: *

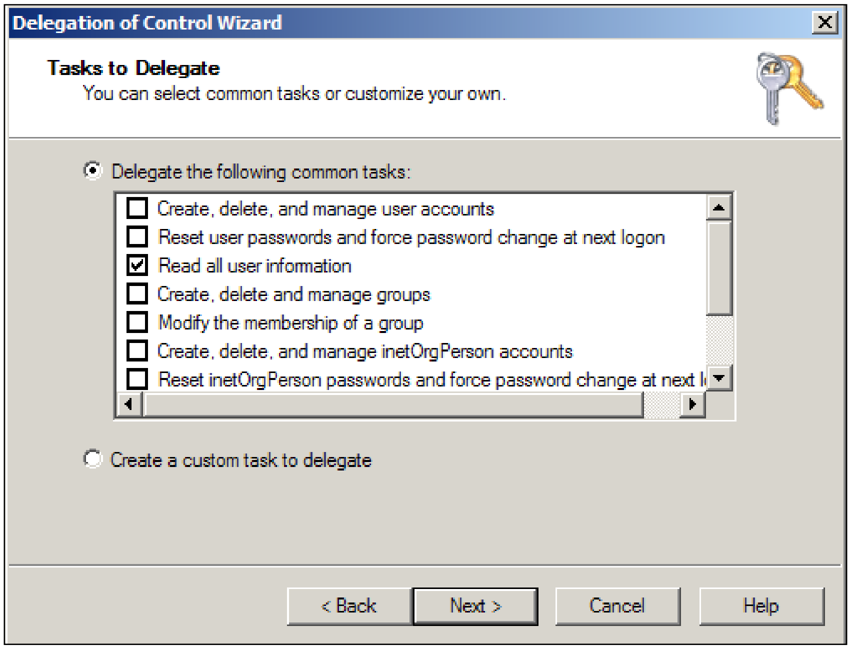
Server	Port	Priority
172.18.0.2	389	1

Looking at the **LDAP Properties** page, we again set the **Profile name** and **Description** textboxes as required. For the moment, we will not worry about users being able to change their passwords. From the **Server type** drop-down dialog, we will choose **Active Directory**. The checkbox **Use secure connections** would toggle between LDAP and LDAPS and port 389 and 636. The server list will again allow for three domain controllers to be added and they are accessed in the order they appear in the list.

> Now the important bit – create an account in the Active Directory for the CAG.

On the right-hand side of the page, we see **Bind Properties**. These are the details that are used by the CAG when accessing Active Directory. The **Administrator DN** textbox is a little misleading. This should be a user account that has read all the user information to the container structure that your users are located in. For us, this is simple; all of our users are in the `Users` folder of the Active Directory. We have created a user called `_LDAP` and delegated control of this folder with the appropriate permissions. Do not use an account that has full administrative rights to the directory. This is not required and would potentially be insecure.

Create an account for CAG to use in the Active Directory and delegate permissions, as shown in the following screenshot:


Delegation of Control Wizard

Tasks to Delegate
You can select common tasks or customize your own.

● Delegate the following common tasks:

☐ Create, delete, and manage user accounts
☐ Reset user passwords and force password change at next logon
☑ Read all user information
☐ Create, delete and manage groups
☐ Modify the membership of a group
☐ Create, delete, and manage inetOrgPerson accounts
☐ Reset inetOrgPerson passwords and force password change at next l

○ Create a custom task to delegate

For the Active Directory **Administrator DN** (distinguished name), we can choose to write it in one of two ways:

- `_LDAP@example.com`
- `cn=_LDAP,cn=users,dc=example,dc=com`

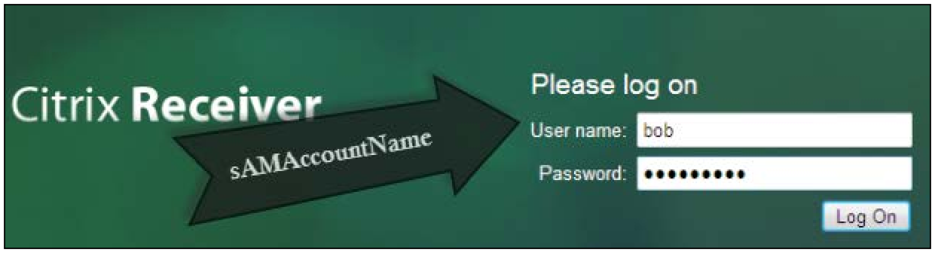
> Note that the LDAP format includes a comma separating the list of objects.

The **Base DN** textbox, where to search, can only be written in the full LDAP format; in our case, we look for users in the default user folder – `cn=users,dc=example,dc=com`.

The LDAP authorization, like the RADIUS authorization, is not used on basic logon points but we can leave it at the default settings. With this set and saved, we have now created an authentication profile for Active Directory. If we wanted to, we could, as before, associate this with the logon point to test authentication.

Authentication using the Active Directory sAMAccountName

When using the Active Directory from Microsoft as the authentication source for your profile, we must specify the attribute or user property that we will use to identify the user. The default is the **sAMAccountName** property, to you and me; more simply, we would see this as the user's login name. This is usually sufficient, as this attribute is unique within the domain.

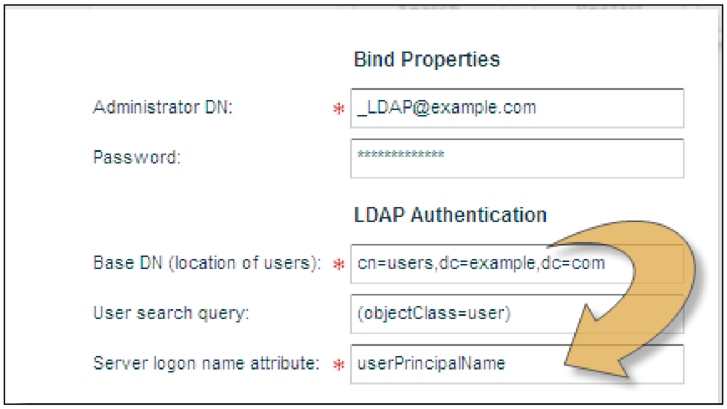


User name: bob
Password: •••••••••

Authenticating using the Active Directory userPrincipalName

If more than the single domain is used, either within an Active Directory forest or implementing a multi-tenanted system with Active Directory Federation Services, the `userPrincipalName` attribute can be used. This is formatted similar to an e-mail address and for our user – `bob`, the UPN would be `bob@example.com`. The attribute to use is changed in the **Authentication Profile** properties. Viewing the **Bind Properties** wizard, we see that we utilize the `userPrincipalName` attribute rather than the default `sAMAccountName` attribute.

> Note that attribute names are case sensitive.



Bind Properties

Administrator DN: * _LDAP@example.com

Password: *************

LDAP Authentication

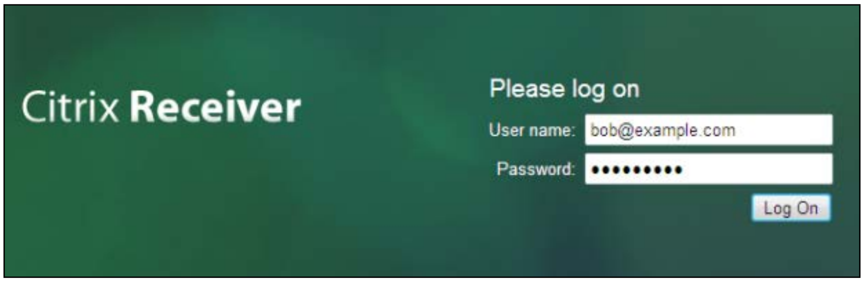
Base DN (location of users): * cn=users,dc=example,dc=com

User search query: (objectClass=user)

Server logon name attribute: * userPrincipalName

With this set, users now authenticate at the CAG using their UPN, which is often the same as their e-mail address.

We can now see how `bob` would have to authenticate using his UPN from the following screenshot:



Please log on

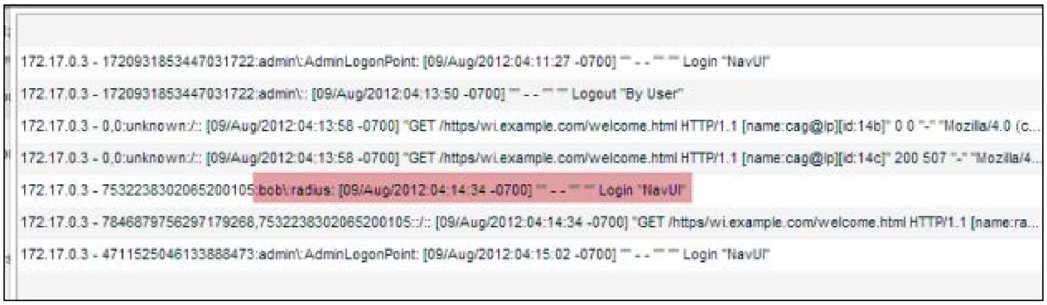
User name: bob@example.com

Password: ●●●●●●●●●

Tracking user access

No matter which form of user authentication (RADIUS, RSA, or LDAP), we are now able to track and audit user access through basic logon points. You may recall that if we select to log access in a web resource property, using the **Monitor** page and the **Audit Log** hyperlink, we can view access to those resources for which logging is enabled. The user account used now shows the IP address that we have viewed previously. From the following screenshot, we can see that the user bob is accessing the radius logon point, (bob\:radius).

The user's name now is logged when we view the audit log on the server, as shown in the following screenshot:



```
172.17.0.3 - 1720931853447031722:admin\:AdminLogonPoint: [09/Aug/2012:04:11:27 -0700] "" - - "" "" Login "NavUI"
172.17.0.3 - 1720931853447031722:admin\:: [09/Aug/2012:04:13:50 -0700] "" - - "" "" Logout "By User"
172.17.0.3 - 0,0:unknown:/:: [09/Aug/2012:04:13:58 -0700] "GET /https/wi.example.com/welcome.html HTTP/1.1 [name:cag@ip][id:14b]" 0 0 "-" "Mozilla/4.0 (c...
172.17.0.3 - 0,0:unknown:/:: [09/Aug/2012:04:13:58 -0700] "GET /https/wi.example.com/welcome.html HTTP/1.1 [name:cag@ip][id:14c]" 200 507 "-" "Mozilla/4...
172.17.0.3 - 7532238302065200105:bob\:radius: [09/Aug/2012:04:14:34 -0700] "" - - "" "" Login "NavUI"
172.17.0.3 - 7846879756297179268,7532238302065200105::/:: [09/Aug/2012:04:14:34 -0700] "GET /https/wi.example.com/welcome.html HTTP/1.1 [name:ra...
172.17.0.3 - 4711525046133888473:admin\:AdminLogonPoint: [09/Aug/2012:04:15:02 -0700] "" - - "" "" Login "NavUI"
```

Creating LDAP authentication profiles in Novell's eDirectory Directory

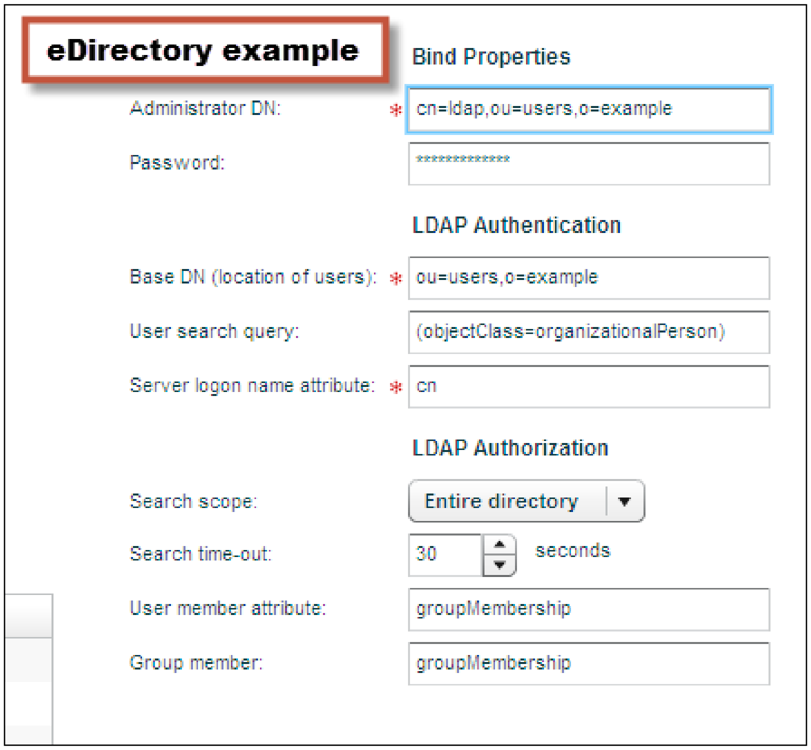
Another commonly implemented identity solution within the corporate IT market is the eDirectory from Novell. The CAG supports authentication directly to eDirectory. The LDAP DN format for the eDirectory is still comma separated; do not get confused with Novell's own dot separator. LDAP names are always comma delimited.

The **Administrator DN** field would be written as cn=ldap,ou=users,o=example.

The **Base DN (location of users)** textbox would be written as ou=users,o=example.

The attribute used for authentication, the **Server logon name attribute** textbox, would be written as CN.

The following is the screenshot of a Novell eDirectory example authentication profile:



eDirectory example

Bind Properties

Administrator DN: * cn=ldap,ou=users,o=example

Password: **************

LDAP Authentication

Base DN (location of users): * ou=users,o=example

User search query: (objectClass=organizationalPerson)

Server logon name attribute: * cn

LDAP Authorization

Search scope: Entire directory ▼

Search time-out: 30 seconds

User member attribute: groupMembership

Group member: groupMembership

Creating LDAP authentication profiles to Linux openLDAP

You may implement your identity solution within Linux and openLDAP. For this, we would select LDAP and other as the authentication profile types. Choosing other will require us to complete all fields.

The **Administrator DN** textbox would be written as `uid=ldap,ou=people,dc=example,dc=com`.

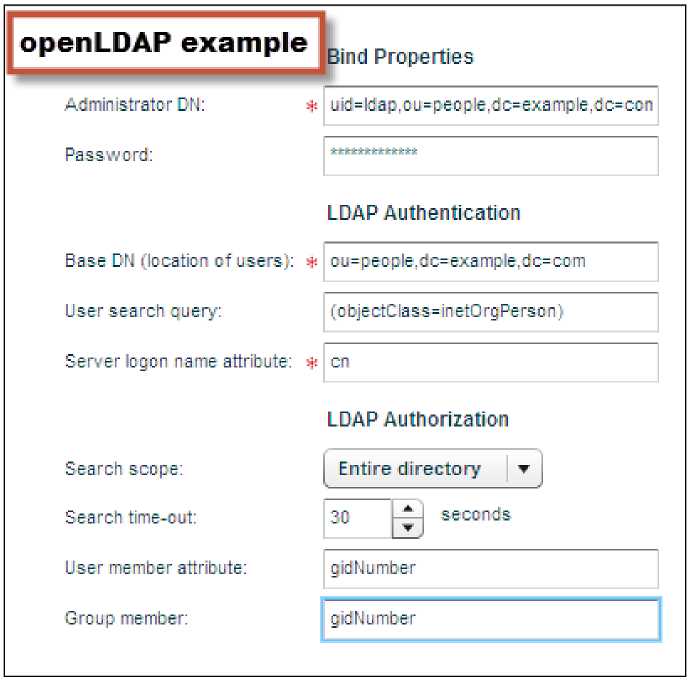
The **Base DN** textbox would be written as `ou=people,dc=example,dc=com`.

The **User search query** textbox would be written as `(objectClass=inetOrgPerson)`.

The attribute used for authentication, the **Server logon name attribute** textbox, would be written as `UID`.

Even though we are not looking at the authorization currently, we would set the **User member attribute** and **Group member** textboxes to `gidNumber`.

The following is the screenshot of an openLDAP authentication profile:



Bind Properties

Administrator DN: * uid=ldap,ou=people,dc=example,dc=con

Password: *************

LDAP Authentication

Base DN (location of users): * ou=people,dc=example,dc=com

User search query: (objectClass=inetOrgPerson)

Server logon name attribute: * cn

LDAP Authorization

Search scope: Entire directory

Search time-out: 30 seconds

User member attribute: gidNumber

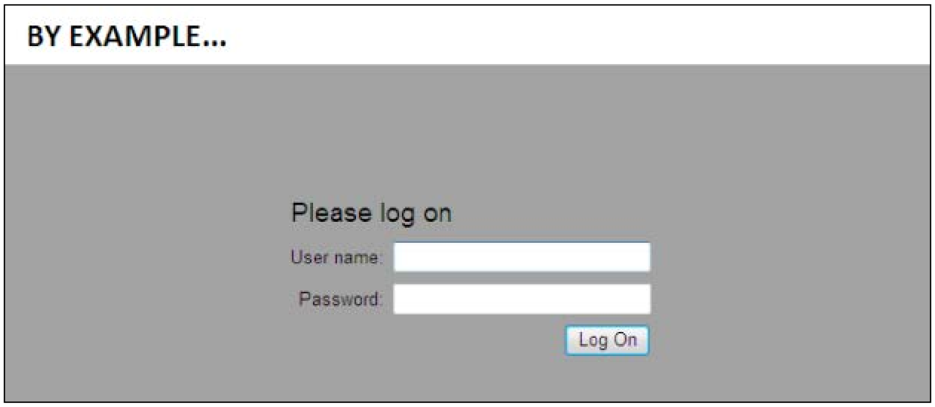
Group member: gidNumber

Customizing the Citrix Access Gateway logon page

So we have been able to configure authentication profiles and have seen how to use them with the basic logon points. With the CAG 5.04 firmware, we are able to customize the appearance of the logon page from the default. Your design can include a header, footer, and main content.

For our logon page, we have included a header logo on a white background and the content area with a gray background and no footer. Citrix provide templates, the Receiver Green, which is the default in 5.04, and the Citrix Default, which is used on the admin logon point and is the only logon page previous to Version 5.04.

Viewing our new custom logon page with CAG 5.04, with our color scheme and logo, is shown in the following screenshot:



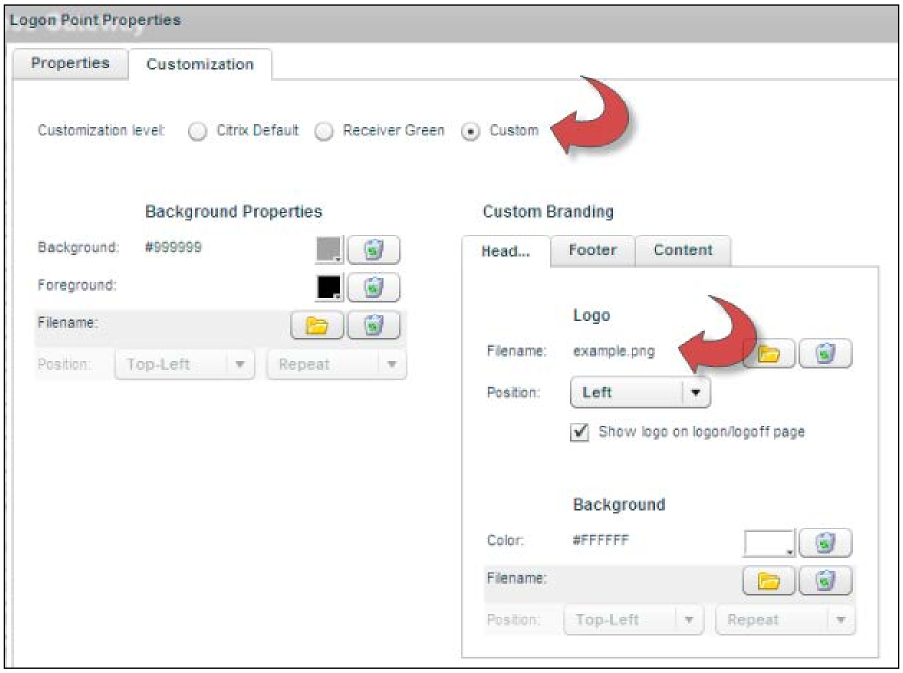
BY EXAMPLE...

Please log on

User name:

Password:

To change the theme of the logon page, we edit the logon point. From the **Logon Point Properties** page, we can find the **Customization** tab using Version 5.04 of the CAG firmware. Once here, it is a simple matter of setting properties for the background, header, footer, and content areas of the logon page. We have used our **BY EXAMPLE...** logo, `example.png`, for the header. The following is the screenshot of the **Customization** wizard:



Logon Point Properties

Customization level: ○ Citrix Default ○ Receiver Green ● Custom

Background Properties

Background: #999999

Foreground:

Filename:

Position: Top-Left Repeat

Custom Branding

Logo

Filename: example.png

Position: Left

☑ Show logo on logon/logoff page

Background

Color: #FFFFFF

Filename:

Position: Top-Left Repeat

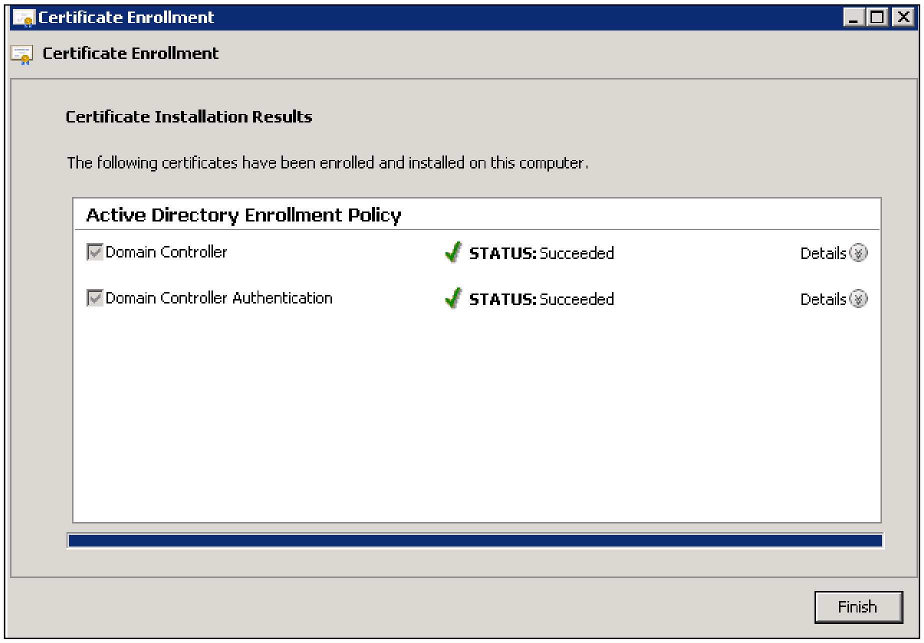
Remember that effective branding of your site can improve the user acceptance with the familiarity that it provides. Do not discount the importance of this and, if necessary, liaise with your marketing team for logos and advice on which colors to use.

Allowing users to change passwords on the logon page

Another major item that we will need to discuss here is user passwords. I know, a horrible phrase that reminds us of those long days resetting passwords in our early careers. User's passwords should expire and they should be changing them regularly. Some users may only ever access resources remotely through the CAG and have no other mechanism to change their password.

If we are using Active Directory, we first have to make sure that your Domain Controllers have certificates assigned to the LDAP service. This can be achieved by running the certificate enrollment wizard on each Domain Controller from the Certificates MMC and the Domain Controller and Domain Controller Authentication.

Note that you do have to have an Enterprise Certificate Authority installed into the Active Directory Domain. The following is the screenshot of the **Certificate Enrollment** wizard:



Certificate Installation Results

The following certificates have been enrolled and installed on this computer.

Active Directory Enrollment Policy

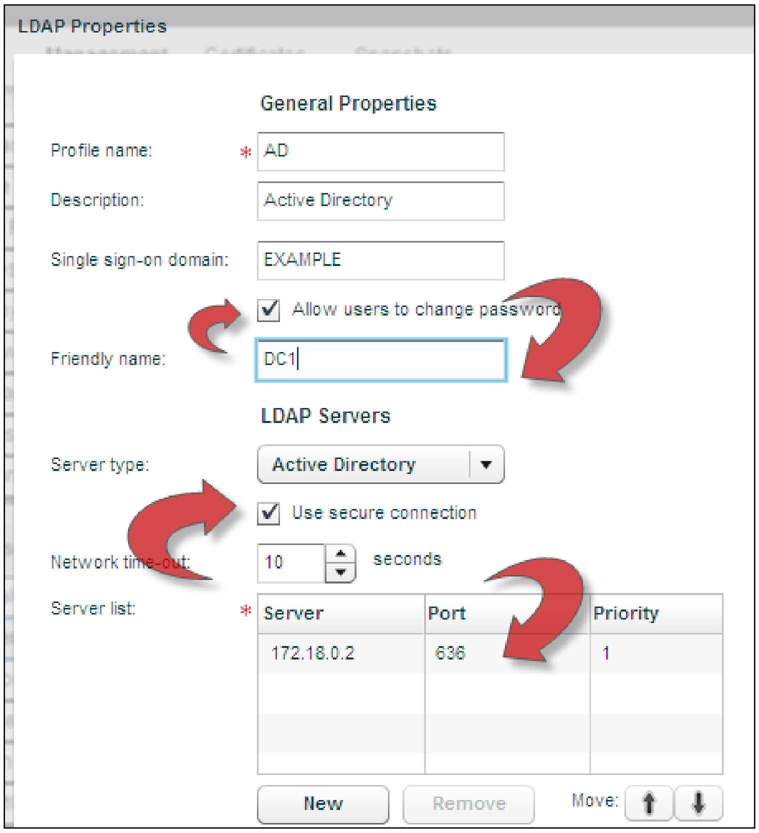
☑ Domain Controller ✓ STATUS: Succeeded Details

☑ Domain Controller Authentication ✓ STATUS: Succeeded Details

With this completed, we can then return to the properties of our authentication profile. We need to have the certificates in place as when using the Active Directory, LDAPS must be used to change passwords with the CAG. From the **Authentication Profile Properties** dialog, we implement these four changes:

- Allow users to change passwords
- Friendly name (if the server name is shown to the users during the password change)
- Use secure connection
- Re-add servers with port 636 in place of 389

Now that we have enabled LDAPS, we can switch to using secure connections to our Active Directory, as shown in the following screenshot:



LDAP Properties

General Properties

Profile name: * AD

Description: Active Directory

Single sign-on domain: EXAMPLE

☑ Allow users to change password

Friendly name: DC1

LDAP Servers

Server type: Active Directory

☑ Use secure connection

Network time-out: 10 seconds

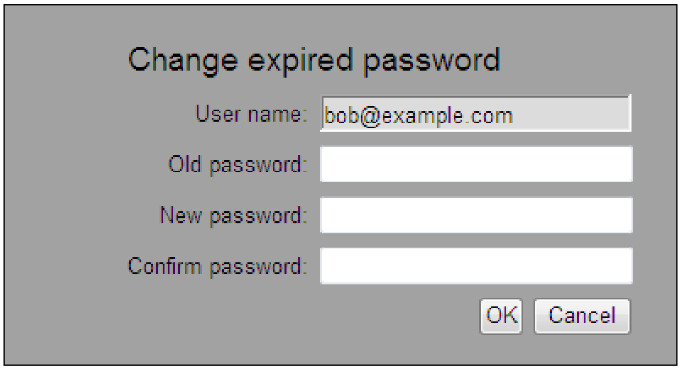
Server list: *

Server	Port	Priority
172.18.0.2	636	1

The CAG must have the Certificate Authority's public key stored on the server to make these connections. We already implemented this during the initial configuration of the CAG, as our CAG has its own certificates signed by the Active Directory CA. If yours used another CA, then import the CA's certificate from the **Certificates** tab of CAG.

If a user's password has expired, they will be first prompted for the original password to identify themselves. Once this is completed, they are shown the password-change dialog.

The CAG password-change dialog is shown in the following screenshot:



Change expired password

User name: bob@example.com

Old password:

New password:

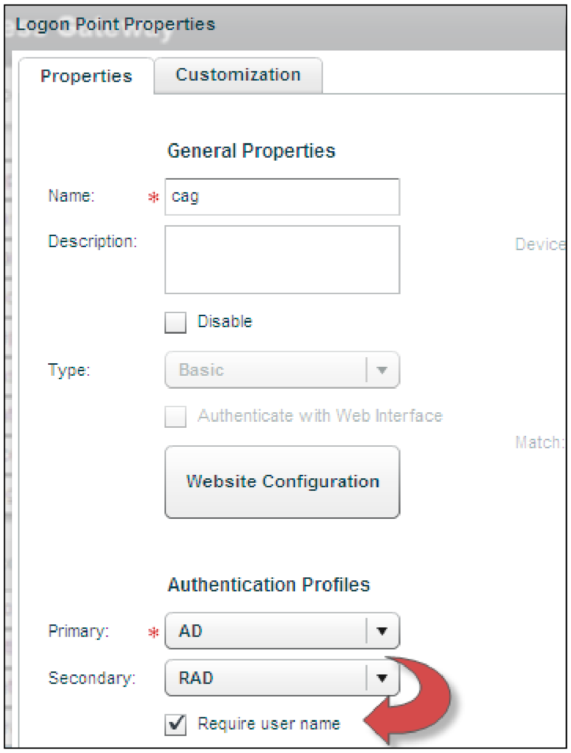
Confirm password:

So we have completed another major step in configuring the CAG for corporate access. Not only have we added security by authenticating at CAG, we now are able to access Microsoft's Active Directory securely with LDAPS and allow users to change their passwords. Our final configuration for this chapter will be to set two-factor authentication.

Implementing two-factor authentication on the Citrix Access Gateway

We have already discussed adding in two authentication profiles to a basic logon point – a primary and a secondary. As soon as a second authentication profile is added to a logon point, you have the choice to select the **Require user name** checkbox. This needs to be selected if the username used in one authentication profile will be different in the other. For example, using the `sAMAccountName` attribute in Windows will allow the username `bob` to be the same on both Windows and our RADIUS solution; however, by using the `userPrincipalName` attribute, we will have `bob@example.com` in Active Directory and `bob` in RADIUS.

We will set **Require user name** when two-factor authentication is used and account names will differ in each authentication source, such as in the following screenshot with Active Directory and Radius:



Name: * cag

Description:

□ Disable

Type: Basic

□ Authenticate with Web Interface

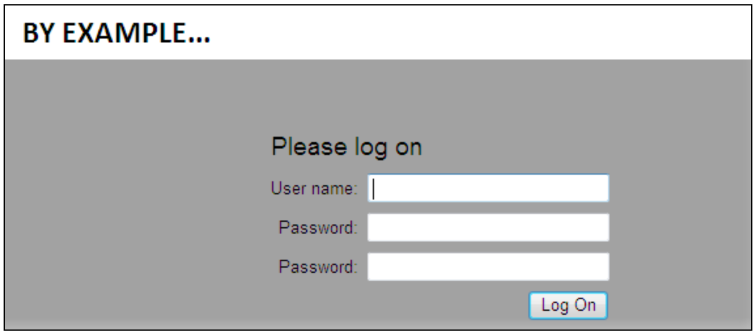
Primary: * AD

Secondary: RAD

☑ Require user name

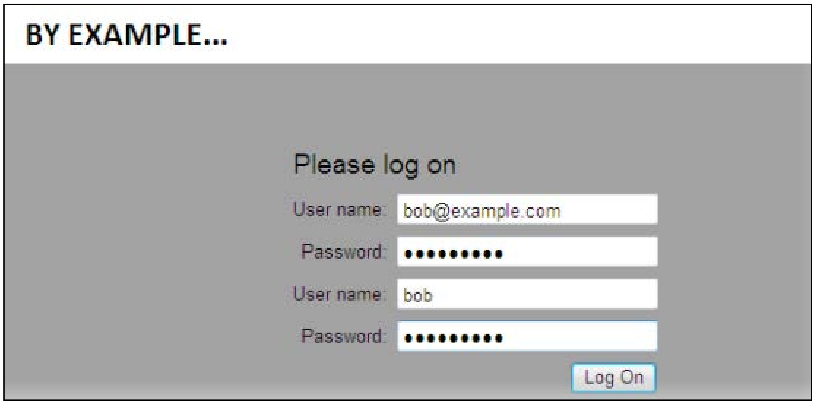
If the usernames were the same in both the primary and secondary profile, then we can leave this deselected.

Without **Require user name** set, we have the opportunity to insert just the one username and the name must be the same in both authentication sources:



With the option set, where the usernames differ, the dialog would be similar but, yes, it will have two username fields:

From the following screenshot, we can see how our trusty user bob would have to authenticate using his UPN and RADIUS login names:



BY EXAMPLE...

Please log on

User name: bob@example.com

Password: ●●●●●●●●●

User name: bob

Password: ●●●●●●●●●

Summary

In this chapter, we have secured our remote access solution further by requiring authentication at the CAG by implementing LDAP and RADIUS authentication profiles. To help user acceptance, we have branded the logon pages and allowed passwords to be changed at CAG.

In the next chapter, we will move on from basic logon points and start to discover what is available when we implement SmartAccess logon points and universal licenses. The era of full virtual private networks is upon us!

6
Beyond the Basics

In this chapter, we go beyond the basic logon points we have created so far and venture into the realms of SmartAccess login points, investigating what becomes available with the use of universal licenses. Not only can we connect to XenApp and XenDesktop, but we will now have full VPN access to internal resources such as internal e-mail, intranets, and file shares. Integrate into this a little endpoint analysis to check the health of end user devices and we have ourselves one heck of a VPN solution. Of course, we will take this little by little and piece by piece in this book; you will get a great understanding and thorough look at the options available.

During this chapter, I will have set up SmartAccess logon points, so we can see what becomes available. We will look in more detail later how these are created. In this chapter, we will start with:

- Adding universal licenses
- CAG plug-in installation
- Integrating the plug-in with the Citrix Receiver
- Using the Citrix Merchandising Server to distribute plug-ins to the client

Adding universal licenses

Previously, in *Chapter 2*, *Licensing the Citrix Access Gateway*, we added the platform license but not the universal licenses. A valid platform license is required for each CAG that is running and this allows for up to 500 concurrent connections through basic logon points. This may be all our organization requires; establishing connections to XenApp or XenDesktop will give us connections to other resources such as network shares in the network. The downside of this solution is that we will be using XenApp or XenDesktop licenses to gain that VPN access.

If we want VPN access independently of XenApp or XenDesktop, then the Citrix solution becomes SmartAccess logon points. We begin our adventure with these in this chapter and we will need universal as well as platform licenses installed onto License Server.

> The platform license is always required, as this license not only licenses the basic logon points but also licenses CAG itself.

Universal licenses are concurrent user licenses. If we have platinum licenses for Citrix XenApp, then these also include universal licenses. Adding the XenApp platinum licenses will also add the same amount of concurrent user universal licenses for use with CAG. So if we add 350 concurrent XenApp platinum licenses, we gain 350 concurrent universal licenses.

However you obtain the universal licenses, they need to be added to License Server. We can import them to License Server using the URL, `http://ls.example.com:8082` in readiness for the new logon points.

> Even though we can gain access to our internal network using XenApp or XenDesktop connections through the basic logon points, we are not able to run any endpoint analysis without SmartAccess logon points.

Feel free to review *Chapter 2*, *Licensing the Citrix Access Gateway* if you need a reminder on how licenses are imported to License Server.

Citrix Access Gateway plug-in installation

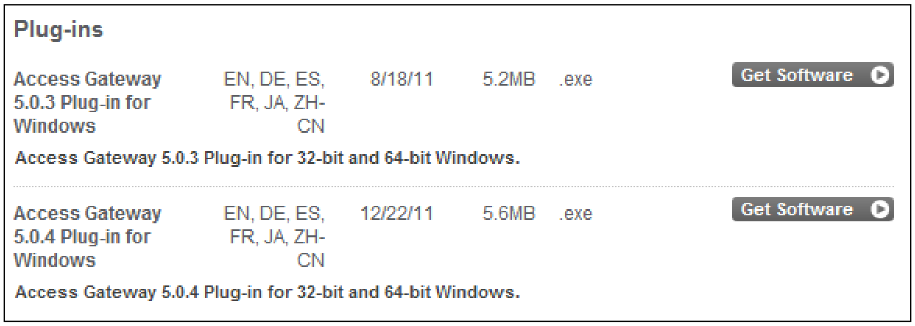
SmartAccess login points offer access to more resources and, moreover, they are able to allow access based on properties of the computers or user groups. To make use of these features, we will need the CAG plug-in installed on our client devices. The plug-in is not needed for a basic login point, but is required for SmartAccess points; think of the plug-in as your VPN client.

Obtaining the plug-in

In the simplest form, we can download the plug-in from the Citrix website, or we can use other methods to distribute this. Currently, the plug-ins are available for MAC OSX 10.5/10.6 and Windows clients from XP SP3. The CAG plug-in establishes a network-layer connection (virtual private network) between a user device and CAG. Network traffic is analyzed and intercepted on the user device and redirected as required to CAG. It is then the job of CAG to terminate the SSL VPN and authorize the traffic before forwarding packets to the intended target on the secure internal network.

To obtain the plug-in:

- Download it from the following Citrix website: `http://citrix.com/downloads/netscaler-access-gateway/plug-ins.html`



Plug-ins

Access Gateway 5.0.3 Plug-in for Windows	EN, DE, ES, FR, JA, ZH-CN	8/18/11	5.2MB	.exe	Get Software
Access Gateway 5.0.3 Plug-in for 32-bit and 64-bit Windows.					
Access Gateway 5.0.4 Plug-in for Windows	EN, DE, ES, FR, JA, ZH-CN	12/22/11	5.6MB	.exe	Get Software
Access Gateway 5.0.4 Plug-in for 32-bit and 64-bit Windows.					

- Download from CAG
- Push out to the client from the Citrix Merchandising Server, electronic software distribution platform

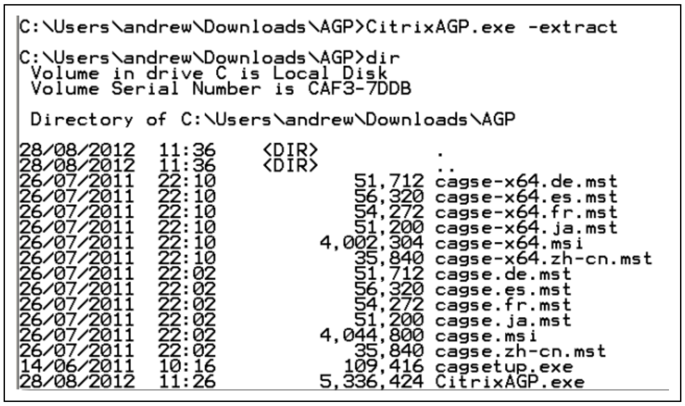
Installing the plug-in

Having downloaded the plug-in from the website, it will be named as `CitrixAGP.exe`. This Windows package does contain an MSI, but we would need to first extract it. The `.exe`, in itself, is fine if we are to install just on the single client. But if we want to integrate the CAG plug-in as part of our standard laptop build or distribute it with our own corporate electronic software distribution system such as Microsoft's SCCM 2012, then having the native MSI is a better idea.

To extract the MSI and MST answer files from the downloaded executable, type `CitrixAGP.exe -extract`.

The files extract into the folder that it is runs from, so it is a good idea to add the file to its own empty folder before you start extracting.

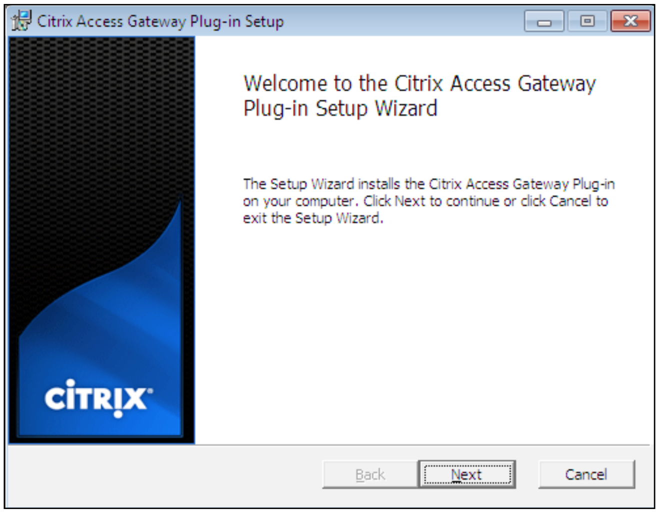
If you want to use the MSI as part of your standard build, then extract the files first, as shown in the following screenshot:



```
C:\Users\andrew\Downloads\AGP>CitrixAGP.exe -extract

C:\Users\andrew\Downloads\AGP>dir
 Volume in drive C is Local Disk
 Volume Serial Number is CAF3-7DDB

 Directory of C:\Users\andrew\Downloads\AGP

28/08/2012  11:36    <DIR>          .
28/08/2012  11:36    <DIR>          ..
26/07/2011  22:10            51,712 cagse-x64.de.mst
26/07/2011  22:10            56,320 cagse-x64.es.mst
26/07/2011  22:10            54,272 cagse-x64.fr.mst
26/07/2011  22:10            51,200 cagse-x64.ja.mst
26/07/2011  22:10         4,002,304 cagse-x64.msi
26/07/2011  22:10            35,840 cagse-x64.zh-cn.mst
26/07/2011  22:02            51,712 cagse.de.mst
26/07/2011  22:02            56,320 cagse.es.mst
26/07/2011  22:02            54,272 cagse.fr.mst
26/07/2011  22:02            51,200 cagse.ja.mst
26/07/2011  22:02         4,044,800 cagse.msi
26/07/2011  22:02            35,840 cagse.zh-cn.mst
14/06/2011  10:16           109,416 cagsetup.exe
28/08/2012  11:26         5,336,424 CitrixAGP.exe
```

The installation performed directly from the executable file is simple, as there is only the need to accept the end user license agreement. Later in the book, we will look at installing the client from the Citrix Merchandising Server and directly from the CAG logon point.

Installing the CAG plug-in from the executable file will run a simple wizard, as shown in the following screenshot:

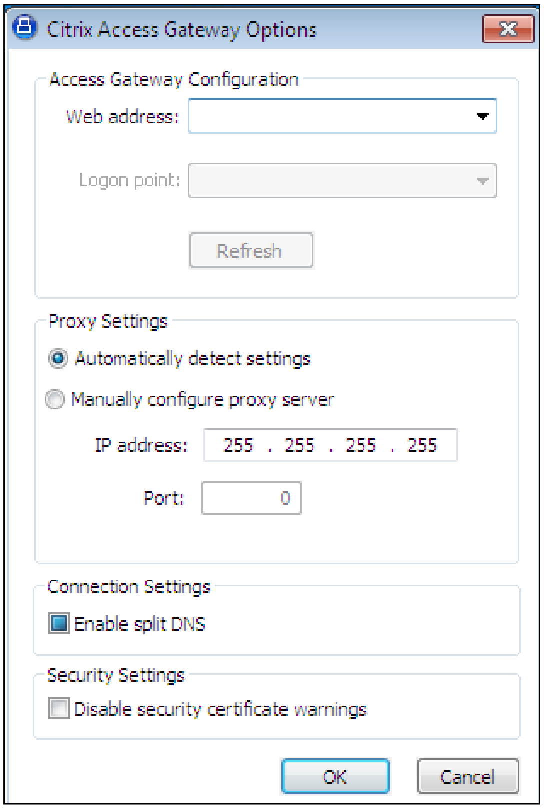


Welcome to the Citrix Access Gateway Plug-in Setup Wizard

The Setup Wizard installs the Citrix Access Gateway Plug-in on your computer. Click Next to continue or click Cancel to exit the Setup Wizard.

Configuring the plug-in properties

Once installed, we can set the properties of the client, as we may need to set web proxy addresses or disable security warnings. To open the CAG **Properties** dialog box from the **Start** menu, go to **Start** | **All programs** | **Citrix** | **Citrix Access Clients** | **Citrix Access Gateway** | **Properties**.



Citrix Access Gateway Options

Access Gateway Configuration

Web address:

Logon point:

Proxy Settings

● Automatically detect settings

○ Manually configure proxy server

IP address: 255 . 255 . 255 . 255

Port: 0

Connection Settings

☑ Enable split DNS

Security Settings

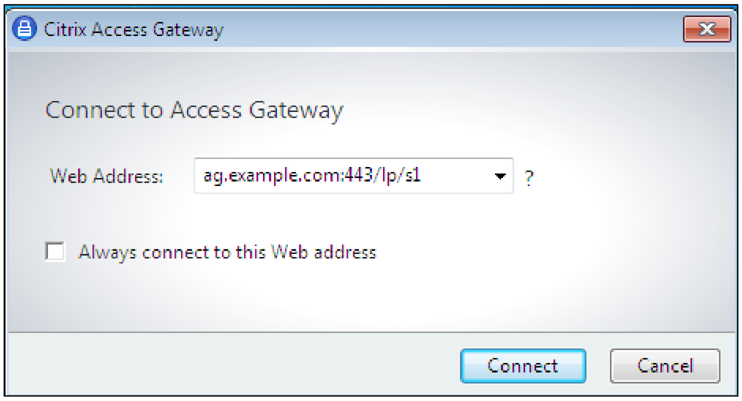
□ Disable security certificate warnings

If the plug-in is installed and the Citrix Receiver is not installed, we are able to log in to CAG from the **Start** menu:

Start | **All programs** | **Citrix** | **Citrix Access Clients** | **Citrix Access Gateway**.

We will first be prompted for the CAG address and logon point, and then our credentials.

Logging on to CAG using the plug-in is shown in the following screenshot:



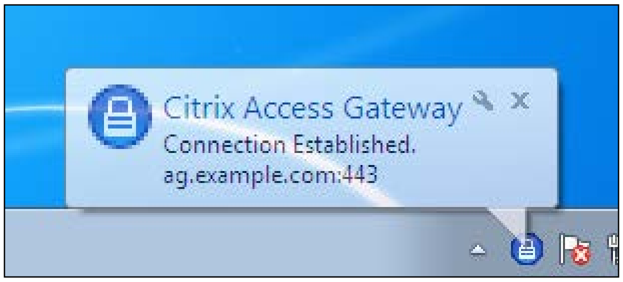
Connect to Access Gateway

Web Address: ag.example.com:443/lp/s1 ?

□ Always connect to this Web address

We are then able to access resources that have been allocated to the SmartAccess logon point. We will look at these in detail later in the book. To monitor the connection, we can use the icon that appears in the system tray or notification area in Windows 7. If the CAG certificate is not trusted, a red warning symbol is also shown across the main icon.

The CAG plug-in is shown in the Windows 7 notification area or the system tray in Windows XP. The Windows 7 example is illustrated in the following screenshot:



Citrix Access Gateway
Connection Established.
ag.example.com:443

Once we have established the connection to the SmartAccess logon point, in this case, we connect to `https://ag.example.com/lp/s1`.

The SmartAccess logon point I have connected to is `s1`. Resources that we are authorized to access will have been assigned to the SmartAccess logon point. Having now connected to the logon point, we should then be able to connect to shares on the internal network. Remember, we have no route to the internal network from the Internet-based clients.

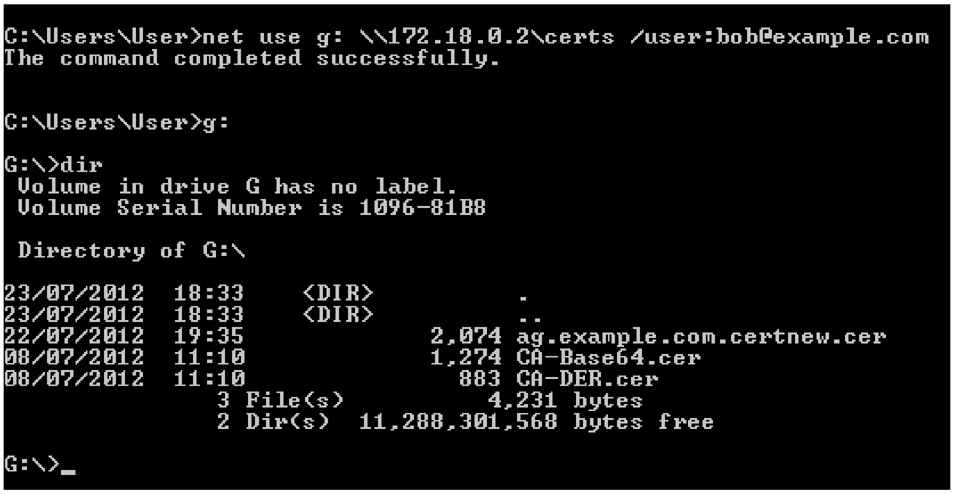
There is a share called `certs` on the domain controller, which we shall now access having established the SSL VPN to CAG. We can access the server with its IP address or DNS name, so long as the DNS name can be resolved by the client. I can connect to the share using any permitted method in Windows, through Windows Explorer, from the **Start** menu or simply by using `net.exe`.

If you are not familiar with connecting to network shares from the command line, then you will see the following command:

```
net use g: \\172.18.0.2\certs /user:bob@example.com
```

With the VPN in place, the plug-in sees that the resource is not accessible locally and is permitted via the gateway. The Internet-based client connects to the gateway using port 443 and the gateway connects to the internal resource using port 139 for Microsoft file sharing.

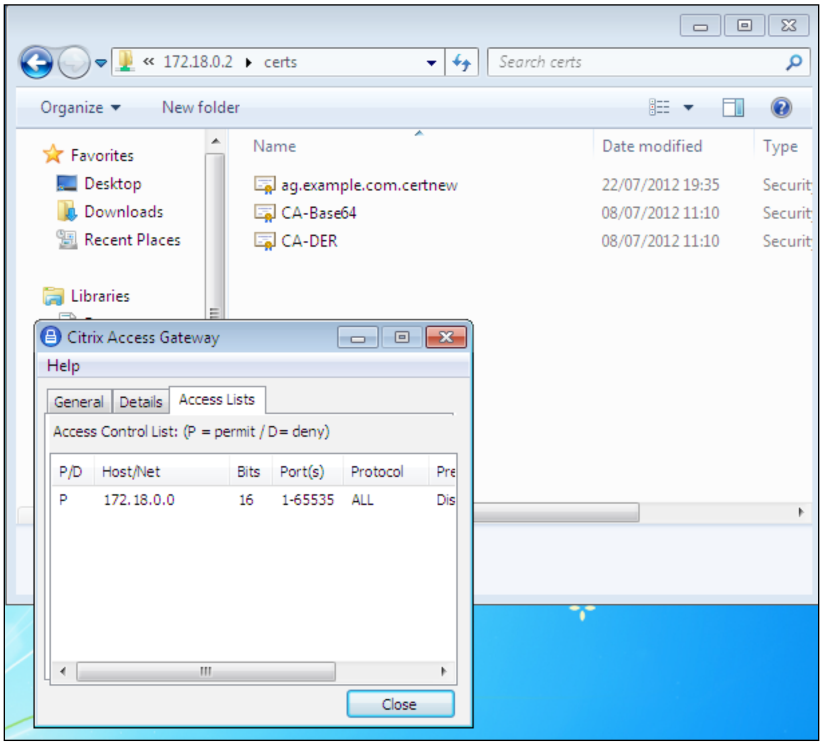
We are now able to map drive letters to shares on the internal private network. From the following screenshot, we can see this using the `net` command:



```
C:\Users\User>net use g: \\172.18.0.2\certs /user:bob@example.com
The command completed successfully.


C:\Users\User>g:

G:\>dir
 Volume in drive G has no label.
 Volume Serial Number is 1096-81B8

 Directory of G:\

23/07/2012  18:33    <DIR>          .
23/07/2012  18:33    <DIR>          ..
22/07/2012  19:35             2,074 ag.example.com.certnew.cer
08/07/2012  11:10             1,274 CA-Base64.cer
08/07/2012  11:10               883 CA-DER.cer
               3 File(s)          4,231 bytes
               2 Dir(s)  11,288,301,568 bytes free

G:\>_
```

By connecting to the resource, we can see the shared contents become available. Additionally, by right-clicking on the plug-in in the Windows 7 notification area, we can select **Connection Status** to view information about the gateway connection we have established. On the **Access List** tab, we see that we are permitted access to all resources on the `172.18.0.0./16` network. This has been set up along with the logon point. This will be detailed later, however, having resources to connect to at this stage helps when illustrating the benefits of universal licenses.

Connecting to a share on the internal network from the Internet, and the connection status dialog, is displayed in the following screenshot using Windows Explorer:



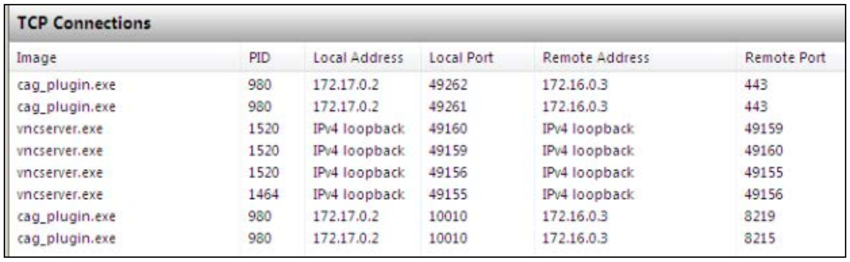
Name	Date modified	Type
ag.example.com.certnew	22/07/2012 19:35	Securit
CA-Base64	08/07/2012 11:10	Securit
CA-DER	08/07/2012 11:10	Securit

Access Control List: (P = permit / D= deny)

P/D	Host/Net	Bits	Port(s)	Protocol	Pre
P	172.18.0.0	16	1-65535	ALL	Dis

Importantly, the client connects to the gateway on port 443, the SSL connection. As with basic logon points, the client has no access to the internal network; all access to the internal network, in our case the file share, is maintained via CAG. With the drive mapped, we can check in the Windows 7 Resource Monitor and we can see that we only have external connections to the gateway, and they all use port 443. We have no connections directly to the server where the share is located.

All access to the internal network is maintained through CAG. The client has no direct connections to the internal resources. The next screenshot shows connections from CAG and not the client:



TCP Connections

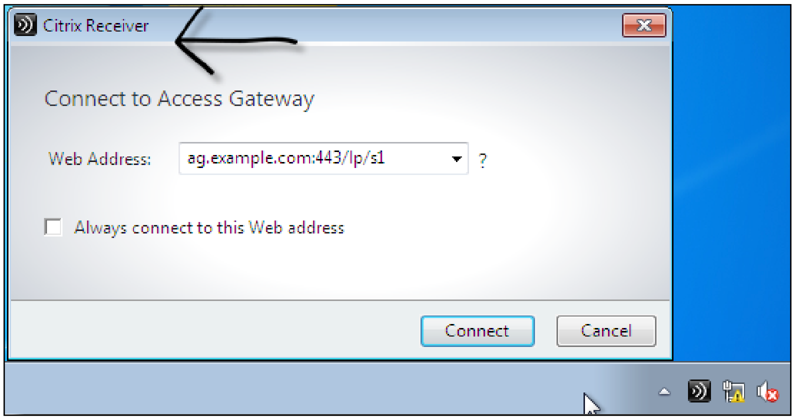
Image	PID	Local Address	Local Port	Remote Address	Remote Port
cag_plugin.exe	980	172.17.0.2	49262	172.16.0.3	443
cag_plugin.exe	980	172.17.0.2	49261	172.16.0.3	443
vncserver.exe	1520	IPv4 loopback	49160	IPv4 loopback	49159
vncserver.exe	1520	IPv4 loopback	49159	IPv4 loopback	49160
vncserver.exe	1520	IPv4 loopback	49156	IPv4 loopback	49155
vncserver.exe	1464	IPv4 loopback	49155	IPv4 loopback	49156
cag_plugin.exe	980	172.17.0.2	10010	172.16.0.3	8219
cag_plugin.exe	980	172.17.0.2	10010	172.16.0.3	8215

Integrating the Access Gateway plug-in with the Citrix Receiver

The Citrix Receiver can be used to manage plug-ins on a user device. Online plug-ins are most commonly used to access hosted applications located on XenApp and XenDesktop servers, and the offline plug-in is used to access streamed applications. If the CAG plug-in is hosted on the same device as the Citrix Receiver, then the receiver will manage the plug-in. This always remains the case, no matter if the receiver is installed before the plug-in or after, the receiver will always manage the plug-in when the receiver is present.

We now access the receiver icon in the Windows 7 notifications area to log on and access the plug-in status. Other than that, the behavior is the same; the receiver is just giving a central access to plug-in control.

If the Citrix Receiver is installed, the CAG plug-in is managed through the receiver, as shown in the following screenshot:



Connect to Access Gateway

Web Address: ag.example.com:443/lp/s1

□ Always connect to this Web address

Distributing the Access Gateway plug-in with the Citrix Merchandising Server

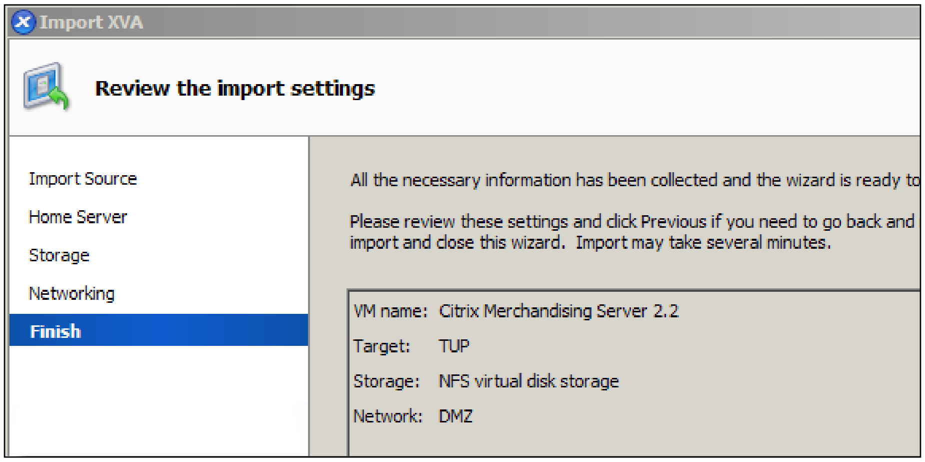
To deliver plug-ins to user devices in a more controlled manner, we must upload and configure the CAG plug-in on to the Citrix Merchandising Server. When users connect to the Merchandising Server, the plug-in will download and install from the Merchandising Server. This server is available as a free, downloadable virtual appliance from the Citrix website. The server acts as **electronic software distribution** (**ESD**) for your Citrix plug-ins. Not only can it distribute and install the plug-ins, but it will configure them too and is available at no cost. As with all the virtual appliances, it must be imported and configured for your virtual machine host. The appliance is available for VMware or XenServer. You may download the virtual appliance from `http://citrix.com/downloads/citrix-receiver/merchandising-server.html`.

The Merchandising Server will require a connection to the Internet to download the plug-ins and receivers directly from Citrix. These are then stored and the Merchandising Server is then able to distribute these to user devices based on the rules we configure. This becomes a simple form of ESD, keeping your user base up-to-date with the authorized versions of plug-ins. Administrators can configure the plug-in meta-data, ensuring that they are delivered preconfigured, so that users do not need to type in the address of CAG and logon point name.

The Merchandising Server would normally be installed in the DMZ. The main steps in installing the Merchandising Server are as follows:

1. Download the XVA file from Citrix.
2. Extract the file and import to your virtual machine servers.
3. Configure basic networking from the command line.
4. Log on to the web console: `https://<yourmsaddress|/appliance`.
5. Use `root` and `C1trix321` as the password.
6. Connect to your internal Active Directory.
7. Add in your own Administrator accounts from Active Directory.
8. Add your own certificates.
9. Download plug-ins to the server.
10. Create deliveries to push the plug-in to users.

Importing the Merchandising Server into XenServer is shown in the following screenshot:



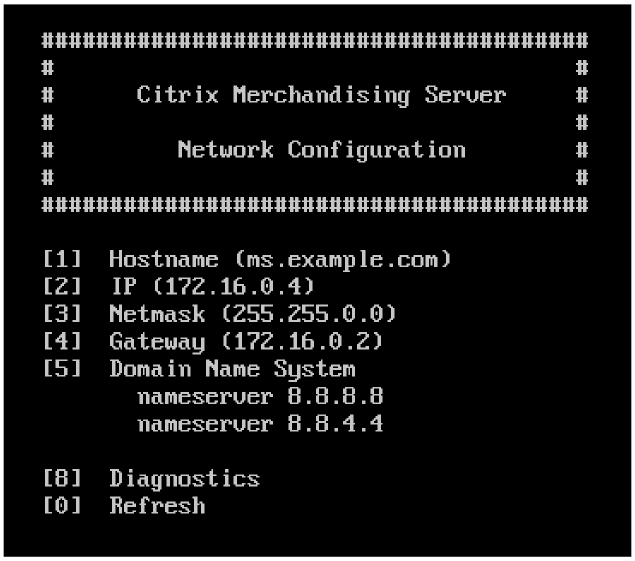
Review the import settings

All the necessary information has been collected and the wizard is ready to

Please review these settings and click Previous if you need to go back and import and close this wizard. Import may take several minutes.

VM name: Citrix Merchandising Server 2.2
Target: TUP
Storage: NFS virtual disk storage
Network: DMZ

Once installed, the first step is to configure the basic networking settings from the command line of the Merchandising Server. The console menu provides a simple mechanism to set up the basics. Refer to the following screenshot:



```
########################################
#                                      #
#      Citrix Merchandising Server     #
#                                      #
#         Network Configuration        #
#                                      #
########################################

[1]  Hostname (ms.example.com)
[2]  IP (172.16.0.4)
[3]  Netmask (255.255.0.0)
[4]  Gateway (172.16.0.2)
[5]  Domain Name System
       nameserver 8.8.8.8
       nameserver 8.8.4.4

[8]  Diagnostics
[0]  Refresh
```

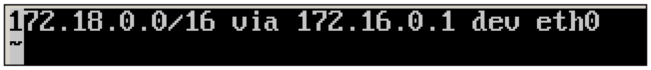
Don't forget though that we are installing the device in the DMZ, as the default gateway would normally be the Internet-facing router. As with CAG, we need to add a static route to the private network to access the Active Directory; unlike the gateway, there is no graphical tool within the web console to achieve this, so we must use the old-school Linux command line to achieve this step.

From the command line menu, we will choose `[8]` for `Diagnostics`, from the `Diagnostics` menu, we then will select `[4]` for `Appliance Terminal`. We will then be prompted to log in as the Linux root user. The password will have been set during the initial configuration. Once we have authenticated, we need to edit the route file for the network card:

```
vi /etc/sysconfig/networking-scripts/route-eth0
```

The Merchandising Server is based on CentOS Linux if you need a reference to command line documentation. The static route to match our configuration would match the following, giving access to the complete `172.18` network using the gateway `172.16.0.1` accessible from interface `eth0`.

Adding a static route to the internal network from CAG is shown in the following screenshot:



```
172.18.0.0/16 via 172.16.0.1 dev eth0
~
```

Configuring deliveries with the Merchandising Server

If users have Citrix Receiver for Windows 3.0, 3.1, or 3.2, users can install the Receiver Updater for Windows. This is the optional component that updates the plug-ins and communicates with the Merchandising Server.

The Merchandising Server is managed through its own web console. Once the initial networking setup is complete on the server, we may log on to the console and configure the Active Directory connectivity and assign an administrator. With this in place, we then log back on as the assigned administrator and from the web console we download the plug-ins to the server.

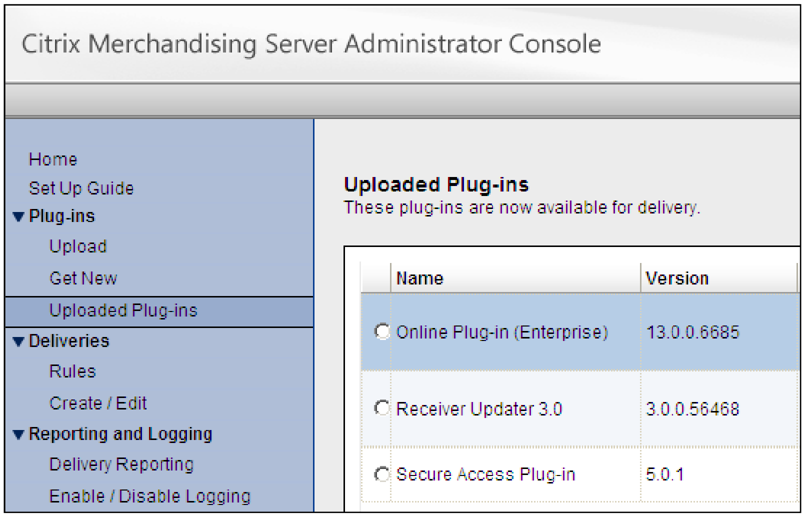
The CAG web address and logon point is part of the metadata configured on the Merchandising Server. When plug-ins are configured via the Merchandising Server, they cannot be changed on the client. This restricts erroneous changes made by well-meaning users and centralizes the configuration for administrators.

> For more technical users, whose configurations may need to change more frequently, consider allowing them to manage and install their own plug-ins independently, so they maintain independent control over the plug-ins.

The Access Gateway plug-in initiates the logon to CAG. If the version of the CAG plug-in for Windows that is installed on the user device is different from the version on the CAG appliance, the plug-in downgrades or upgrades automatically when users log on. As of this writing, the latest Version of the CAG plug-in for the Merchandising Server is 5.01 (Secure Access Plug-in 5.01). If we push this out to our Windows users, then it will upgrade to 5.04 when the users connect to the gateway.

The CAG plug-in for Mac OS X does not downgrade automatically. To install an earlier version of the plug-in on a Mac computer, users must first uninstall the CAG plug-in and then download the earlier version from CAG.

Adding the CAG plug-in to the Merchandising Server is a simple task through the web console, as shown in the following screenshot:



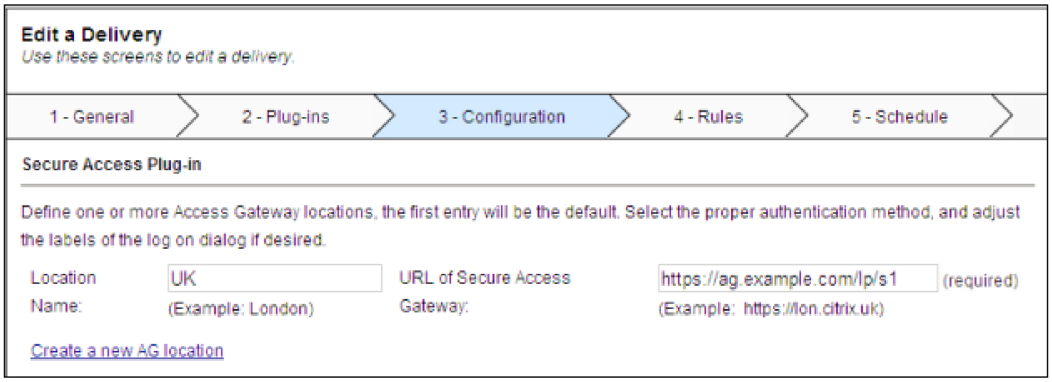
Uploaded Plug-ins

These plug-ins are now available for delivery.

Name	Version
○ Online Plug-in (Enterprise)	13.0.0.6685
○ Receiver Updater 3.0	3.0.0.56468
○ Secure Access Plug-in	5.0.1

We can configure CAG plug-in delivery on the Merchandising Server. This then makes it very easy for our users, as they do not need to configure the gateway address or manage the installations. Through the management console, we create a delivery and specify which plug-ins should be sent. We can control where they are sent by rules which specify criteria, such as username or operating system.

The plug-ins are delivered pre-configured to the user device, eliminating helpdesk calls due to misconfigurations by well-meaning users, shown in the following screenshot:



Edit a Delivery

Use these screens to edit a delivery.

Secure Access Plug-in

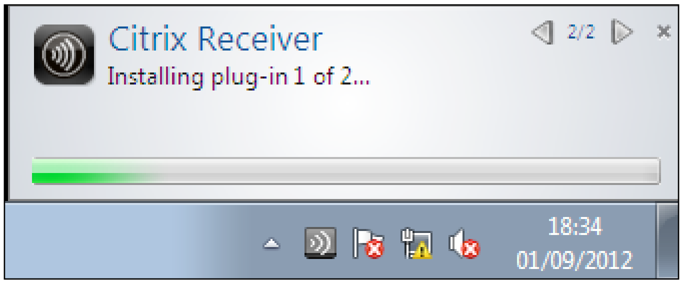
Define one or more Access Gateway locations, the first entry will be the default. Select the proper authentication method, and adjust the labels of the log on dialog if desired.

Location Name: UK (Example: London)

URL of Secure Access Gateway: https://ag.example.com/lp/s1 (required) (Example: https://lon.citrix.uk)

Users connect to the Merchandising Server with their browser and install the Receiver. With this installed, the Receiver prompts for a username and password, so it can authenticate the user to the Merchandising Server using their Active Directory credentials. The server then delivers the required plug-ins through the Receiver.

We can see from the following screenshot that the plug-ins are delivered to the Citrix Receiver:



Citrix Receiver

Installing plug-in 1 of 2...

Summary

In this chapter, we have seen how we can install the CAG plug-in. This gives users access to SmartAccess logon points and independent access to the private network without using XenApp. We added in the universal licenses to support SmartAccess logon points and investigated how installing the Merchandising Server can help in ensuring that plug-ins can be delivered pre-configured.

We did not look at how to create the SmartAccess logon points; so in the next chapter, we will look at creating Address Pools, one of the first components that we need for SmartAccess to allow unique IP addresses for each client connect through CAG.

7
Address Pools

When users connect to SmartAccess logon points, they may need a unique IP address assigned to their connection; some resources may not allow multiple connections from a single IP address. This issue is managed on the CAG through the use of address pools. These are configured in the System Administration Section of the CAG web management point. It also then becomes pertinent to investigate other options that are made available for configuration within System Administration.

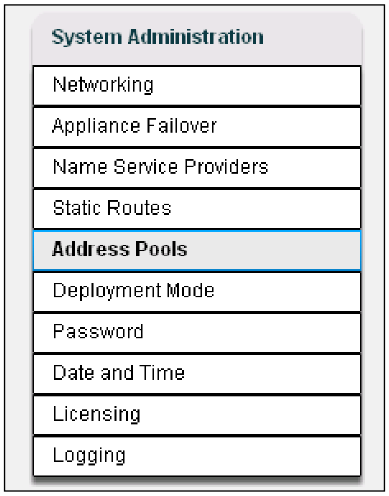
The main points within this section include:

- Creating address pools
- Investigating Citrix Access Gateway System Administration options

Creating address pools

As we mentioned in the introduction, before we can effectively use SmartAccess logon points, we are going to have to create address pools. The easiest way to think of address pools is comparing them with the address ranges in a DHCP server, in that it can assign IP addresses automatically. The CAG can assign an IP address for the clients' plug-in to use while the session is active; unlike DHCP, the IP address is assigned to the CAG and not to the client itself, so security is maintained and clients have to access resources with the CAG.

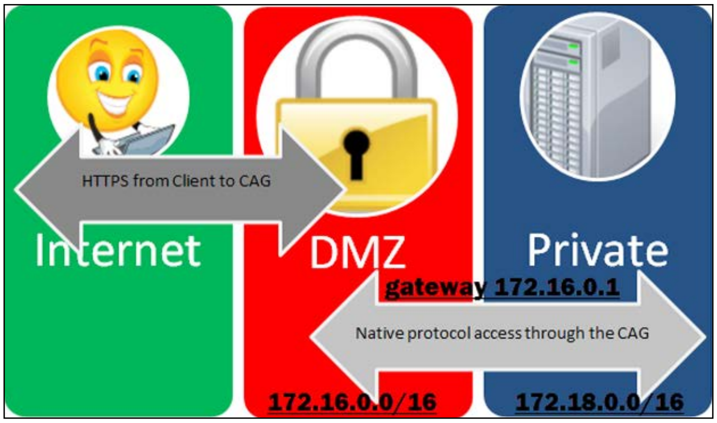
An address pool can be created from within the **System Administration** section of the CAG console.



As with a DHCP address range, there really is not too much to do here. However, we do have to understand the address ranges to add to the address pool.

In the setup that we have, the CAG is on the `172.16.0.0/16` network; the addresses we issue should be within that address range or at least routable to the private network from the `172.16` network. The default router that our CAG uses is the Internet-facing router, `172.16.0.2`. The router that needs to be used to access the internal private network is `172.16.0.1`. This is the router that we add to the address pool, giving our authorized clients access to the private network resources.

In the following image, we illustrate the network topology and the DMZ:



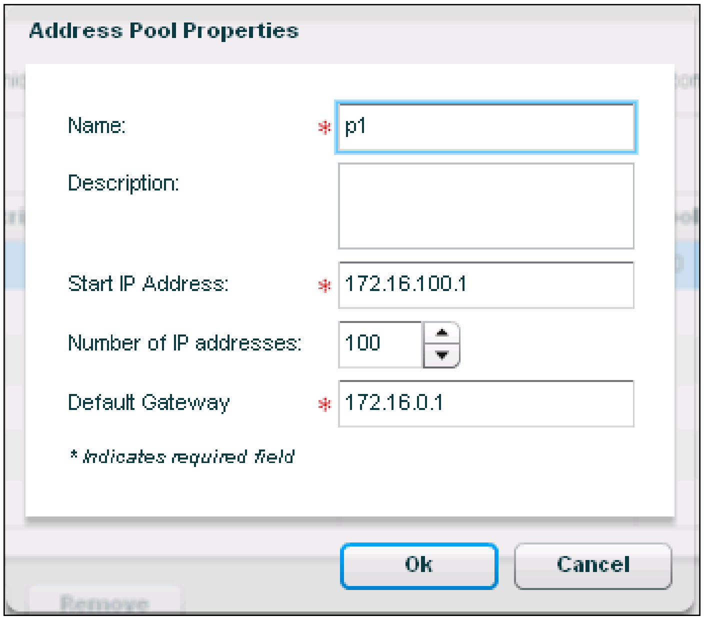
Through SmartAccess logon points, our authorized clients log on to the CAG using the CAG plug-in. Once they have authenticated, the resources they are permitted to access are verified and the gateway will permit or deny access to the resource. To access the resource, the CAG will issue:

- An IP address from its pool (if available; where no address is available, the access will be denied)
- A default gateway allowing access to the private network
- The DNS server entries used by the CAG

The client is then able to access permitted resources through the CAG using the native protocol – http, ftp, smb, and so on. From the address pool, we start with the IP address—`72.16.100.1`, and add 100 addresses to the range. The default gateway has been allocated as `172.16.0.1`, which faces the private network.

> If an address pool is not implemented on the CAG, the CAG will use its own address when accessing resources. This will work with most network resources, but those that require each client to use a separate IP address will not be accessible to more than one client connection. Usually, this is the result of some form of policy in place on the resource, which allows only one connection per IP address.

The address pool we created is shown in the following screenshot:



Address Pool Properties

Name: * p1

Description:

Start IP Address: * 172.16.100.1

Number of IP addresses: 100

Default Gateway * 172.16.0.1

* Indicates required field

When the client accesses the resources through the CAG's SmartAccess logon point, an address is issued for that session. Enough addresses should be in the pool to support the concurrent connections required at any one time.

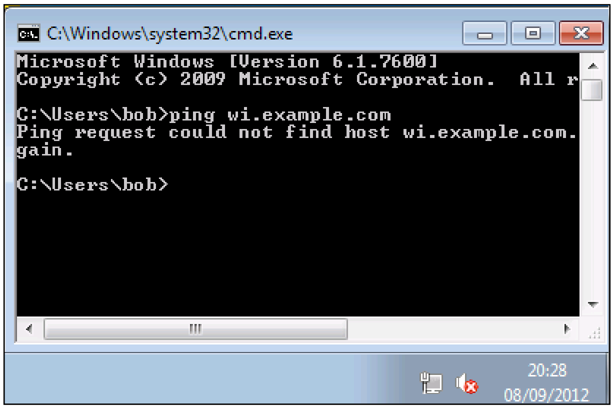
> If you have 100 universal licenses and just a single CAG, it is safe to say you should implement 100 addresses in your pool. If you have more than one CAG that share the license server, the address pool on each CAG will need to support concurrent connections on the CAG and not the shared universal licenses. If we implement two CAGs and share 100 licenses, we would probably need 50 addresses in the address pool of each CAG.

We can see the process of the address pool in action if we investigate how we can gain native access to internal private resources by using the gateway plug-in and the SmartAccess logon points we have previously used in demonstrations.

Before we connect with the plug-in

As an Internet-based client, we cannot access the private network or resolve DNS names defined in the internal and private DNS systems of the corporate network. This can be verified from the Internet client with the `ping` command. When trying to access the private resource, `wi.example.com`, without logging in to the plug-in, the results show that the name cannot be resolved.

If we use a network ping before we connect to the VPN with the plug-in, it will fail. Note that there is no plug-in icon in the notification area. In other words, without establishing a VPN connection to the private resources, they cannot be accessed from devices on the Internet.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All r

C:\Users\bob>ping wi.example.com
Ping request could not find host wi.example.com.
gain.

C:\Users\bob>
```

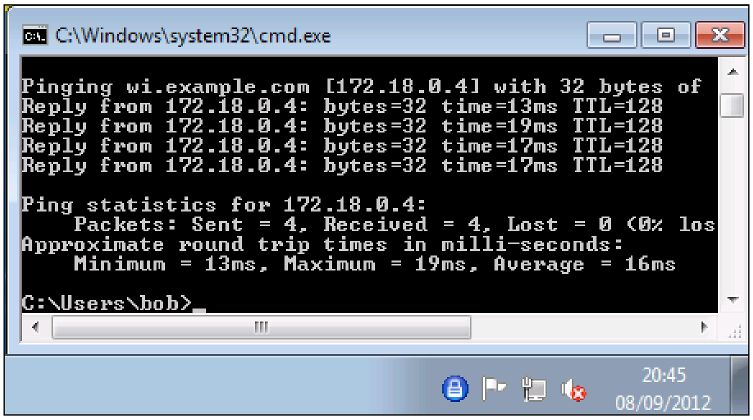
So, without connecting to the CAG VPN, we have no access to private resources.

Ping after the VPN is created with the plug-in

If we then log in to the gateway using the plug-in, the internal DNS and the resource will become available to the client device. We can verify that the resource becomes available once the icon for the plug-in shows as active in the notification area. Note that the blue icon now shows we have logged in to the plug-in.

> You may need to issue the command `ipconfig/flushdns` if name resolution fails after connecting with the plug-in. The client remembers the previous resolution failure and it will cache the failure for some hours.

Once connected, the resource is available. Refer to the following screenshot:

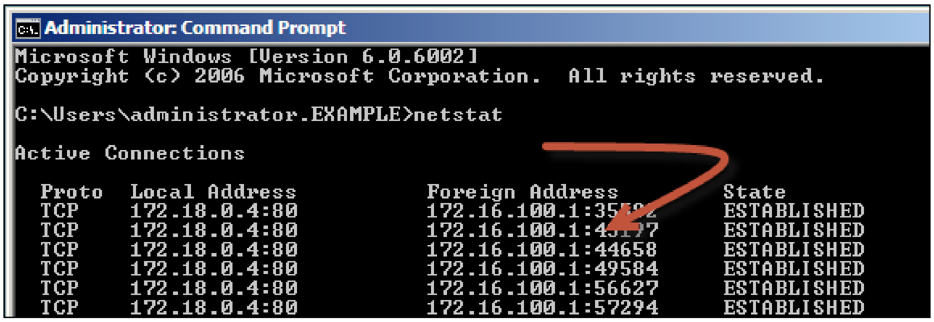


```
Pinging wi.example.com [172.18.0.4] with 32 bytes of
Reply from 172.18.0.4: bytes=32 time=13ms TTL=128
Reply from 172.18.0.4: bytes=32 time=19ms TTL=128
Reply from 172.18.0.4: bytes=32 time=17ms TTL=128
Reply from 172.18.0.4: bytes=32 time=17ms TTL=128

Ping statistics for 172.18.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% los
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 19ms, Average = 16ms

C:\Users\bob>_
```

Accessing the welcome page on the web server

If we now use the browser on the Internet client to access the welcome page on the WI site, we access the resource transparently through the gateway. The gateway will use an address from the pool to access the website. Issuing the `netstat` command on the web server, we can see that we have open connections from the IP address `172.16.100`—the first address in the pool.

If we use `netstat.exe` from the command line to display connected ports on the web server, we will see the address pool in use. This is similar to the results we saw with the Resource Monitor earlier in the chapter, but from the command line.



```
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\administrator.EXAMPLE>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.18.0.4:80          172.16.100.1:35582     ESTABLISHED
  TCP    172.18.0.4:80          172.16.100.1:43197     ESTABLISHED
  TCP    172.18.0.4:80          172.16.100.1:44658     ESTABLISHED
  TCP    172.18.0.4:80          172.16.100.1:49584     ESTABLISHED
  TCP    172.18.0.4:80          172.16.100.1:56627     ESTABLISHED
  TCP    172.18.0.4:80          172.16.100.1:57294     ESTABLISHED
```

The `Local Address` mode shows `172.18.0.4` as the address of the WI, and port 80 as the web server port. Looking across at `Foreign Address`, we see that the connections are from `172.16.100.1`, from the address pool.

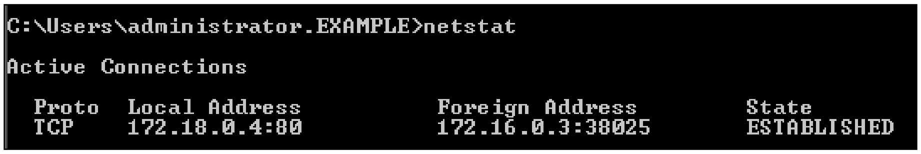
> It is good to see that stable network diagnostics tools such as netstat (part of the tool kit we have been using for many years) can still serve a useful purpose in the latest versions of Windows servers.

Remember though, you may not need to use address pools. The dependency is for services that require unique IP addresses for each connection. If we have no such requirement, there is no need to use a unique IP address for each connection. Then the CAG can use its own IP and route table to access the internal resources.

> The requirement for uniqueness in the connecting IP address will relate to policies that you implement, perhaps for auditing, and are external to the CAG, or perhaps for licensing requirements within software that requires a unique IP address for each connection. Citrix added this feature in recognition that it may be restrictive using the CAG without it, in some situations.

If we disable the address pool and then reconnect to the VPN using the CAG plug-in, we notice that when accessing the WI welcome page the address in use is that of the Access Gateway—`172.16.0.3`.

If no address pool is in use, the IP address of the CAG is used to access resources, as shown in the following screenshot:



```
C:\Users\administrator.EXAMPLE>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.18.0.4:80          172.16.0.3:38025       ESTABLISHED
```

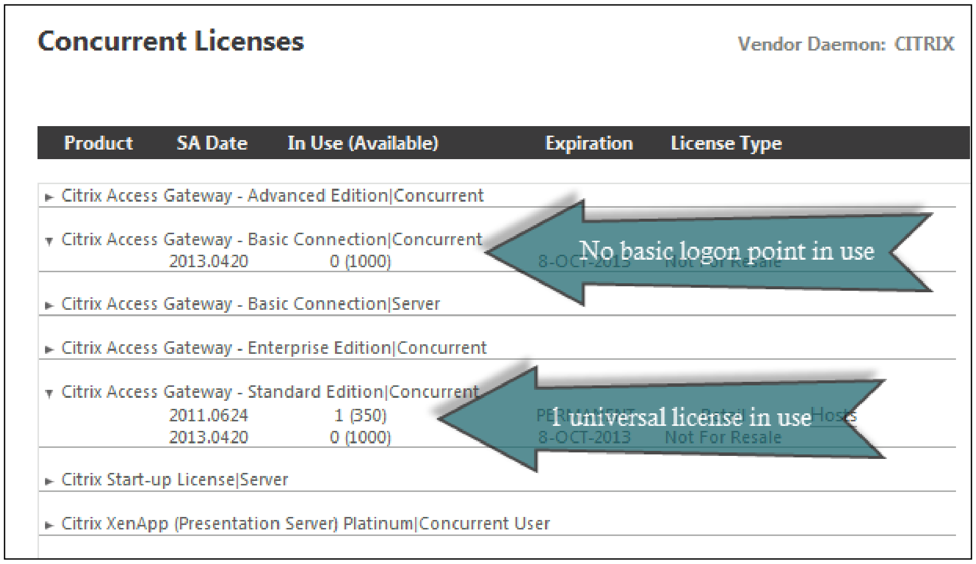
Smart logon points use universal licenses

We know by now that SmartAccess logon points require universal licenses. We added them in the previous chapter to our License Server. We can now access the License Server from our computer having Internet connection and view license usage. We can access the License Server, which is on the private network, as we now have a full VPN connection to the private network; our connection is proxied by the CAG. The License Server is accessed using the following URL:

```
http://ls.example.com:8082
```

This URL will take us to the web console of the License Server. The dashboard shows license usage. In a controlled environment, it is easy to see which connections are in place. Currently we know we only have a connection to the SmartAccess logon point and the utilization shows this. We can also see that we do not use a basic connection license. These licenses are for basic logon points and are not used when connections are made via SmartAccess logon points. The universal license is displayed in the dashboard as Standard Edition licenses and we have one out of 350 concurrent connections in use. The Access Gateway Enterprise Edition licenses would be used by the NetScaler physical appliances running the enterprise edition of CAG.

License usage on the server dashboard when a single connection is made to the SmartAccess logon point is illustrated for you in the following screenshot:



Concurrent Licenses

Vendor Daemon: CITRIX

Product	SA Date	In Use (Available)	Expiration	License Type
▸ Citrix Access Gateway - Advanced Edition|Concurrent				
▾ Citrix Access Gateway - Basic Connection|Concurrent				
	2013.0420	0 (1000)	8-OCT-2013	Not For Resale
▸ Citrix Access Gateway - Basic Connection|Server				
▸ Citrix Access Gateway - Enterprise Edition|Concurrent				
▾ Citrix Access Gateway - Standard Edition|Concurrent				
	2011.0624	1 (350)	PERMANENT	Retail Hosts
	2013.0420	0 (1000)	8-OCT-2013	Not For Resale
▸ Citrix Start-up License|Server				
▸ Citrix XenApp (Presentation Server) Platinum|Concurrent User				

No basic logon point in use

1 universal license in use

System Administration Options

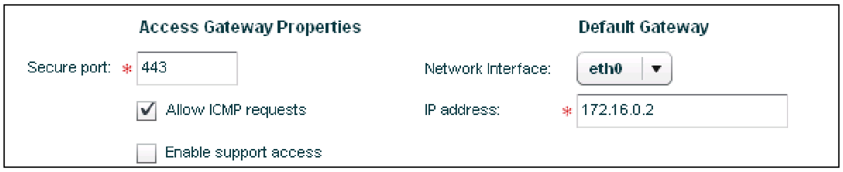
Address pools are configured within the upper section of the Access Gateway management console labeled **System Administration**. We have seen some options in here, such as the static routes; however, it seems pertinent to review these options at this time:

- Networking
- Appliance failover
- Name service providers
- Static routes
- Address pools
- Deployment mode
- Password
- Date and time
- Licensing
- Logging

Networking

From here, we can set the hostname of the Access Gateway that would default to CAG. We have set ours to AG to match the DNS name of the server. Even though we set the IP address of the CAG through the express setup on the command line, we can also set it via the **Networking** options. By default, we can ping the CAG's IP address. Should we not want this, there is the **Allow ICMP requests** option here; it is checked by default, but we could uncheck this.

Networking allows users not only to set the address but also the ICMP option and SSH access. Refer to the following screenshot:



Access Gateway Properties

Secure port: * 443

☑ Allow ICMP requests

□ Enable support access

Default Gateway

Network Interface: eth0

IP address: * 172.16.0.2

The **Enable support access** checkbox is used if you would like to access the server console via SSH; this is not permitted by default.

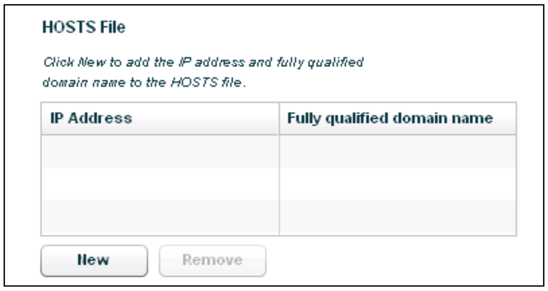
Appliance failover

This option allows us to configure high availability of the CAG. We shall look at this later in *Chapter 14*, *Command Line Management of the Citrix Access Gateway*.

Name service providers

From here we can set the DNS entries for the CAG and populate the localhost file of the gateway. Editing of the localhost file has to take place through the web console, as other than the menu no access is allowed to the servers console. This keeps the server more secure.

If edits to the localhost files are required, they are made through this page.



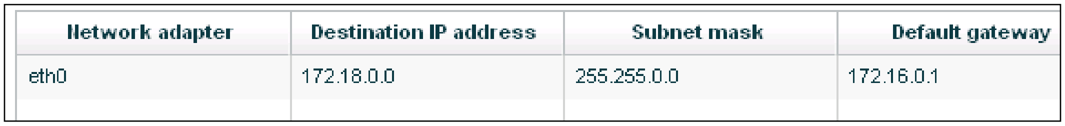
HOSTS File

Click New to add the IP address and fully qualified domain name to the HOSTS file.

IP Address	Fully qualified domain name

Static routes

From here we provided the route for the gateway to access the private network, `172.16.0.0/16`. The default route from the CAG would always point to the Internet-facing router of the DMZ. It would be unusual for the DMZ Internet router to have a route into the private network. The following screenshot shows the static route to the private network:



Network adapter	Destination IP address	Subnet mask	Default gateway
eth0	172.18.0.0	255.255.0.0	172.16.0.1

Address pools

Address pools are covered in this chapter in detail.

Deployment mode

The deployment mode can be Standalone or Access Controller. This was set in the `Express Setup` mode from the command line as the default `standalone` command. In this mode, the CAG acts autonomously to any other appliance. In the `Access Controller` mode, we install additional software on Windows Server 2008. With this in place, we can use policy rules from within XenApp or XenDesktop to control how access to those resources is established. Use of the `Access Controller` mode is a topic of discussion in *Getting Started with XenApp 6.5 Administration, Guillermo Musumeci, Packt Publishing*. The `Access Controller` mode passes connection details from the CAG to policies within XenApp and XenDesktop.

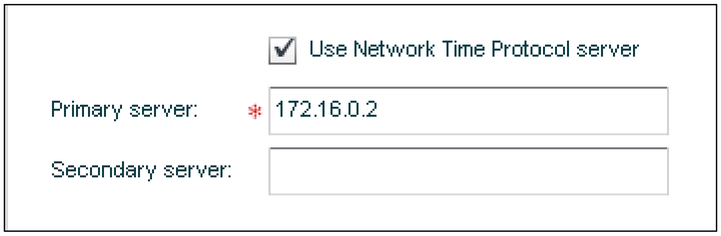
Password

The administration password can be changed by using this option.

Date and time

As the title suggests, we can set the time and date by using this option. The default time zone will be US/Pacific time. Of course, you should set this to match your own location. Mine is set to Europe/London. To keep accurate time, we would always suggest adding a Network Time Protocol server. Tick the `Use Network Time Protocol server` checkbox and add one or two NTP servers. This may be an internal server on your network or, if you don't have one, use something such as `uk.pool.ntp.org` (or a pool server for your location). Using `ntp.org` pool servers represent free-to-access public NTP servers.

From the following screenshot, you can see that we are connecting to a local NTP server as our primary NTP time source:



☑ Use Network Time Protocol server

Primary server: * 172.16.0.2

Secondary server:

Licensing

This was covered back in *Chapter 2*, *Licensing the Citrix Access Gateway*. If we have to change the License Server, we can point to the new server from this page as well as see the licenses that are installed. We cannot see license usage from here, however, but the main **Monitor** tab has a **License usage** dialog to show this.

Logging

From the main **Monitor** tab, we can access the logfiles. We saw this when looking at logging access to website resources with basic logon points in *Chapter 4*, *Configuring a Basic Logon Point for XenApp/XenDesktop*. From here we can set when to rotate the logs. The default is every 4 hours and we can set these archived logs to be transferred to a remote server via SCP or FTP for archiving. We will cover more information on monitoring the logs later, in *Chapter 14*, *Command Line Management of the Citrix Access Gateway*.

Summary

Our journey through this chapter has seen us investigate and create address pools. These are used by the CAG so that the unique IP addresses are used when accessing internal resources. If address pools do not exist, the CAG can use its own IP address; however, results may be unreliable if internal resources do not permit multiple connections from the single IP address. The address pools that are configured in the System Administration are of the management console, so we choose at this time to investigate the other options that this section offers.

In the next chapter, we will continue building up the properties that we can use to allow or disallow access to network resources by creating and using device profiles. Using these, we can grant or deny access to resources based on properties that we can read from the user device. We have been demonstrating SmartAccess logon points and we will continue to do this in the next chapter. The properties and profiles that we create, such as address pools and device profiles in the previous sections, are all referenced by the logon point to effectively control access to our internal resources.

8
Device Profiles and Endpoint Analysis

Device profiles in CAG allow you to create a profile that validates a user device against an administrator that defines a set of criteria. The validation occurs during user logon. Before the user is allowed access to our network, the device must meet the criteria that we set up in the device profile. We can define device profiles to represent the variety of endpoint devices with which users may access internal resources.

For example, as administrators at EXAMPLE, we may define a device profile named `Example owned Win7 laptop`, which matches Windows 7 computers and includes our own internally added entry in the Windows registry. If the user device matches those criteria, then we can allow access to the network.

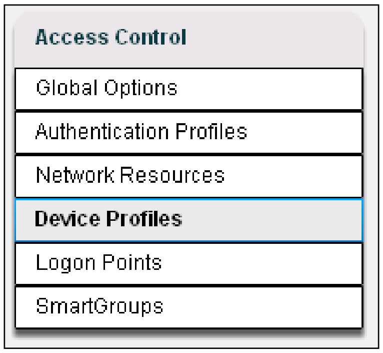
Device profiles are referenced in a logon point by means of SmartGroups. We can also reference them directly in the logon point, which may then allow for messages to be sent to the client if they do not match the criteria.

In this chapter we will define:

- Device profiles
- Installing the endpoint analysis plug-in
- Control access to the network using device profiles and endpoint analysis

Device profiles

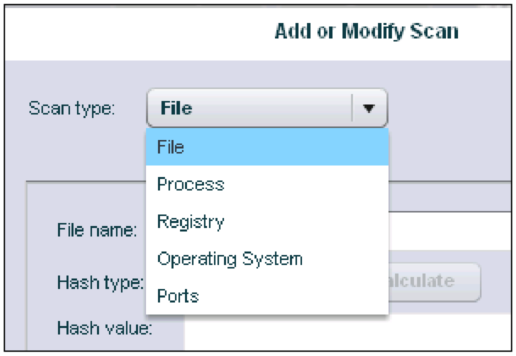
We configure device profiles in the **Access Control** section of the **Management** tab in the CAG web console. They are employed in SmartGroups that, in turn, assign logon points to network resources. Investigating SmartGroups is implemented in *Chapter 11, Linking it All Together with SmartGroups*. Following is the screenshot of **Device Profiles** in the management console:



When we create device profiles, they are made up of one or more scan expressions. The characteristics of a device that we can search for within a scan include:

- **File**
- **Process**
- **Registry** settings
- **Operating System** versions
- **Ports** (open ports)

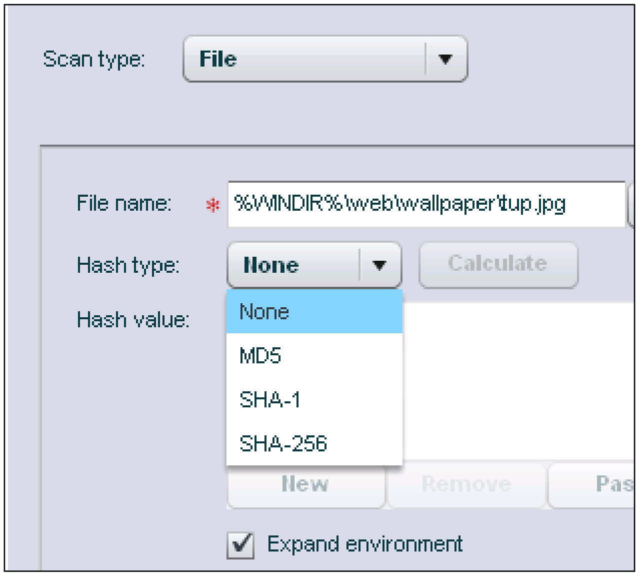
These components make up the scan type and an expression can comprise one or more scan types, as shown in the following screenshot:



File

Using the file scan, we can check for the presence of a file in the end user's device filesystem. Perhaps one way of checking for corporate machines could be the presence of the company wallpaper. We are not saying that it has to be the current wallpaper or desktop background, but just has to exist in the file system. We would then search for `%WINDIR%\Web\Wallpaper\tup.jpg`.

For this type of file, we are probably not concerned with whether or not the file has been modified or is a specific version. So, we will not add in a hash type, but if we were, we could include the hash of the file to check if it matches our source version. Care should be taken when including hashes, as this can increase the scan time of the client.



Scan type: File

File name: * %WINDIR%\web\wallpaper\tup.jpg

Hash type: None

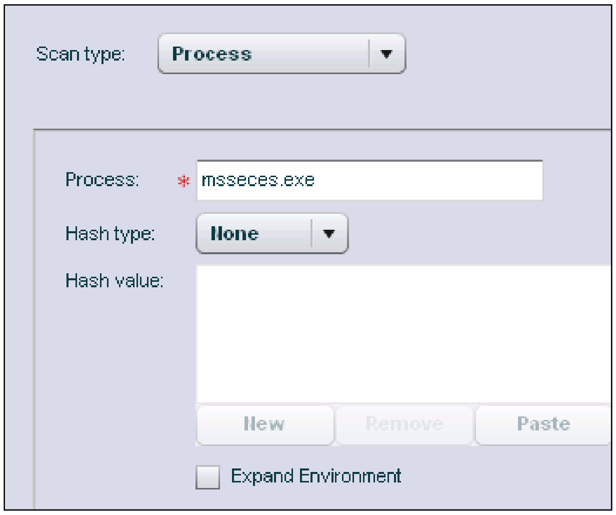
Hash value:

☑ Expand environment

Process

If we need to check for anti-virus, it is possible that we could check for a running process that matched anti-virus software that we trust. This is not only checking that the anti-virus is installed but is actually running. In checking for the presence of the process `msseces.exe`, we are investigating whether or not Microsoft Security Essentials is installed and running.

Checking for Microsoft Security Essentials running on device is shown in the following screenshot:



Scan type: Process

Process: * msseces.exe

Hash type: None

Hash value:

□ Expand Environment

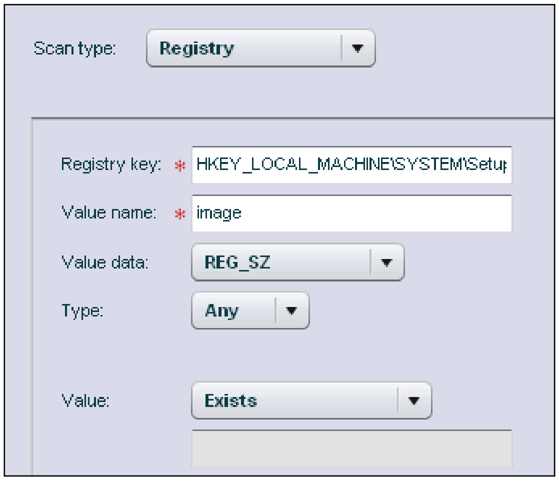
Registry

We may need to check that these are corporate-built desktops or laptops that are connecting. Then it is possible for you to add your own registry keys with the image-built type or number. Of course, we can scan for any registry values that we choose, not just our own custom entries.

For a custom entry, the registry key to scan could be `HKEY_LOCAL_MACHINE\SYSTEM\Setup\install`.

The value name then may then be entered similarly to this as `image`.

We then decide if we just need the value name to exist or to have a certain value. In our example, we just need the value to exist. Scanning for a custom registry entry is shown in the following screenshot:



Scan type: Registry

Registry key: * HKEY_LOCAL_MACHINE\SYSTEM\Setu

Value name: * image

Value data: REG_SZ

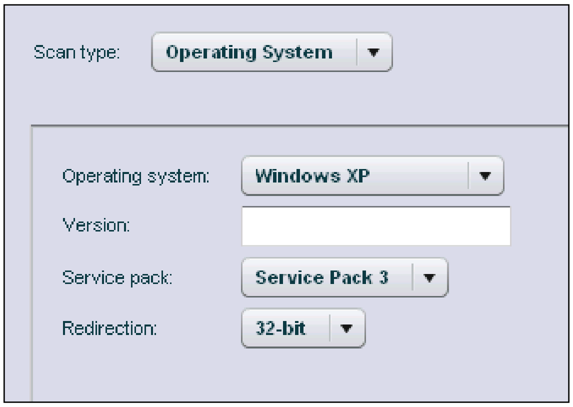
Type: Any

Value: Exists

Operating System

The **Operating System** scan type can be very useful. For example, we could say that we require Windows XP to be Service Pack 3, therefore excluding all XP OSs that are not patched to this service pack level.

Although many operating systems exist in the dialogue, we can only detect Windows operating systems with the endpoint analysis plug-in. The additional OS exists for CAG when accessing XenApp and XenDesktop. Scanning for Windows XP Service Pack 3 is shown in the following screenshot:



Scan type: Operating System

Operating system: Windows XP

Version:

Service pack: Service Pack 3

Redirection: 32-bit

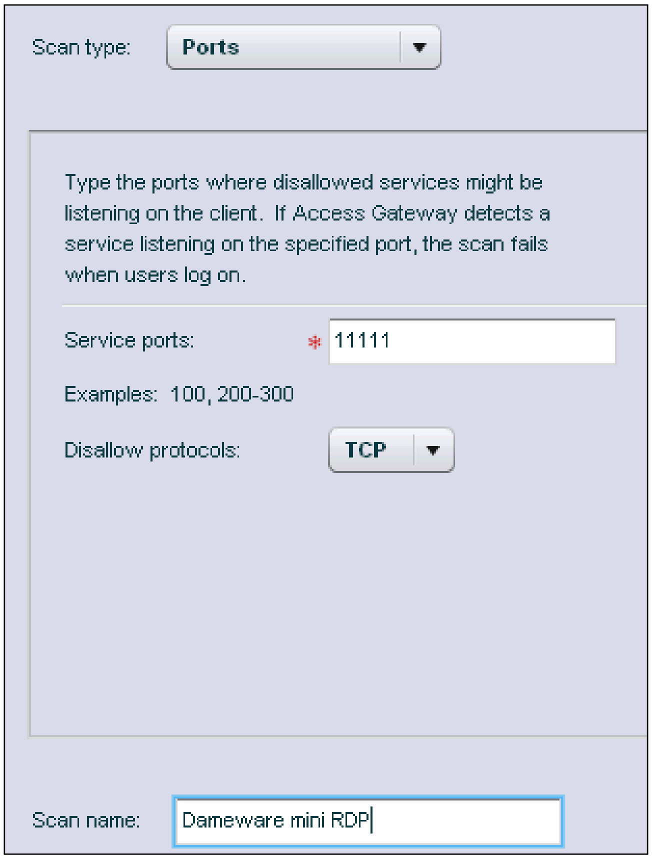
In this scan, we are checking for 32-bit versions of Windows XP with Service Pack 3. We could choose **Any** in the **Redirection** option if we needed to include 64-bit and 32-bit versions of XP Service Pack 3 in the single scan.

Ports

The final scan type is **Ports**. These scans look for open ports on the user device that we do not authorize. These ports can be TCP or UDP. We can set **Any** for ports that could work on TCP or UDP such as DNS.

For example, we may not want machines to connect that have TCP ports 11111 and 6129 open. These are indications that DameWare is installed on the device and it may be maliciously remote controlled.

The underlying logic used for ports is that the device does not have to have the ports open in order to match the criteria. Following is the screenshot of **Ports** scan:



Scan type: Ports

Type the ports where disallowed services might be listening on the client. If Access Gateway detects a service listening on the specified port, the scan fails when users log on.

Service ports: * 11111

Examples: 100, 200-300

Disallow protocols: TCP

Scan name: Dameware mini RDP

Building an effective scan expression

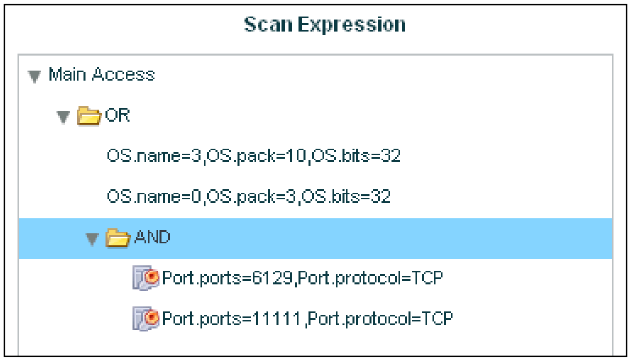
We have seen that we have multiple scan types available to us. A scan expression may exist as a single scan, but is more likely to contain multiple scans. These scans may be of the same type, such as when detecting both port 11111 and 6129. The logic for this could include the `AND` or `OR` operator. If we were checking the operating system, then the only feasible logical operator to use with this would be `OR`. We could never use XP and Windows 7 at the same time.

We may wish to restrict access to Windows XP SP3 or Windows 7 as long as both ports 6129 and 11111 are closed. From the middle expression builder window, we can add the correct `AND` or `OR` component to ensure the expression is evaluated as required. Of course, as the requirements increase, the expressions will increase as well; testing time will be a valuable asset to ensure correct operation.

To match the expression:

- The device OS should be Windows XP SP3 32 bit or any version of Windows 7
- The device should not be listening on port 11111 and port 6129

Multiple scans within in a single expression using `AND`/`OR` operators is shown in the following screenshot:

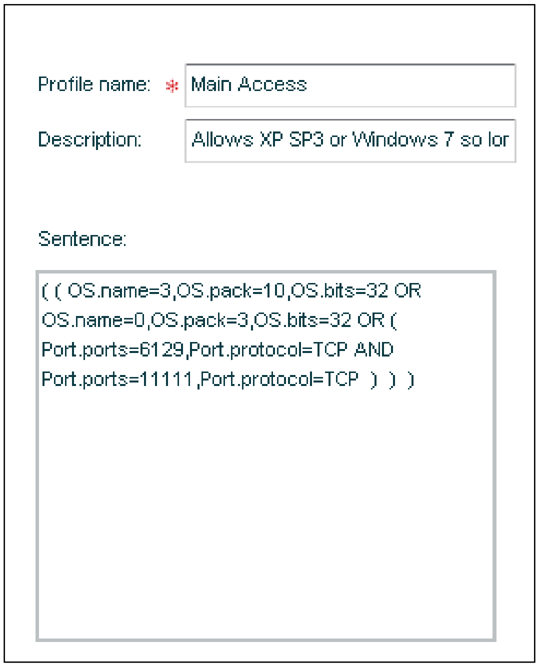


Scan Expression

```
▼ Main Access
    ▼ OR
        OS.name=3,OS.pack=10,OS.bits=32
        OS.name=0,OS.pack=3,OS.bits=32
    ▼ AND
        Port.ports=6129,Port.protocol=TCP
        Port.ports=11111,Port.protocol=TCP
```

Access to the `AND` and `OR` operators are found at the bottom of the **Scan Expression** page. You must add the operators first, and then add scans to the existing operators. The term **Main Access** in this example represents the name of the device profile.

We may view the logic graphically with the scan expression builder, but the expression is additionally displayed in raw text as **Sentence** and is displayed under the name and description of the device profile. This is only for display purposes and cannot be edited through the **Sentence** text. It is provided, though, as some people may find reading the text simpler.



Profile name: * Main Access

Description: Allows XP SP3 or Windows 7 so lor

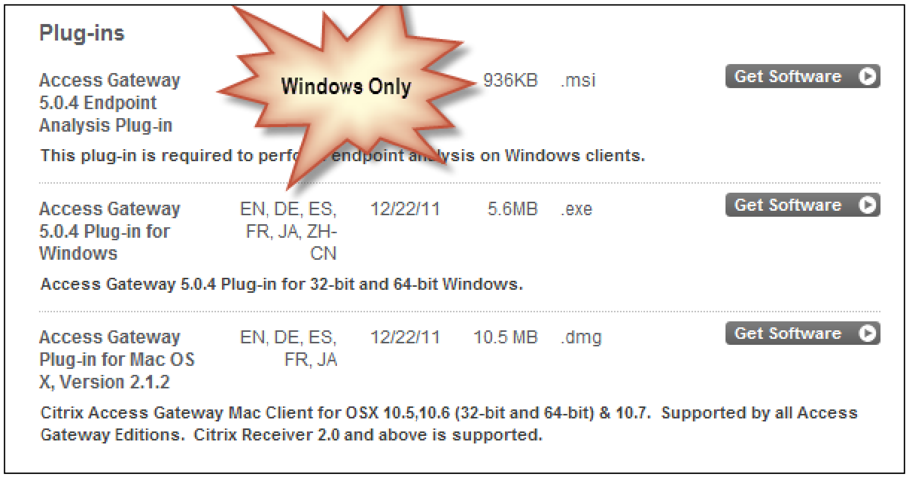
Sentence:

((OS.name=3,OS.pack=10,OS.bits=32 OR OS.name=0,OS.pack=3,OS.bits=32 OR (Port.ports=6129,Port.protocol=TCP AND Port.ports=11111,Port.protocol=TCP)))

Installing the endpoint analysis plug-in

The actual scans are performed on the user device and an additional plug-in is required for this. Unfortunately, the plug-in is for Windows only. So, even though the CAG plug-in can be installed on MAC OSX or Windows, full endpoint analysis is only possible on Windows devices. This can be distributed via the Merchandising Server or downloaded from the Citrix website, `http://www.citrix.co.uk/downloads/netscaler-access-gateway.html`.

The endpoint analysis plug-in is only available for Windows and not OSX, as shown in the following screenshot:

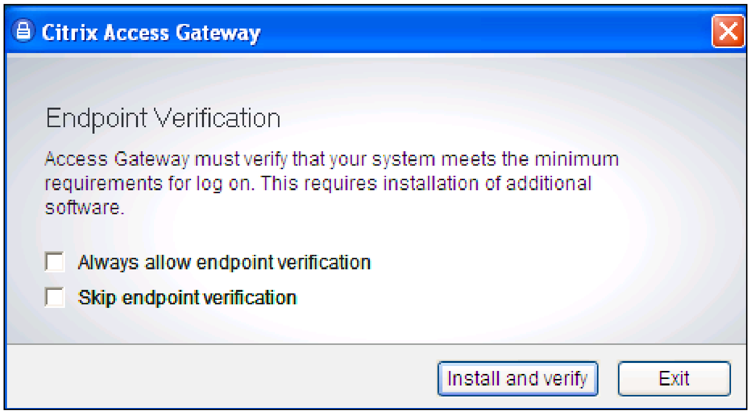


Plug-ins

Access Gateway 5.0.4 Endpoint Analysis Plug-in			936KB	.msi	Get Software
This plug-in is required to perf endpoint an ysis on Windows clients.					
Access Gateway 5.0.4 Plug-in for Windows	EN, DE, ES, FR, JA, ZH-CN	12/22/11	5.6MB	.exe	Get Software
Access Gateway 5.0.4 Plug-in for 32-bit and 64-bit Windows.					
Access Gateway Plug-in for Mac OS X, Version 2.1.2	EN, DE, ES, FR, JA	12/22/11	10.5 MB	.dmg	Get Software
Citrix Access Gateway Mac Client for OSX 10.5,10.6 (32-bit and 64-bit) & 10.7. Supported by all Access Gateway Editions. Citrix Receiver 2.0 and above is supported.					

If the endpoint analysis plug-in is not installed, then it will be automatically downloaded from CAG when access is first made to a logon point where endpoint analysis is enabled. The user will see two dialogue boxes during the process. The first will be to trust CAG for scans and then the installation will continue displaying the progress bar.

Trusting CAG to allow scans to run is shown in the following screenshot:



Citrix Access Gateway

Endpoint Verification

Access Gateway must verify that your system meets the minimum requirements for log on. This requires installation of additional software.

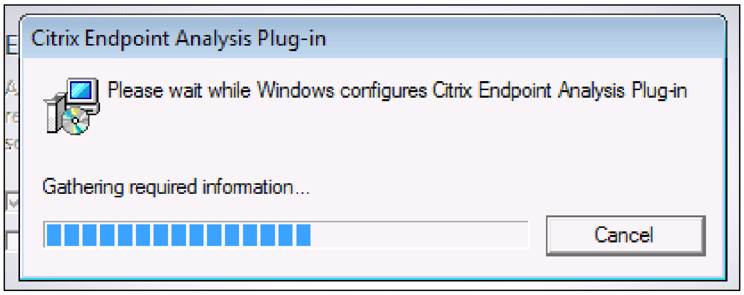
☐ Always allow endpoint verification

☐ Skip endpoint verification

The user can leave these selections at their default values, so that the scan can run from this CAG. However, if they choose **Always allow endpoint verification**, they are not prompted each time a scan needs to take place when connecting to CAG.

Skipping endpoint verification would disallow access to the SmartAccess logon points that have EPA enabled. The user would be expected to proceed with **Install and Verify** to successfully enable EPA on this device. We can understand that having this delivered by the Merchandising Server or pre-installed will make life easier for the help desk and your users.

As the installation continues, the progress of the MSI installation will be shown as follows:



Citrix Endpoint Analysis Plug-in

Please wait while Windows configures Citrix Endpoint Analysis Plug-in

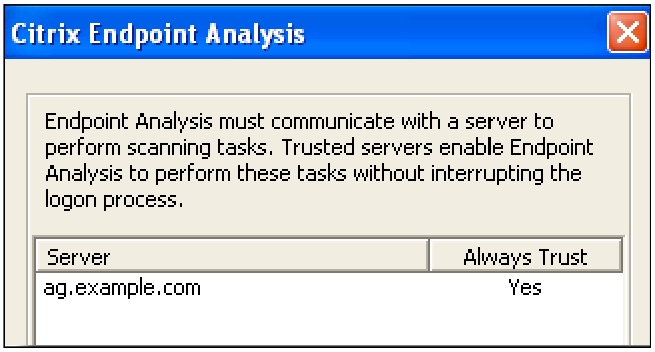
Gathering required information...

The client does not need access to the plug-in once installed. Scans will run automatically when logging in to a logon point where EPA is enabled. Having said that, users can return to the plug-in configuration should they need to adjust trust relationships with CAGs.

To access the plug-in, navigate to:

Start | **All Programs** | **Citrix** | **Endpoint Analysis Plug-in** | **Manage Endpoint Analysis Plug-in**.

From here we can view CAGs that we have accessed with EPA enabled in SmartAccess logon points. We can delete or allow trust relationships, as shown in the following screenshot:



Citrix Endpoint Analysis

Endpoint Analysis must communicate with a server to perform scanning tasks. Trusted servers enable Endpoint Analysis to perform these tasks without interrupting the logon process.

Server	Always Trust
ag.example.com	Yes

Control access to network using device profiles

Once we have created the device profiles, they can be referenced in the SmartAccess logon point itself or the SmartGroup. Any reference is the logon point itself and will deny access to the logon point if the requirements are not met. This is useful, allowing remediation messages to be displayed to the users on the failed logon. The normal use of the device profiles is to control access to network resources referenced in the SmartGroups.

SmartGroups link logon points to network resources; access is controlled with device profiles and other mechanisms such as authorizations. As we build up our compendium of tools, progressing through the chapters in the book, we will gradually complete the jigsaw created by these individual elements of secure access.

Summary

In this chapter, we have looked extensively at device profiles, and how we can build scans into expressions to effectively monitor user devices before connecting them to resources on our private network. This is essential in maintaining secure access, as rogue machines may disrupt other users or services.

In the next chapter, we will look at how we can define the network resources that we can access and how Citrix Branch Repeater can be used both with CAG and independently with Branch Repeater appliances.

9
Defining Network Resources

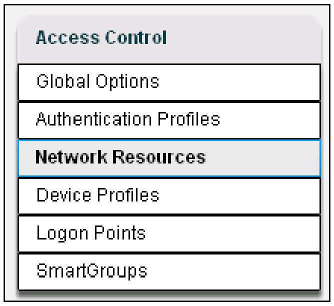
To be able to connect to a resource using a SmartAccess logon point defined on CAG, we must previously have configured those network resources. Network resources are ranges of IP addresses that we wish to be accessible via CAG and the protocols that we want to include in those network targets. The protocols we can control are TCP, UDP, ICMP, and Citrix Branch Repeater.

In this chapter, building on what we have created so far, we will:

- Define network resources within CAG
- Introduce the Citrix Branch Repeater

Network resources

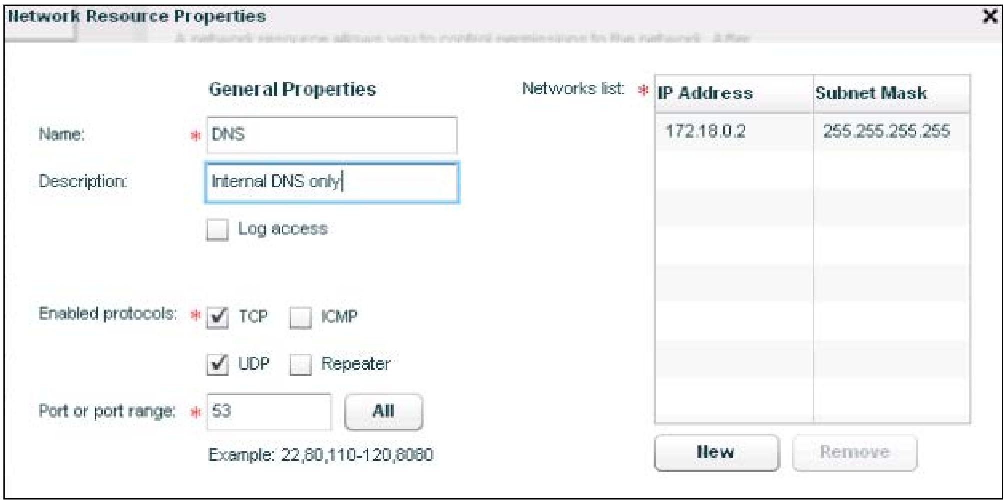
Network resources define connection targets that are valid when initiated through the CAG SmartAccess logon points. Although they define connection targets, access to these targets can be permitted or denied when referenced in a SmartGroup. The network resource definition simply defines the target without granting access to it. Network resources are defined in the CAG management console, and by now, we should be familiar with visiting the **Access Control** section of the **Management** tab. The **Network Resources** section is shown in the following screenshot:



As CAG administrators, we will now discover that we require knowledge similar to that of our network infrastructure administrators; perhaps we share this role. We certainly need a good understanding of which ports are used by which services and the underlying transport protocols they use.

When defining CAG network resources, we should bear in mind that users will normally require access to the internal DNS servers; DNS servers listen on port 53, and this could be used on UDP or TCP protocol stacks, or possibly on both. To enable access to DNS, we should define entries for port 53 on TCP and UDP. In order to allow access to a network resource, we must first define it. As our DNS server is `172.18.0.2`, we will create a single entry like we did for other servers to support access control to the internal DNS server.

The following screenshot illustrates defining DNS as a resource on a single server:



General Properties

Name: * DNS

Description: Internal DNS only

□ Log access

Enabled protocols: * ☑ TCP □ ICMP ☑ UDP □ Repeater

Port or port range: * 53

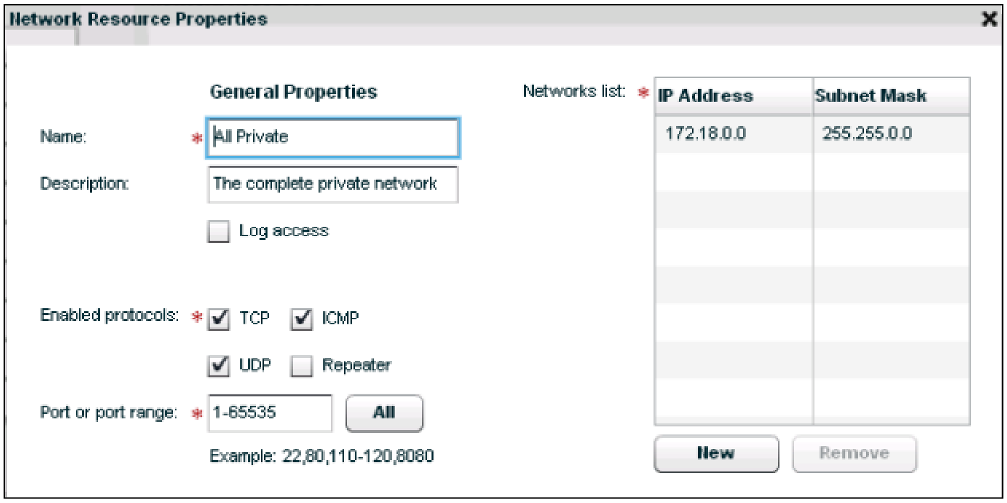
Example: 22,80,110-120,8080

Networks list: *

IP Address	Subnet Mask
172.18.0.2	255.255.255.255

If we need to audit access to the network resource (even if we succeed or fail doing so), this is maintained with the **Log access** checkbox in much the same way as we saw in *Chapter 4*, *Configuring a Basic Logon Point for XenApp/XenDesktop*.

The subnet mask used here, `255.255.255.255`, indicates the address that represents a single host. This, then, could be used to allow or deny access to query the DNS, but this is the only service we will have included (port 53 on this solitary server). In many respects, this is the most secure method of defining access. Referencing each resource granularly in this way permits us to individually control access to these resources. Practically though, this may be difficult and time consuming, and as with so many issues such as this, we have to balance time with security. The other extreme would be to define a resource as the complete network range and define all ports across all protocols. The following is a screenshot of the **Network Resource Properties** window:



General Properties

Name: * All Private

Description: The complete private network

□ Log access

Enabled protocols: * ☑ TCP ☑ ICMP

☑ UDP □ Repeater

Port or port range: * 1-65535

Example: 22,80,110-120,8080

Networks list: *

IP Address	Subnet Mask
172.18.0.0	255.255.0.0

Here we define the resource as the complete `172.18` network, defining all ports, both TCP and UDP, as well as ICMP traffic. This then becomes simpler to manage but does not allow for granular access control. We have now just one resource we can allow or deny access to. Undoubtedly, in this extreme situation, we are exposing too many resources, and many should not and need not be accessible through CAG.

The reality is that the common ground will always lie somewhere between the two extremes. Potentially, both of these examples can and will be used. Administrators may need access to the whole network; validate a resource to be defined and permitted to members of the Domain Admins group. A single entity resource to DNS servers may be created as the starting point for other users. Most certainly, access to the DNS will be required before access to other resources is possible. Starting with these two extreme situations may then prove more practical than first thought. Access to other resources for users will be required, but the starting point will be DNS.

> Without any network resources defined, no one will have access to any private resources via CAG's SmartAccess logon points.

When we are designing the IP address range for the `172.18` network, it would be useful if we could group servers used for similar purposes into groups. At the very least, we could say that the `172.18.100.0` network was reserved for DHCP client. Even though DHCP clients would still have a 16-bit subnet mask of `255.255.0.0` issued by the server, we could define `172.18.100.0` as a network resource to exclude, with a subnet mask of `255.255.255.0`. The network resource would include IP addresses from `172.18.100.1` to `172.18.1.254`. We now have an effective way of denying access to the Client DHCP network resource via CAG.

Defining network resources could be implemented with creativity in your subnet masking. The possible solutions are listed as follows:

- `172.18.1.0/24`: XenDesktop
- `172.18.2.0/24`: File server
- `172.18.100.0/24`: DHCP scope

> Remember that defining a **Network Resource** section does not permit or deny access to the resource but allows resources to appear in an **Access Control** list, where they can subsequently be permitted or denied.

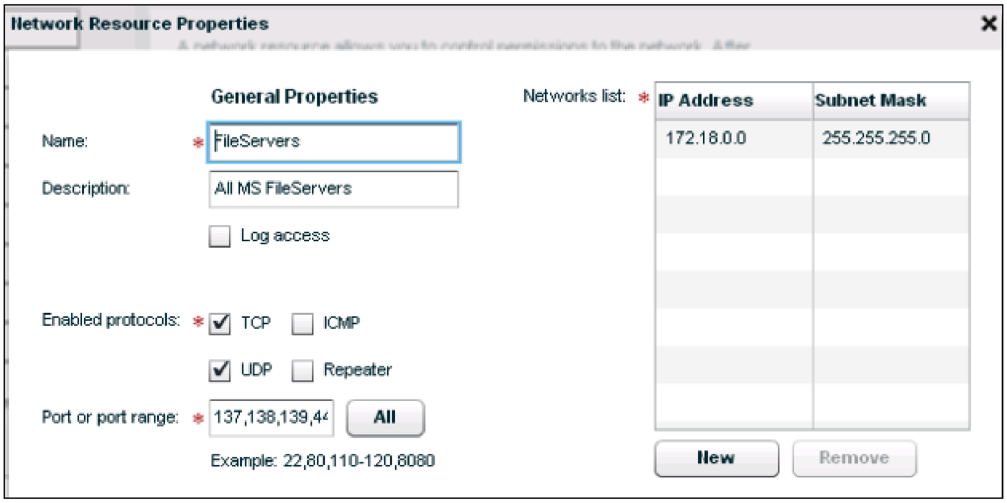
In the network layout that we utilize for `EXAMPLE.COM`, all of our file servers exist on the `172.18.0.0/16` network. Additionally, all of the file server addresses start with `172.18.0`. In this case, we could define a network resource for Microsoft File Servers, on the network `172.18.0.0`, with a subnet mask of `255.255.255.0` or `172.18.0.0/24`.

The ports that are required for file services on a Microsoft Windows Server machine are listed as follows:

Application Protocol	**TCP/UDP**	**Port**
NetBIOS datagrams	UDP	138
NetBIOS name resolution	UDP	137
NetBIOS session	TCP	139
Server Message Blocks (SMB)	TCP	445

We would define both TCP and UDP as the protocols, and the ports would appear as the comma-separated list, – 137, 138, 139, 445.

We would then allow or deny access to this network resource, as required. If we were to allow it, we could have included the DNS resource in the same **Access Control** list, allowing for DNS hostname resolution. The following is a screenshot of the **Network Resource Properties** window:



Network Resource Properties

A network resource allows you to control permissions to the network. After

General Properties

Name: * FileServers

Description: All MS FileServers

☐ Log access

Enabled protocols: * ☑ TCP ☐ ICMP

☑ UDP ☐ Repeater

Port or port range: * 137,138,139,44 All

Example: 22,80,110-120,8080

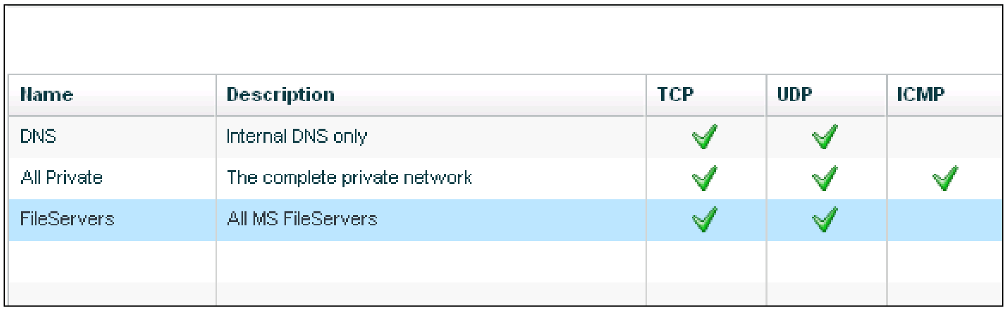
Networks list: *

IP Address	Subnet Mask
172.18.0.0	255.255.255.0

Access control to network resources is managed via SmartGroups.

Resources that we define are likely to be a hybrid mix of granular and more global definitions to provide for an extensible framework for permission assignments.

Examples of defined network resources are shown in the following screenshot:



Name	Description	TCP	UDP	ICMP
DNS	Internal DNS only	✓	✓	
All Private	The complete private network	✓	✓	✓
FileServers	All MS FileServers	✓	✓	

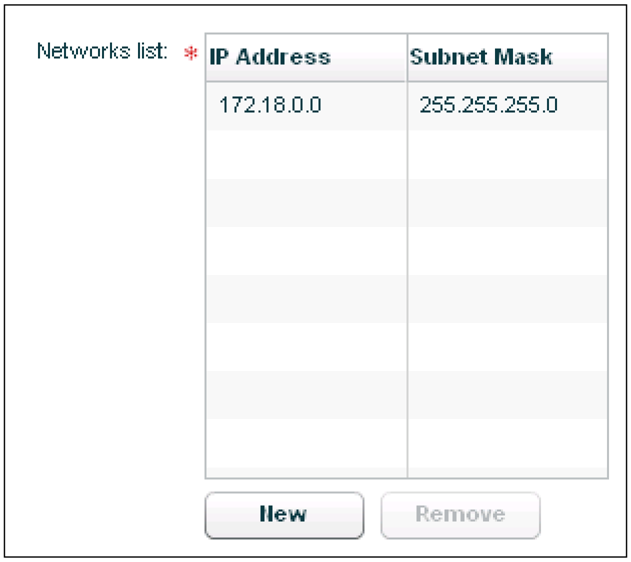
We can now understand a little of how we create these network resources within CAG. So, we will now break down the individual elements.

Network lists

These lists contain one or more networks defined as an IP address and subnet mask. These do not need to represent the actual subnet mask used on the internal network but can allow administrators blocking servers together, as discussed earlier, and could be similar to the following addresses:

- `172.18.0.0/16`: This network acts as our physical network
- `172.18.0.0/24`: This network is for file servers; all host addresses would start with `172.18.0.x/16`
- `172.18.1.0/24`: This network is for XenDesktop virtual machines; all host addresses would start with `172.18.1.x/16`
- `172.18.2.0/24`: This network is for database servers; all host addresses would start with `172.18.2.x/16`
- `172.18.100.0/24`: This network is for internal DHCP client; all hosts addresses would start with `172.18.100.x/16`

All devices are configured on the physical network with the normal 16-bit subnet mask. Careful planning, though, allows us to use the third octet (`0` for file servers, `1` for XenDesktop, and so on), logically grouping devices to allow for accurate and specific network access control. The following is a screenshot of network list:

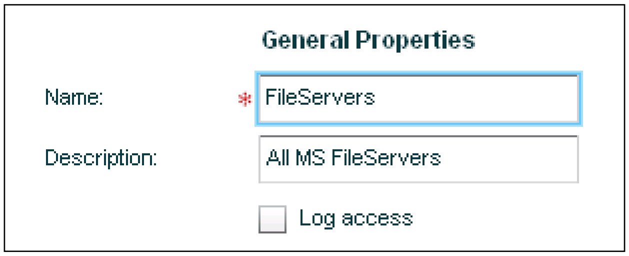


Networks list: *

IP Address	Subnet Mask
172.18.0.0	255.255.255.0

General Properties

In the **General Properties** wizard of **Network Resource**, we can set the name (which is required) and a description (which is optional). You may also remember that, when we looked at basic logon points, we could choose to log access to XenApp and XenDesktop resources; similarly, here we can choose to log access to these resources. Logging is maintained and recorded in the audit log, accessible from the **Monitor** tab of the main web management console. The following screenshot shows the **General Properties** wizard:



General Properties

Name: * FileServers

Description: All MS FileServers

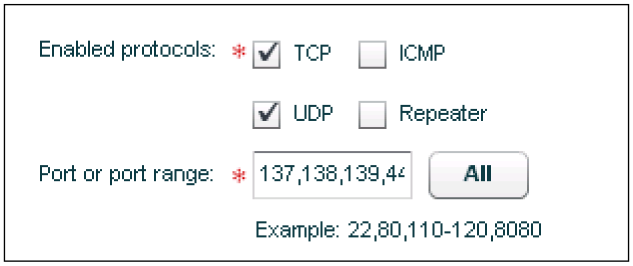
□ Log access

Protocols and port ranges

Finally, we have the enabled protocols and ports that can be included in the network resource. The three usual suspects for the protocols exist, along with Repeater. TCP, UDP, and ICMP represent the main industry transport protocols. Refer to the following list for information about them:

- **TCP** (**Transport Control Protocol**) is a reliable and connection-oriented protocol and is usually associated with upper-level applications that produce larger amounts of network traffic, such as the file-sharing protocol, **SMB** (**Server Message Blocks**). As we can transfer large files, we want a reliable protocol to inform us what has been received and what hasn't.
- **UDP** (**User Datagram Protocol**) is said to be unreliable (but not in a bad way) and connectionless. This is best suited to upper-level applications such as the name resolution services, NetBIOS and DNS. If you do not receive a response the first time, you can easily ask again, and it is far quicker than TCP, which would require connection negotiations.
- **ICMP** (**Internet Control Message Protocol**) is quite different from the other two protocols as it also is the upper-level application. It is most commonly used with the ping program to detect the availability of devices on the network, but is also used in router communications.

- **Repeater** represents traffic from Citrix Branch Repeater Appliance or plug-in, which is used to optimize WAN traffic. Remote users can use the Branch Repeater plug-in to optimize their bandwidth usage between themselves at home and their Branch Office Appliance, giving faster access to those remote users; this is discussed in the next subsection. Ports represent the upper-layer protocols, such as HTTP on port 80, and so on. Port ranges can be added in comma-separated strings. For example, we could construct a network port list similar to **22,80,110-120,8080**. This list would include the following ports:
    - Port 22
    - Port 80
    - Ports 110 to 120 (both inclusive)
    - Port 8080



Enabled protocols: * ☑ TCP □ ICMP

☑ UDP □ Repeater

Port or port range: * 137,138,139,44

Example: 22,80,110-120,8080

Introducing the Citrix Branch Repeater

One of the protocols we can detect is Repeater. This represents traffic using the Citrix **high definition user experience** (**HDX**) WAN optimization protocol. This is categorized as a wide area network optimization product that operates transparently. Unlike many other similar products, the transparent approach means that tunnelling is not implemented and the upper-level protocols remain visible and controllable through CAG network resources, as well as traditional firewalls.

Citrix Branch Repeater products

Citrix Branch Repeater, much like CAG, can exist as firmware on a physical NetScaler appliance or as a virtual appliance. Additionally, the Citrix Branch Repeater is available to install onto Microsoft Windows Server 2008 or 2008 R2 as a service. Mobile and remote users who are not at a branch office can optimize their communications by using the Branch Repeater plug-in, which will connect into the Branch Repeater server located within the corporate network.

Citrix Branch Repeater optimizes the user experience for all services delivered to branch offices and remote users, including access to their virtual desktops, hosted applications, and multimedia services. This is achieved by caching and compression of data across the WAN.

Service-centric optimization simplifies the way companies assess their network usage, identify and classify their applications and service traffic, prioritize and control service delivery across the WAN, and ensure a high level of service performance and availability across the whole organization.

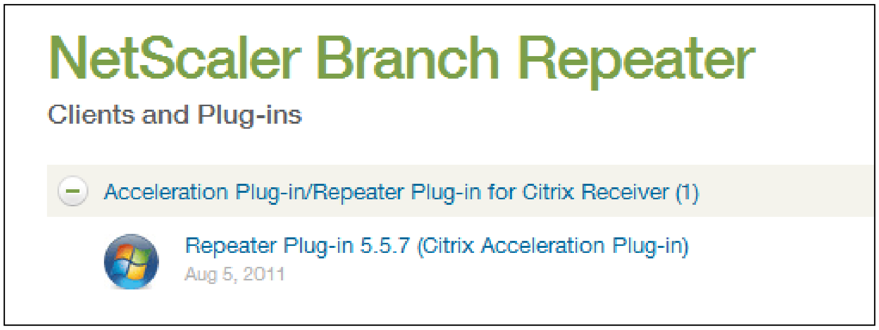
Addressing the full range of corporate user requirements—not just remote users—the Branch Repeater product family delivers unparalleled acceleration and service optimization for applications. This is not limited to just Citrix products such as Citrix XenDesktop and Citrix XenApp but goes beyond their range, stretching to include services needed by many companies, such as Microsoft Exchange and SharePoint, as well as support for protocols such as HTTP, HTTPS, TCP, **CIFS** (**Common Internet File System**), SMBv2, signed SMBv1/v2, **MAPI** (**Mail Application Programming Interface**), and encrypted MAPI.

Our remote users will now need:

- The Citrix Access Gateway plug-in
- The Citrix Endpoint Analysis plug-in
- The Citrix Branch Repeater plug-in

As with most of these plug-ins, deployment via Citrix Merchandising Server becomes a simple one-stop shop for this, easing the administration and user workload involved in deploying and configuring plug-ins. If you need to include this in the standard build, let's say for your laptops, the plug-in may be downloaded from the Citrix website, `http://citrix.com/downloads/netscaler-branch-repeater/clients-and-plug-ins.html`.

Downloading the Repeater plug-in is illustrated in the following screenshot:



NetScaler Branch Repeater

Clients and Plug-ins

Acceleration Plug-in/Repeater Plug-in for Citrix Receiver (1)

Repeater Plug-in 5.5.7 (Citrix Acceleration Plug-in)
Aug 5, 2011

You will notice, as with many products, that this too is a Windows-only plug-in. Combine the plug-in, though, with your Branch Repeater server within your office, and you will find that you can improve your effective bandwidth by up to 30 times.

Citrix calls this technology accelerated orchestration, which consists of the following groupings making up the HDX WAN optimization protocol:

- **Adaptive TCP flow control**: This can adjust the TCP packet six and packet flow to meet the needs of the upper-level applications and network conditions
- **Adaptive Compression**: This, as the name suggests, is able to compress packets to meet the needs of the application and network conditions
- **Adaptive Protocol Acceleration**: This works specifically with XenApp and XenDesktop in tuning the ICA streams from the client to the server
- **Traffic Prioritization and Quality of Service**: This allows us, as administrators, to assign priorities and QoS tags to protocol and addresses to ensure best results where specifically needed

As mentioned earlier, this is transparent to routers and CAG. Just the transport protocol is recognized as Repeater traffic in place of TCP or UDP, the upper-level protocols remain visible and completely under our control, both at CAG and on our firewalls.

Branch Repeater was a very popular product when bandwidth costs were high. It is still popular today and will remain so even though the cost of bandwidth has reduced a lot. The more bandwidth we have, the more we want to use it!

If you choose the VPX edition of Branch Repeater, the virtual appliance may be imported into the CAG, XenServer, or VMware environments. The virtual appliance requires 100 MB of disk space, 2 GB of RAM, and 1-Gbps NIC. The VPX Express edition is free and works with just 1 GB of RAM. The paid options represent how much bandwidth you can optimize and measures it in Mbps:

- 2 Mbps
- 10 Mbps
- 45 Mbps

The cost of these virtual appliances starts at $4,000 for the 2-Mbps unit and touches $13,000 for the 45-Mbps unit (current prices at the time of this writing).

Summary

This chapter has seen us discover network resources within CAG. We have seen how these are used to define elements of our private network to which we would like to control access. Without any network resources, we are unable to access any network services located within our secured private network.

We have seen how we can detect traffic of different data types, including the optimized traffic of the Citrix Branch Repeater.

In the next chapter, we will look at defining the SmartAccess logon points. These are almost the final piece within our CAG jigsaw. We will investigate creating the logon points and controlling visibility from the logon point to the device profiles, enabling messages so that feedback may be sent to devices that do not meet the requirements.

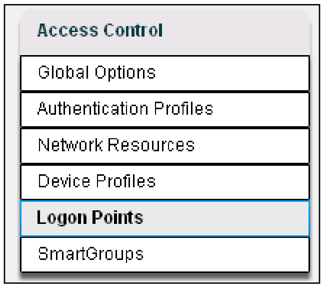
10
SmartAccess Logon Points

In this chapter, we will delve a little further and create SmartAccess logon points to use with our universal licenses. This will allow for full VPN access to our private network, acting as the penultimate cog in the mechanism that secures our network. This will culminate in the next chapter, with SmartGroups. While defining the SmartAccess logon point, we can choose the visibility level, which can enable feedback for users whose devices fail endpoint analysis checks implemented through device profiles; this was investigated in earlier chapters. In this chapter we will see:

- Defining SmartAccess logon points
- Defining logon point visibility
- Branding the logon point

Defining SmartAccess logon points

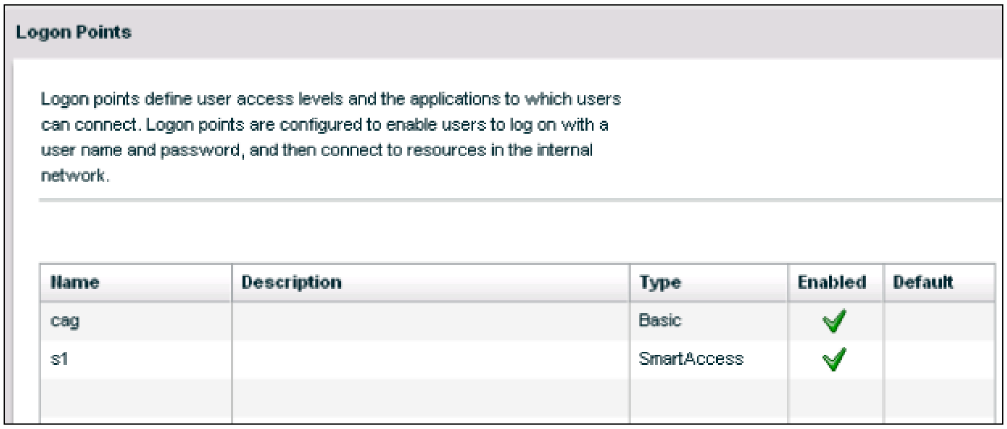
We can return to some initial configuration that we looked at in earlier sections pertaining to logon points. But this time, instead of a basic logon point, which we looked at in *Chapter 2*, *Licensing the Citrix Access Gateway*, we will create SmartAccess logon points to support the full VPN access to our private network. We can see from the **Access Control** section that **Logon Points** are just one item from the bottom; we are nearing completion of our configuration. The following is a screenshot of the **Access Control** section:



When defining the logon point and selecting **SmartAccess** from the drop-down menu, we are able to complete many more entries in the properties page and not just the website configuration we saw with basic logon points. Once created, we can see the logon points listed by name and type.

Logon points may be defined as basic (ICA Proxy only) or SmartAccess for full VPN.

The following is a screenshot of the **Logon Points** window:



Logon Points

Logon points define user access levels and the applications to which users can connect. Logon points are configured to enable users to log on with a user name and password, and then connect to resources in the internal network.

Name	Description	Type	Enabled	Default
cag		Basic	✓	
s1		SmartAccess	✓	

For simple access to XenApp or XenDesktop servers, the basic logon point will be enough, and only a platform license is required. However, for full VPN access, we will need to implement the SmartAccess logon point with platform universal licenses. The following table summarizes the features and license requirements of each logon point type:

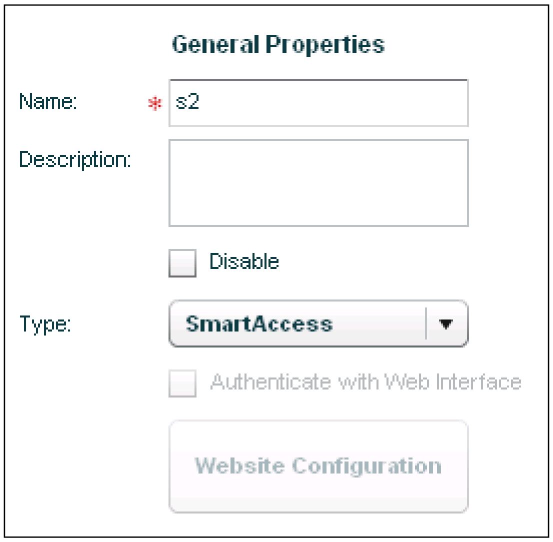
Features	Logon Point Type	
	Basic	**SmartAccess**
Authenticate at Web Interface	Yes	No
Website Configuration	Yes	No
Authenticate at CAG	Yes	Yes
Authorization	No	Yes
EPA with device profiles	No	Yes
License required	Platform only	Platform and universal
ICA Proxy only to XenApp / XenDesktop	Yes	No
Full VPN	No	Yes

General Properties

The **General Properties** section allows for the name and description of the logon point. The name, as before, makes up part of the URL needed for clients to gain access. Unlike the basic logon point, we do not configure the website or home page here. These will be done in the SmartGroups.

The **Type** drop-down list allows us to select between the **SmartAccess** and **Basic** logon points. The **Disable** checkbox allows for the logon point to be disabled without losing any of the logon point settings.

When setting the **SmartAccess** logon points, we configure the website as shown in the following screenshot:



General Properties

Name: * s2

Description:

□ Disable

Type: SmartAccess ▼

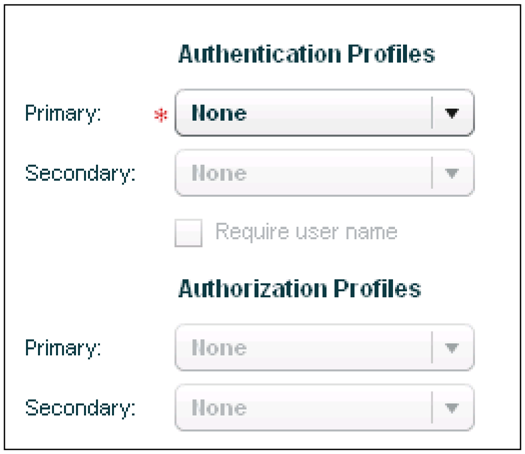
□ Authenticate with Web Interface

From this, we can also see that, when using **SmartAccess** logon points, authentication must occur at CAG and cannot be passed through to the WI server.

> Authenticating at the first point of contact should always be your preference, irrespective of what your **Basic** or **SmartAccess** logon points are, and is considered best practice.

Authentication

Authentication takes place from CAG when using SmartAccess logon points. When defining the logon point, we select the authentication profiles to include it. In addition to this authentication, we can now add authorization. Authorization profiles look at the group membership of the authenticated users, and subsequently, we can choose to use this as part of our site's access mechanism, allowing some groups but not others. Although authentication profiles could be used within a basic logon point, authorization is not possible with basic logon points. The following is a screenshot of the **Authentication Profiles** wizard:



Authentication Profiles

Primary: * None

Secondary: None

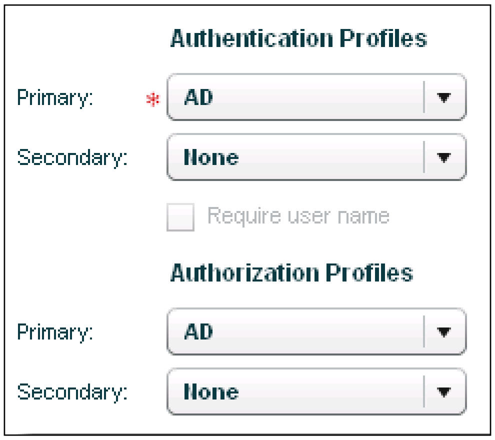
□ Require user name

Authorization Profiles

Primary: None

Secondary: None

To enable authorization, we simply would choose both a primary authentication profile and authorization profile. They can be, and often are, the same profile. Here, we use the **AD** profile pointing to our Microsoft Active Directory LDAP profile, as shown in the following screenshot:



Authentication Profiles

Primary: * AD

Secondary: None

□ Require user name

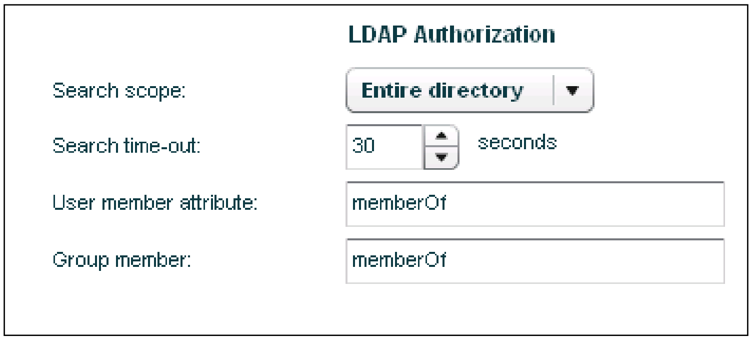
Authorization Profiles

Primary: AD

Secondary: None

Depending on the directory type, the search attribute will differ. However, with Active Directory, group membership is determined by the **memberOf** attribute. If we return to the authentication profile, we can view the group membership attribute from the profile properties of the authorization profile in Active Directory.

Group membership is determined by the **memberOf** attribute in Active Directory, as shown in the following screenshot:



LDAP Authorization

Search scope: Entire directory

Search time-out: 30 seconds

User member attribute: memberOf

Group member: memberOf

Each LDAP directory server maintains its own schema; this schema defines the objects and the attributes of those objects. As we have seen, Microsoft uses the **memberOf** attribute to determine group membership for its user objects. The following table lists other common directory schema supported by CAG.

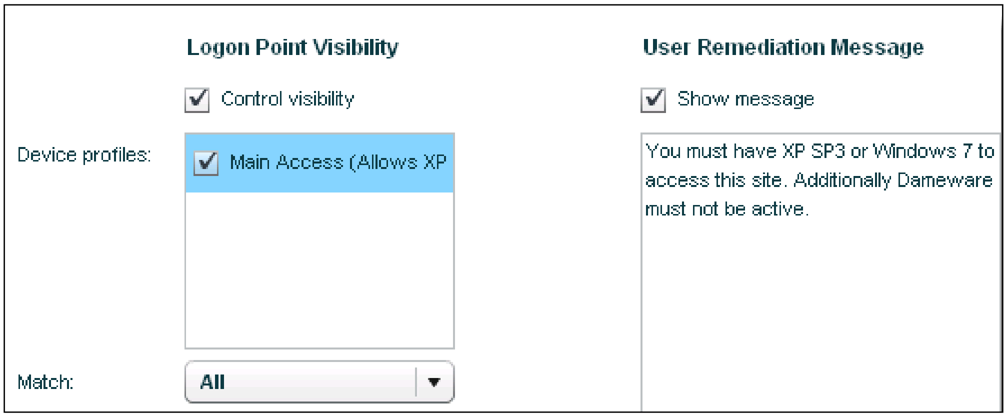
Group membership attributes as used across different directory systems:

Directory server	**Group attribute**
Microsoft Active Directory	memberOf
Novell eDirectory	groupMembership
IBM Tivoli Directory Server	ibm-allGroups
Sun ONE directory	nsRole

The logon point only determines where to look for group membership and not what the group membership should be in order to gain access to the resources. Adding the authorization profile to the SmartAccess logon point allows for the SmartGroup to require certain group memberships for site access. Group names are case insensitive and are defined within the SmartGroup. The group name we set in the SmartGroup must match a group name in our authorization profile, and the user must belong to this group in order to obtain access.

Defining the term Logon Point Visibility

Device profiles provide a mechanism to implement for a level of endpoint analysis, preventing devices that do not meet the required configuration from accessing the private network. Checking the **Control visibility** checkbox for logon point visibility denies access to the logon point itself and not just the resources it points to. The idea is to display a message to the user, so they will understand why their access has been blocked. In this way, the **Logon Point Visibility** and the **User Remediation Message** dialogs work together to provide the user a level of feedback. Device profiles that must be matched are selected once we have checked **Logon Point Visibility**. Additionally, we can choose to match all or any profiles selected.



You must have XP SP3 or Windows 7 to access this site. Additionally Dameware must not be active.

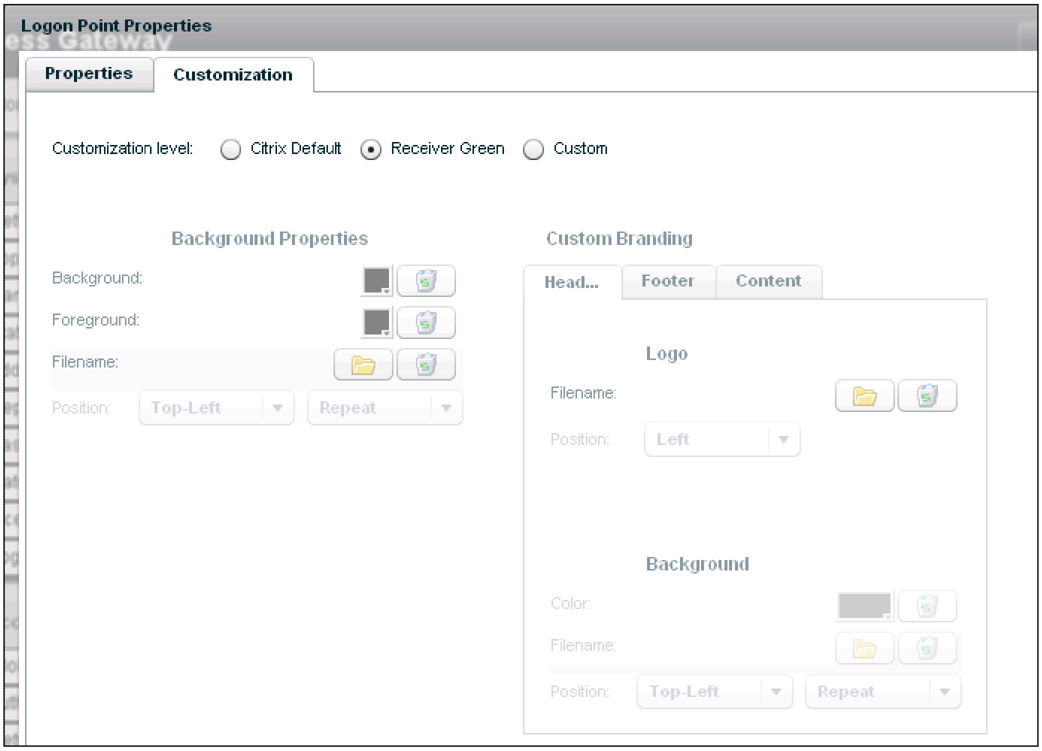
It is possible that we can define more than one SmartAccess logon point. The remediation message of the main site may point users to try the additional SmartAccess logon point. These access points may allow access to lower classification networks and perhaps network file shares that can deploy the required service packs or whatever the client is missing. As with all levels of remote access, correct planning at the early stages can go a long way in providing a useable and effective long-term solution.

Branding the logon point

As with the basic logon point, we can customize the logon point web page that is displayed to the user. Unlike the basic logon point though, users may not regularly visit the web logon point for SmartAccess. As SmartAccess logon points provide VPN access via the CAG plug-in, there is no need for users to visit the web page with a browser. Usually, this would only be required if we wanted to use the SmartAccess logon point to distribute the plug-in. After distributing, access to the network would be made direct from the plug-in to the logon point.

That said though, we still need to ensure that we brand the site, so all pages maintain the same look and feel as other web content we direct users to. We edit the web page's look and feel for the SmartAccess logon point in the same way as with basic logon points, using the **Customizations** tab on the **Logon Point Properties** wizard. This became available in Version 5.04 of the CAG firmware. The default selection is the **Receiver Green** theme. Also, we can select **Citrix Default**, which comprises of two shades of gray, and then our own customized theme, including uploading our own graphics.

Branding of the logon point in CAG 5.04 is shown in the following screenshot:



Logon Point Properties

Customization level: ○ Citrix Default ● Receiver Green ○ Custom

Background Properties

Position: Top-Left Repeat

Custom Branding

Logo

Position: Left

Background

Position: Top-Left Repeat

Summary

We are beginning to finalize the configuration of CAG. We see that, by creating the SmartAccess logon points, we are nearing our goal. We have also seen, from these logon points, that we cannot only control access, but define messages to act as feedback to our users to assist them in locating the correct configuration to gain access.

In the next chapter, we will complete the configuration by looking at SmartGroups, which become the glue that links all these separate components that we have viewed together, finalizing the secure access we need for the private network by using the CAG plug-in.

11
Linking It All Together with SmartGroups

Finally, we are ready to link all of our components together using SmartGroups. In this chapter, we will define SmartGroups and include within those groups the elements that we have discussed building up to this:

- Network resources
- Address pools
- Authorization groups
- Device profiles
- SmartAccess logon points

Add into this the ability with SmartGroups to link into corporate intranet sites for the home page. These include:

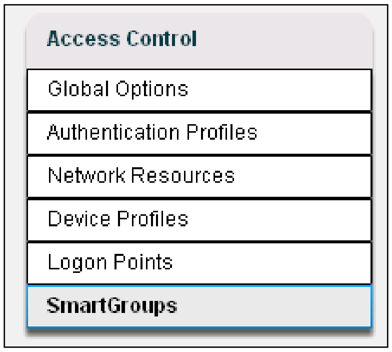
- Citrix WI
- Microsoft OWA 2007/2010
- Microsoft SharePoint Server

The glue is SmartGroups and we cement the knowledge within this section seeing our hard work come together as one unified component. SmartGroups link device profiles, logon points, authorizations (group membership), address pools, and network resources together and control access to those resources based on the user and their device characteristics.

Defining SmartGroups

We can find SmartGroups at the bottom of the **Access Control** section and they do literally link the previous components together.

SmartGroups link components together unifying access to resources:



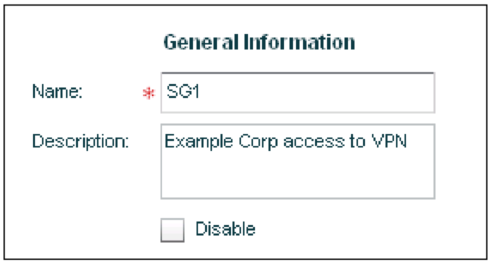
The **SmartGroups** component then becomes the final piece to fit into our jigsaw, linking all of the SmartAccess components as one.

The **SmartGroups** link components come together to provide secure remote access; the objects they link are shown in the following table:

SmartGroups				
Device Profiles	SmartAccess Logon Points	Address Pools	Network Resources	Authorization Groups

General Information

When completing the **SmartGroups** properties, the first section to run through, like before, is the **General Properties** section. Here we set the name, description, and we have the option to enable and disable the SmartGroup temporarily if required, as shown in the following screenshot:


General Information

Name: * SG1

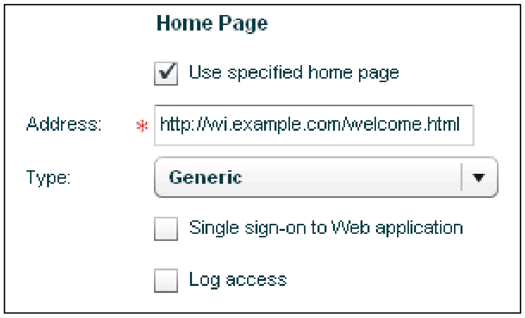
Description: Example Corp access to VPN

□ Disable

Home Page

A user may not regularly visit the home page of the SmartAccess logon point, for example, if they only use the CAG plug-in to access the VPN, they do not have to access the home page of the SmartAccess logon point. However, if you need people to visit the home page of your site regularly, it is possible, through the **Home Page** section of the SmartGroup, to redirect users through to a web resource. In this way, we enforce the business process that users should visit the corporate intranet on a regular basis.

In the following screenshot, we redirect users to a **Generic** web page if they have successfully authenticated to the SmartAccess logon point associated to the SmartGroup:



Home Page

☑ Use specified home page

Address: * http://wi.example.com/welcome.html

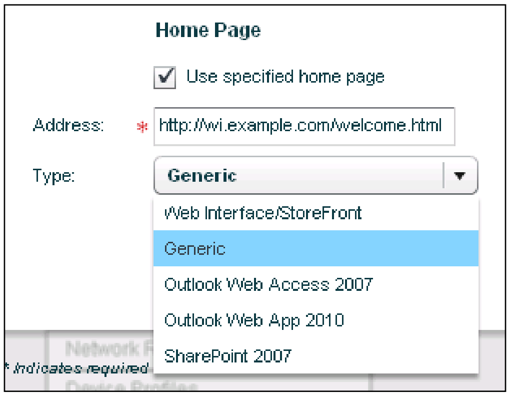
Type: Generic ▾

□ Single sign-on to Web application

□ Log access

You can see that it may be possible, depending on the website type, that single sign-on can be used and we can log access to the web page through the audit log that is accessible on the **Monitor** page of the CAG web console. The website type that we can redirect users to include Citrix and Microsoft-specific services.

The following screenshot shows the specific website types that can be included using the drop-down list:



Home Page

☑ Use specified home page

Address: * http://wi.example.com/welcome.html

Type: Generic ▾

- Web Interface/StoreFront
- Generic
- Outlook Web Access 2007
- Outlook Web App 2010
- SharePoint 2007

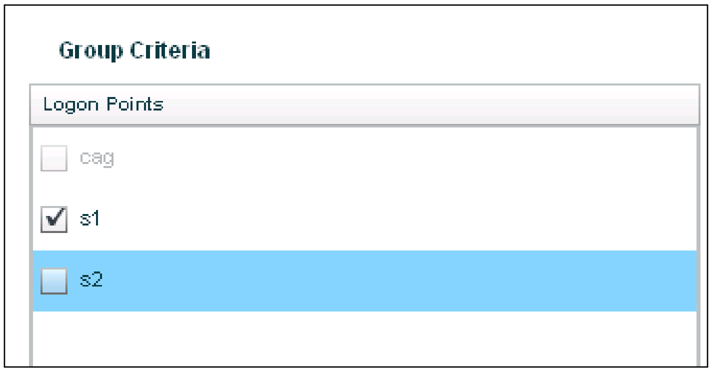
The home page, though, is used only when accessing the logon point using a browser, and not when accessing the logon point using the CAG plug-in. Access is always made to the logon point when using either the browser or plug-in and never the SmartGroup itself.

Group Criteria

On the **SmartGroups** properties page, we can start to link the previously created objects such as **Device Profiles** using the **Group Criteria** section.

Logon Points

One or more SmartAccess logon points can be selected for each SmartGroup. Notice that the previously created basic logon point `cag` cannot be selected to be used within a SmartGroup definition. We cannot use the logon point named `cag`, as this is a basic logon point. We looked at basic logon points earlier in the book in *Chapter 4*, *Configuring a Basic Logon Point for XenApp/XenDesktop*, and we should be familiar that these provide ICA Proxy access only and do not make up any port of SmartAccess. SmartAccess logon points can be used with SmartGroups and all of the extra associated features that they offer. The following screenshot shows linking of SmartAccess logon points:



Group Criteria

Logon Points

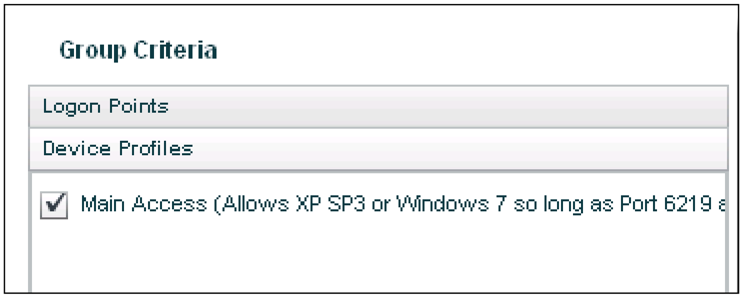
□ cag

☑ s1

□ s2

Device Profiles

Next on the list, below the **Logon Points** tab, we can link to the **Device Profiles** section. The **Device Profiles** tab selected here has no impact on the visibility of the logon point; device profiles linked here just control access to the network resources we specify within the SmartGroup. We can again link one or more device profiles. The following screenshot shows the linking of device profiles:



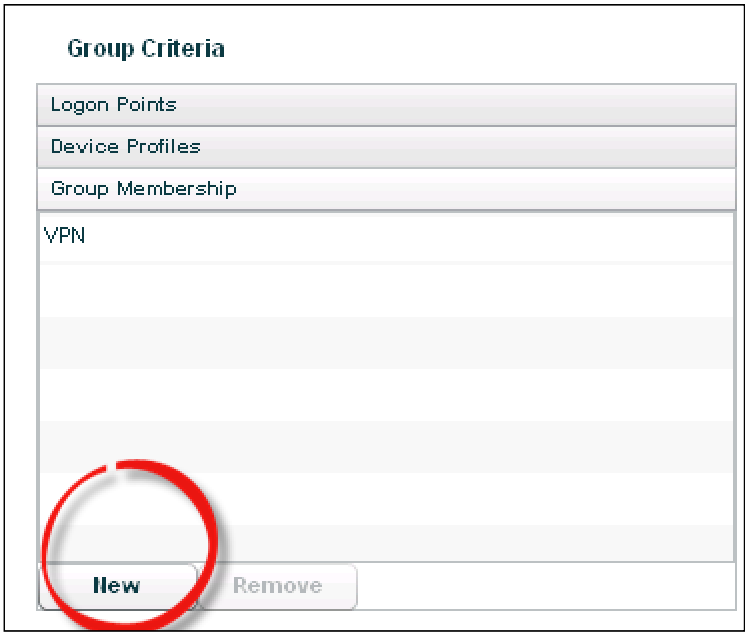
Group Criteria

☑ Main Access (Allows XP SP3 or Windows 7 so long as Port 6219 a

Group Membership

The final tab with the **Group Criteria** section is the **Group Membership** tab. This is where we can take advantage of the authorization profiles we reference within SmartAccess logon points.

Authorization profiles are used from the **Group Membership** tab. In this case, only members of the VPN group are permitted access:



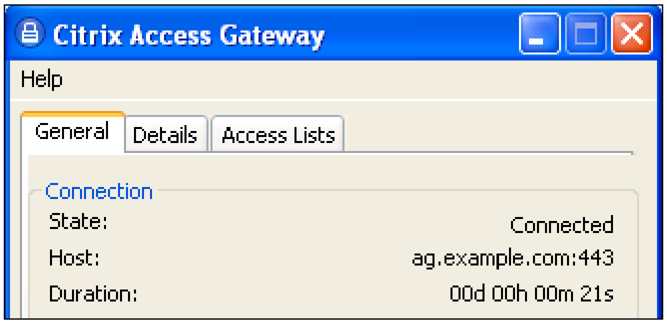
Group Criteria

VPN

Using the button labeled **New**, we can reference the group name that we want to be allowed to access this SmartGroup. The group name that we add here must match a group name in our authorization profiles. The name is not case sensitive. We can see that the group named **VPN** is referenced here. Only members who belong to the Active Directory group **VPN** will be allowed access to resources protected with this SmartGroup. We know that this is an Active Directory group, as our authentication profile is from Active Directory. Other Directory systems can be used and you may wish to review *Chapter 5*, *Creating Authentication Profiles*.

If access is authorized with correct group membership, the connection status of the CAG plug-in will display the three tabs.

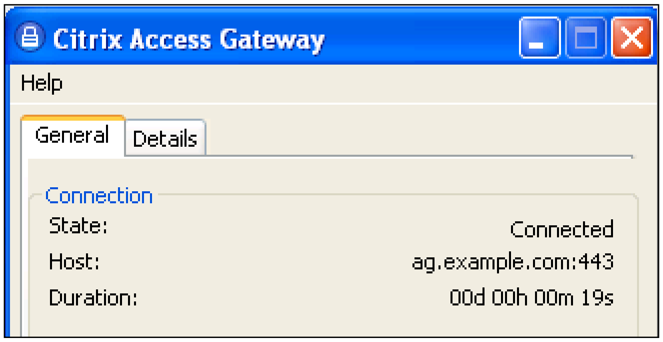
When authorization is successful, we see three tabs from the client, as shown in the following screenshot:



State: Connected
Host: ag.example.com:443
Duration: 00d 00h 00m 21s

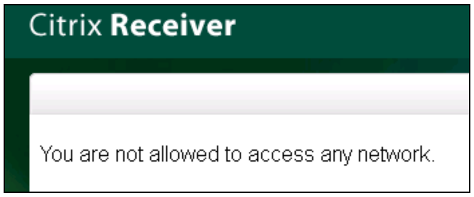
Should the user not belong to the correct group, then authorization will fail. We can view the effects from the **Connection Status** tab of the CAG plug-in; the **Access Lists** tab will be missing.

Authorization has failed, and we can see that there is no **Access List** tab displayed in the client now, as shown in the following screenshot:



State: Connected
Host: ag.example.com:443
Duration: 00d 00h 00m 19s

Additionally, if we tried to log on to the logon point using the website, `https://ag.example.com/lp/s1`, we would be shown that we had no access to any resources, indicating, in this case, that the group authorization has failed. When authorization fails, the following screenshot appears:



You are not allowed to access any network.

It is authorization failing here, not authentication. The correct username and password has been entered, but the group membership does not meet the requirements.

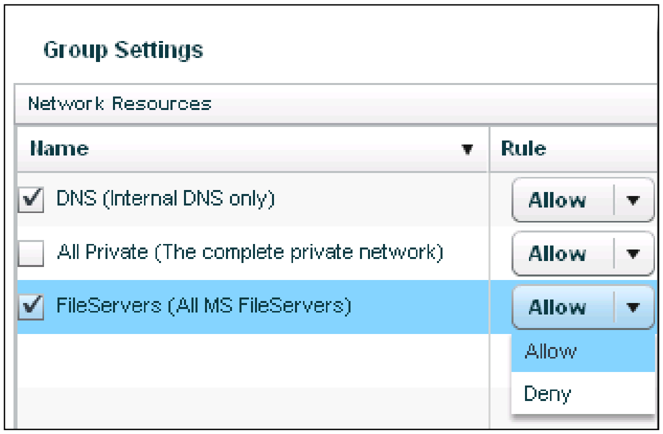
Group Settings

The last section we have access to via the **SmartGroups** properties is the **Group Settings** section found on the far right-hand side of the property pages. From here, we can then link, upon successful authentication and authorization, the user to network resources, address pools, and configure settings for their sessions.

Network Resources

Here, we can select previously defined network resources. Also, we can choose to allow or deny access to these resources.

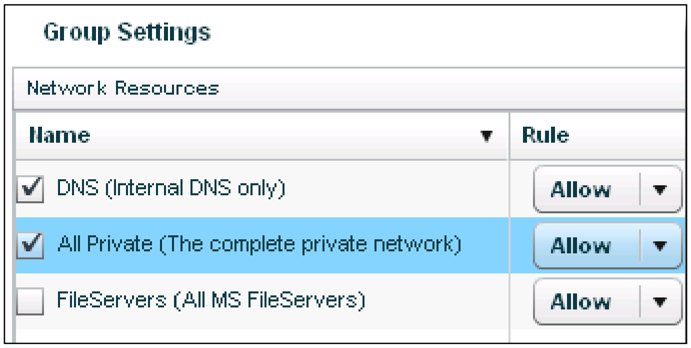
From the following screenshot, you will notice that it is possible to control access to network resources that we have previously defined:



Name	Rule
☑ DNS (Internal DNS only)	Allow
□ All Private (The complete private network)	Allow
☑ FileServers (All MS FileServers)	Allow

If a network resource is not selected, it is neither allowed nor denied. It is possible that a user may gain access to a resource if it is included within another resource definition. However, if it is explicitly denied, then access to the resource is not allowed even if it is mentioned elsewhere.

From the following screenshot, you may see that we have explicitly allowed access to the network resources – **DNS (Internal DNS only)** checkbox and **All Private (The complete private network)** checkbox. All Private network resources allow access to the complete private network. So, even though we have not selected the **FileServers (All MS FileServers)** checkbox, access to the resources listed in file servers network resources is permitted by means of the **All Private (The complete private network)** network resource.

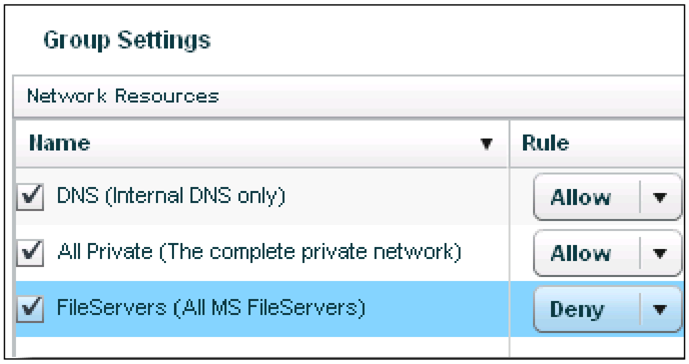


Group Settings

Network Resources

Name	Rule
☑ DNS (Internal DNS only)	Allow
☑ All Private (The complete private network)	Allow
□ FileServers (All MS FileServers)	Allow

However, if we select all three network resources and explicitly deny access to the **FileServers (All MS Fileservers)** network, then access will not be permitted to those resources.

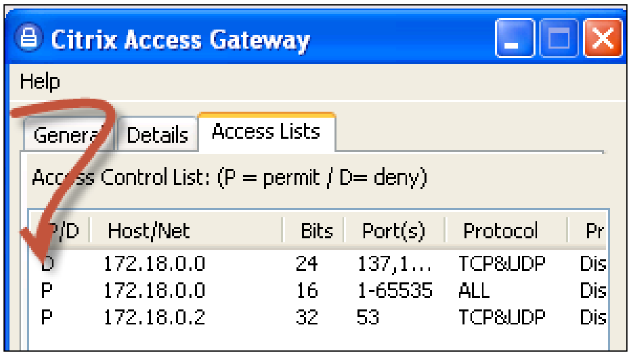


Group Settings

Network Resources

Name	Rule
☑ DNS (Internal DNS only)	Allow
☑ All Private (The complete private network)	Allow
☑ FileServers (All MS FileServers)	Deny

In the previous screenshot, access to the **FileServers (All MS Fileservers)** network is denied as they have been explicitly marked as such. A user can confirm their access by using the **Connection Status** tab of their CAG plug-in. The **Access Lists** tab will show which resources they have access to as well as those that are denied. The following screenshot shows the level of access marked with a letter **P** for **permit** and a letter **D** for deny:

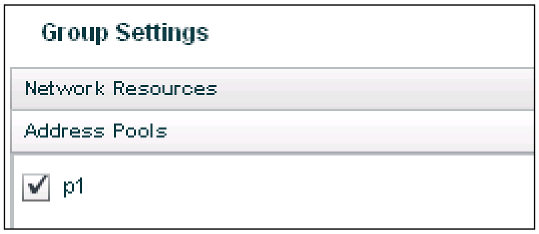


Access Control List: (P = permit / D= deny)

P/D	Host/Net	Bits	Port(s)	Protocol	Pr
D	172.18.0.0	24	137,1...	TCP&UDP	Dis
P	172.18.0.0	16	1-65535	ALL	Dis
P	172.18.0.2	32	53	TCP&UDP	Dis

Address Pools

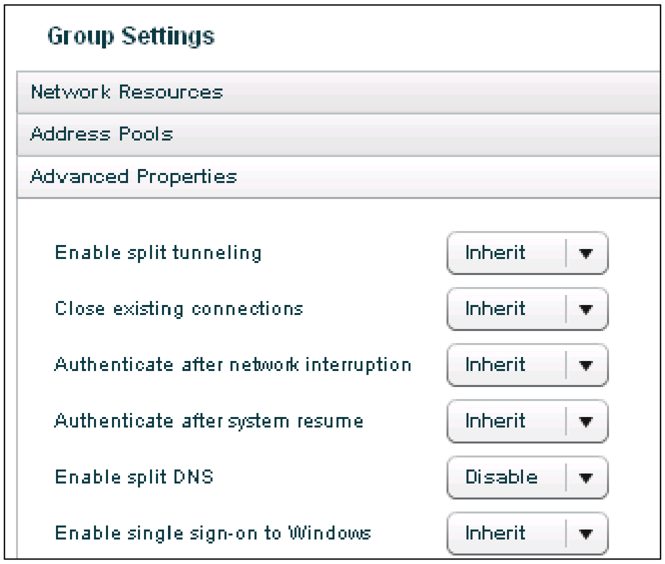
From the **Address Pools** node in the **Group Settings** tab, we can choose to include previously defined address pools. If we remember, address pools can be used where resources may not allow multiple connections from a single IP address. If address pools are not implemented, all access is gained by using the IP address of CAG. The linking of address pools is shown in the following screenshot:



☑ p1

Advanced Properties

Using the advanced properties, we can choose to control settings that are inherited from the global settings of CAG. These affect the usage of network resources and session control. The following screenshot shows the advanced properties:

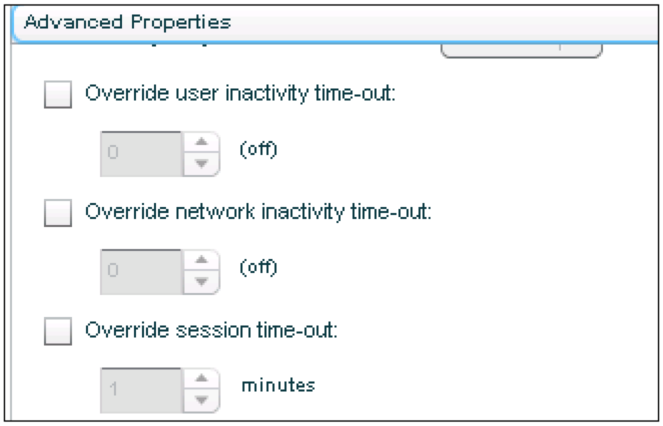


Enable split tunneling	Inherit
Close existing connections	Inherit
Authenticate after network interruption	Inherit
Authenticate after system resume	Inherit
Enable split DNS	Disable
Enable single sign-on to Windows	Inherit

- **Enable split tunneling**: This listbox controls which traffic is sent via the VPN. When split tunneling is enabled, all traffic is sent out on the client's local network except the traffic that is addressed to a destination defined in the SmartGroup.
- **Close existing connections**: This will terminate any existing connections for a user when the user connects a second time without having previously logged off. This will ensure that each client uses just one universal license and one connection.
- **Authenticate after network interruption**: This determines whether or not authentication is required, should the user's connection have been disrupted temporarily such as is common with mobile networks or switching between wireless access points.
- **Authenticate after system resume**: As with the previous setting, you can require that users log on after interruptions, such as when a computer comes out of hibernation or standby, as well as when the user switches to a different wireless network, or when a connection is forcefully closed.

- **Enable split DNS**: With this enabled, the user can access the DNS server defined on CAG to resolve names that match the DNS suffix of CAG. For us, this would mean that `example.com` would be resolved to the DNS server on the private network.
- **Enable single sign-on to Windows**: Our users typically open a connection to CAG by starting the CAG plug-in. We can specify that the CAG plug-in starts automatically when the user logs on to Windows by enabling single sign-on with Windows. When we configure single sign-on, the user's Windows logon credentials are passed to CAG for authentication.

Below these settings, we can configure timeouts for the user sessions. These again would be inherited from the global settings and are configured to 30 minutes for each setting, as shown in the following screenshot:



Advanced Properties

□ Override user inactivity time-out:

0 (off)

□ Override network inactivity time-out:

0 (off)

□ Override session time-out:

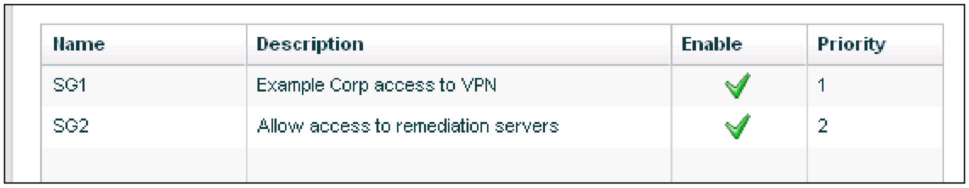
1 minutes

- **Override user inactivity time-out**: This detects the absence of keyboard or mouse input.
- **Override user network time-out**: This detects the absence of any network activity to and from the client device.
- **Override session time-out**: If this is not adjusted, then the sessions will have a maximum length of 30 minutes, as set in the global options. It would be reasonable to override at least this setting to ensure users have adequate opportunity to complete their tasks. Configuring a value of **0** is not permitted for this option, configuring a value of **1440** minutes allows a connection to last for 24 hours.

Defining SmartGroup priority

With careful planning, we will design a system to work seamlessly with our user devices. We can expect that users, from time to time, will access the network with devices that do not meet the EPA scans for the network. Creating multiple SmartGroups that utilize the single SmartAccess logon point can allow the device to be redirected to other resources such as remediation servers. These remediation servers allow service packs to be installed or virus software to be configured. The priority of a SmartGroup determines the order in which it is evaluated.

From the following screenshot, we would attempt to access **SG1**. If we fail this, we would be passed through the **SG2** SmartGroup, the SmartGroup with the next priority level down. The following screenshot shows multiple SmartGroups with priority levels:

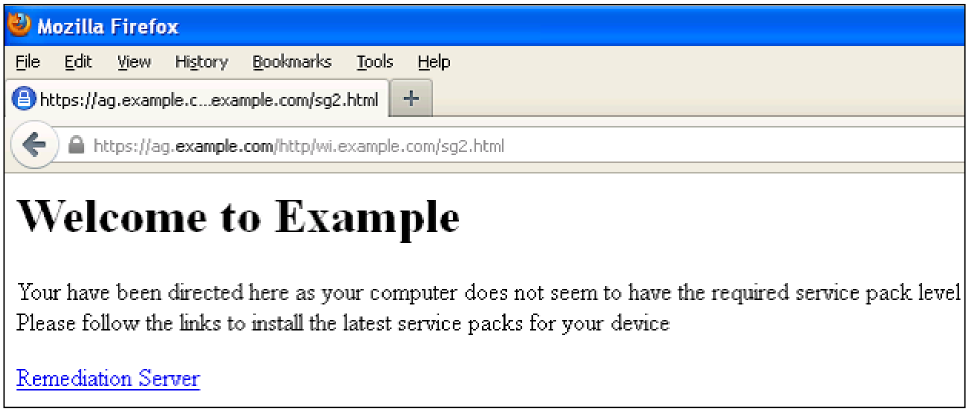


Name	Description	Enable	Priority
SG1	Example Corp access to VPN	✓	1
SG2	Allow access to remediation servers	✓	2

If we fail to meet the requirements for **SG1**, then we will try **SG2** and so on, if we add more; the operation is totally transparent to the user. The SmartGroup **SG2** would have a home page that explains to users why they have been quarantined there and what they need to do to improve the health of their device. The network resources would allow access to the DNS server and perhaps network file shares on remediation servers so that virus protection could be installed or service packs added.

The users would still access the same logon point **s1**; the single URL would be able to redirect to the resources within **SG1** or **SG2**. The URL to access the logon point is `https://ag.example.com/lp/s1`.

The SmartAccess logon point **s1** would be referenced in both the **SG1** and **SG2** SmartGroups. Failing to meet the device profile requirements for **SG1** will then fail us over to **SG2**. The homepage for **SG2** would point to the remediation home page. Following is the screenshot of the remediation home page:



Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://ag.example.c...example.com/sg2.html
+
https://ag.example.com/http/wi.example.com/sg2.html

Welcome to Example

Your have been directed here as your computer does not seem to have the required service pack level
Please follow the links to install the latest service packs for your device

Remediation Server

Using effective prioritization of our SmartGroups will allow for less help desk calls and easier long-term management, as we are able to automate the provision of resources based on the endpoint analysis of the users' device without intervention from ourselves or the user.

Summary

In this chapter, we have learned how to configure SmartGroups and link our components together to create a secure and reliable remote access solution. SmartGroups link the individual elements of the complete VPN SmartAccess solution together into a cohesive unit, even providing failover to allow devices not meeting requirements to be remediated.

In the next chapter, we will look at how we can use the SmartAccess logon points to deploy the plug-in and how we can access resources on the VPN network.

12
Connecting to SmartAccess Logon Points

In this section, we get to grips with using SmartAccess logon points. To start with, we shall see that it is possible to deliver the CAG plug-in from the logon point, should we so wish. Once we have the plug-in, we can see how we can gain VPN access to our private network and adjust settings as required along the way. In this chapter we will cover:

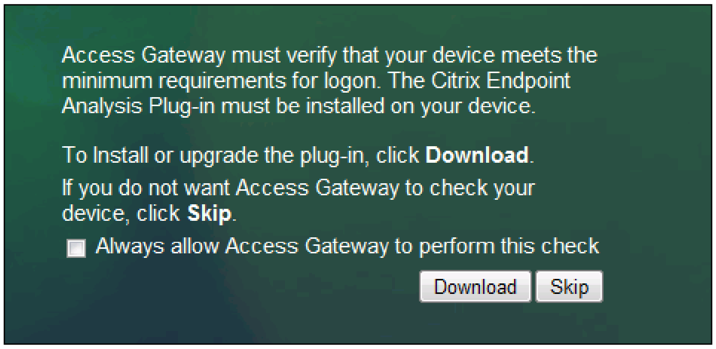
- Delivering the plug-in from a SmartAccess logon point
- Configuring plug-in settings
- Connecting to private resources

Delivering the Access Gateway plug-in

In earlier sections of this book, we saw that we can deliver the CAG plug-in using Merchandising Server or simply by downloading it from the Citrix website. However, if a user uses a browser for their initial contact with CAG, the SmartAccess logon point will deliver the plug-in if it is not installed. Additionally, if we as administrators have set device profiles to be enforced prior to access, Endpoint Analysis Plug-in will be installed.

In the first instance of attempting to access a smart logon point with a web browser, if device profiles have been enabled in the SmartGroup, we will be asked to install the Citrix Endpoint Analysis Plug-in.

If device profiles are enabled, we will need the Endpoint Analysis Plug-in:



Access Gateway must verify that your device meets the minimum requirements for logon. The Citrix Endpoint Analysis Plug-in must be installed on your device.

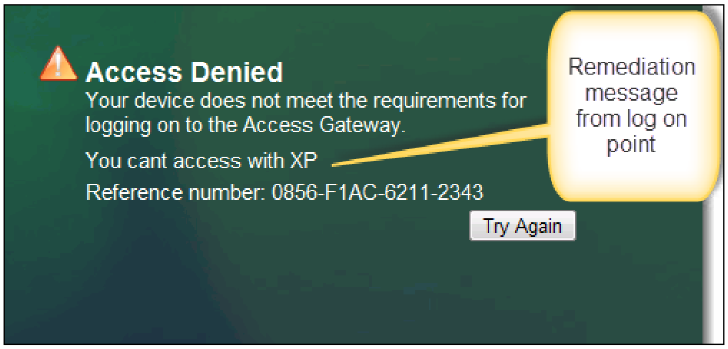
To Install or upgrade the plug-in, click **Download**.

If you do not want Access Gateway to check your device, click **Skip**.

□ Always allow Access Gateway to perform this check

Choosing the **Download** option would allow us to install. Choosing the **Skip** option would cause us to fail the analysis test and the remediation message would be shown. We have to bear in mind here that the remediation message we would see would be that which we had declared in the logon point and is not generated specifically for the Endpoint Analysis Plug-in's not being present. So, consider this as part of your help desk training; do not forget to always check for the presence of the EndPoint Analysis Plug-in when the remediation message is shown.

The following screenshot shows the remediation message for a device that does not meet the EPA requirements set in the device profile associated with the logon point:



Access Denied

Your device does not meet the requirements for logging on to the Access Gateway.

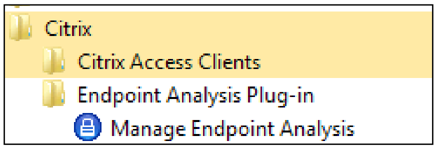
You cant access with XP

Reference number: 0856-F1AC-6211-2343

If we needed to check whether the Endpoint Analysis Plug-in was installed, the most simple way would be to use the **Start** menu in Windows. The presence of the EndPoint Analysis Plug-in can be checked for via **Start** | **All Programs** | **Citrix**. Remember that, currently, this is a Microsoft Windows only plug-in:

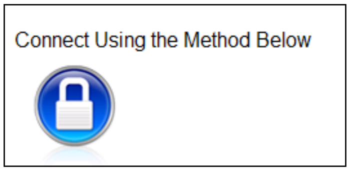
To access the EndPoint Analysis management program, we can choose **Start** | **All Programs** | **Citrix** | **Endpoint Analysis Plug-in** | **Manage Endpoint Analysis**.

Check to see whether the Endpoint Analysis Plug-in is installed. Refer to the following screenshot:



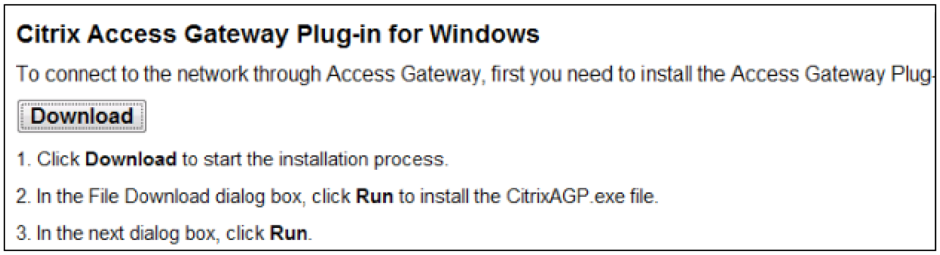
Of course, if device profile checks are not in place, the user can connect directly to the logon point without interruption. If checks are implemented and the client now has the Endpoint Analysis Plug-in, and if they meet the criteria, they too are directed to the logon point where they are shown an icon of a padlock. Users are meant to recognize this as the CAG plug-in.

The padlock icon represents the download of the CAG plug-in, and is shown in the following screenshot:



Clicking on the padlock allows users to download and install the plug-in. They will use the plug-in to gain access to the VPN network in most cases.

Clicking on the icon will show instructions on installing the plug-in.



Citrix Access Gateway Plug-in for Windows

To connect to the network through Access Gateway, first you need to install the Access Gateway Plug-

1. Click **Download** to start the installation process.
2. In the File Download dialog box, click **Run** to install the CitrixAGP.exe file.
3. In the next dialog box, click **Run**.

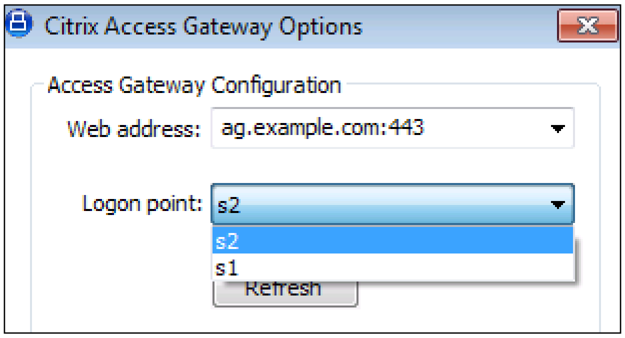
Configuring Access Gateway Plug-in settings

Once the plug-in is installed, it may be accessed from the computer's start menu. Before this, though, we can scan for available logon points, so we know where we can connect.

Choose **Start** | **All Programs** | **Citrix** | **Citrix Access Clients** | **Citrix Access Gateway** | **Properties**.

From **Citrix Access Gateway Properties**, we can add the address of CAG, and then, using the **Refresh** button, logon points defined on the server are displayed.

Locating SmartAccess logon points on the server is made simple by using the CAG options, as shown in the following screenshot:



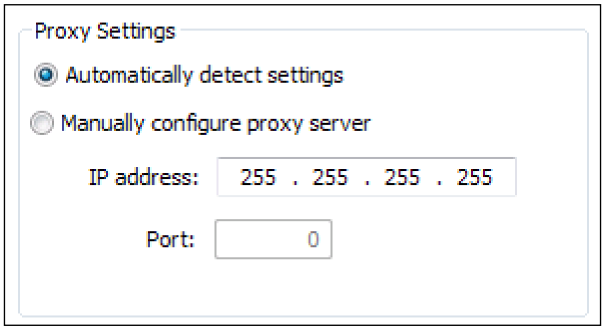
Citrix Access Gateway Options

Access Gateway Configuration

Web address: ag.example.com:443

Logon point: s2

If the client needs to connect to the Internet using a web proxy server, this too can be configured on this page, directly below the address configuration. The default settings will allow for the proxy to be automatically detected; if this is not working for your environment, a specific proxy is required for the VPN. Then, we can choose to manually enter the proxy. The following is a screenshot of the **Proxy Settings** wizard:



Proxy Settings

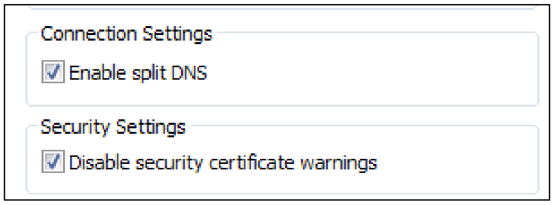
● Automatically detect settings

○ Manually configure proxy server

IP address: 255 . 255 . 255 . 255

Port: 0

The final settings on the **Citrix Access Gateway Options** page allow for the user to select split DNS and to enable or disable certificate warnings. If the **Enable split DNS** option is checked, DNS name resolution is first performed on the DNS server from CAG. With **Enable split DNS** disabled, name lookups are only performed on the CAG DNS server and not the client, when connected to the VPN network.



Connection Settings

☑ Enable split DNS

Security Settings

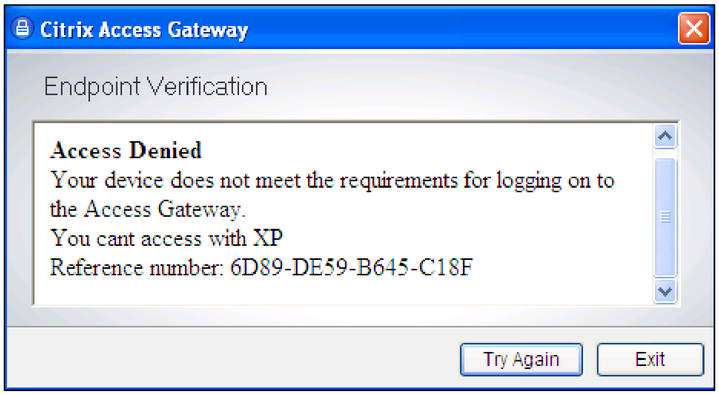
☑ Disable security certificate warnings

Having selected the desired client options, and with the SmartAccess logon point configured, we can now connect to VPN. If we have Citrix Receiver installed, we can access the plug-in via the Receiver icon in the system tray. If we do not have the Receiver installed, and if it is not required, we can access the plug-in from the start menu.

Choose **Start** | **All Programs** | **Citrix** | **Citrix Access Clients** | **Citrix Access Gateway**.

When connecting to a logon point with **Control Visibility** enabled, we will notice that the endpoint analysis checks will run even before we are prompted to log on. If we meet the requirements, we are prompted to log on, and if we don't, a message is displayed along with the remediation message if this has been configured.

The remediation message is displayed if we set control visibility.



Access Denied
Your device does not meet the requirements for logging on to the Access Gateway.
You cant access with XP
Reference number: 6D89-DE59-B645-C18F

If we do not meet the requirements and the administrator has not opted to control the visibility in the logon point, we will be prompted to log on. Providing that administrators—that's us—have set multiple SmartGroups, it is possible for us to be redirected to another logon point. This logon point may allow us to access shares to install updates that may be required; in our case, that are accessible to Windows XP.

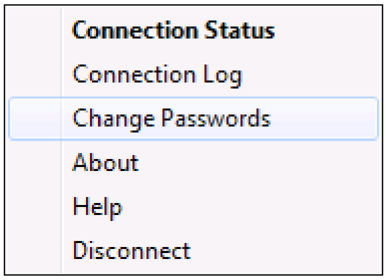
Device requirements and the logon screen behavior are summarized in the following table:

Meet device requirements	Logon point visibility	Logon screen
No	No	Yes
No	Yes	No
Yes	Yes	Yes
Yes	No	Yes

Managing the client plug-in

Once having successfully logged on with the CAG plug-in, it will be displayed in the system tray. We can right-click on the context menu to display information about the connection.

From the context menu of the running plug-in, we can manage our connection, as shown in the following screenshot:

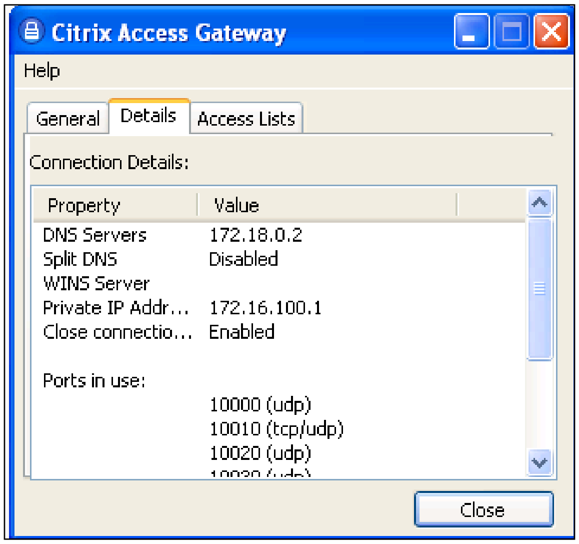


The main element here is the **Connection Status** option. With this option, we can see the connection properties and the resources that we have access to. The following are the connection properties:

- **Connection Status**: This enables us to view how much data we have accessed, the connection settings (including the IP address in use), and resources that we have access to
- **Connection Log**: This displays information about connectivity and the endpoint analysis activity

- **Change Passwords**: It is fairly obvious what this does and will do what it says if password changes have been allowed in the authentication profile
- **Disconnect**: This closes the connection and plug-in when we have finished with the VPM session

From the **Connection Status** menu item, we can view the DNS and IP addresses of our VPN connection, as shown in the following screenshot:

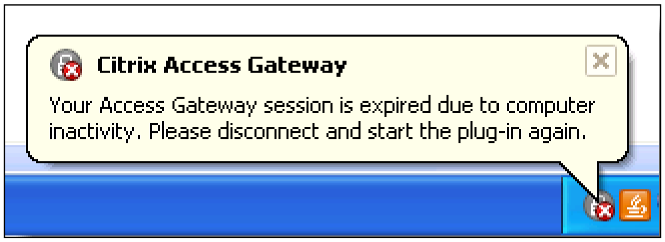


Connection Details:

Property	Value
DNS Servers	172.18.0.2
Split DNS	Disabled
WINS Server	
Private IP Addr...	172.16.100.1
Close connectio...	Enabled
Ports in use:	
	10000 (udp)
	10010 (tcp/udp)
	10020 (udp)

As administrators of CAG, we can control the length of user sessions and implement inactivity timeouts. In this way, we are governing the way in which the gateway is used and the number of users we can support. Therefore, ensuring that idle sessions are closed down in adequate time makes good sense and will also free up resources for others. If the user has been busy with other things, or perhaps has fallen asleep at their desk, their connection will time out after 30 minutes, by default. Of course, we can change these settings in the global settings or within the advanced properties of the SmartGroup. In this way, this chapter took us through configuring SmartGroups. When the user finally wakes up and readjusts their eyes, they can focus on the screen. The user will see that the icon for the CAG plug-in has changed due to inactivity, and a message will inform them that they should disconnect and then reconnect to regain access to resources.

In the following screenshot, we can see the inactivity message displayed by the CAG plug-in when they have been disconnected:



Citrix Access Gateway

Your Access Gateway session is expired due to computer inactivity. Please disconnect and start the plug-in again.

Connecting to resources on the private network

Once we have made the connection to the VPN, we are able to access resources that are permitted through the SmartGroup.

> Remember that the permissions to access resources are defined in the SmartGroup and not in the logon point.

To access any resources, we can use methods that we are used to. To access a website on the private network, for example, just using the browser will work fine. If we use a DNS name, the name will try to be resolved locally first. If it can be resolved, but only to an address on the private network, the VPN connection will be used. If the name cannot be resolved locally—the resolution can be made via the DNS on CAG—a VPN connection is made to the resource. All access is managed first by HTTPS (up to the gateway) and then by the native protocol (from the gateway to the resource).

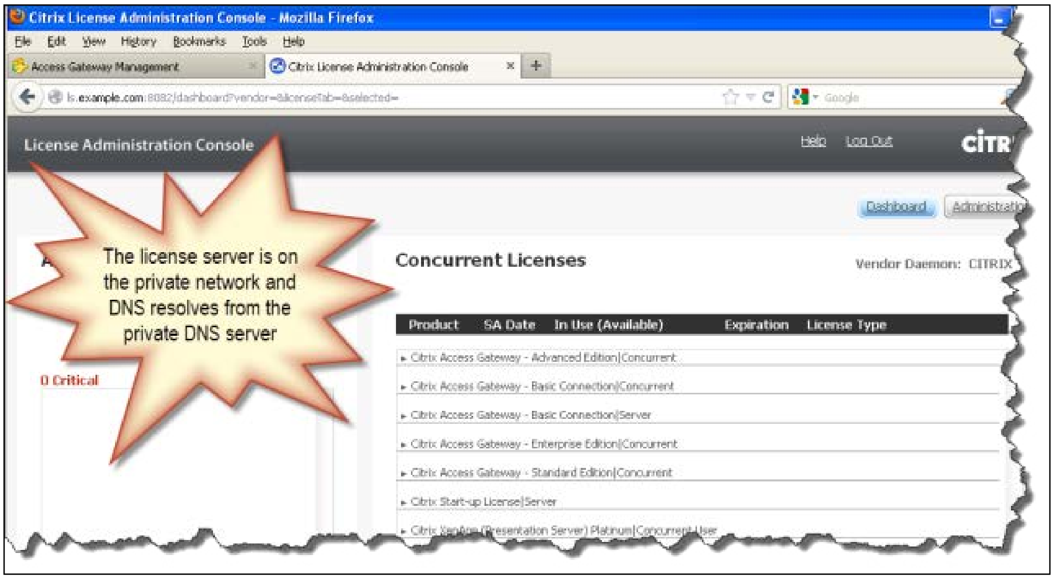
> All access, as with basic logon points, is made using the gateway as a proxy. No direct access is permitted even with the CAG plug-in and the established VPN.

If we needed to access the Citrix License Server from outside of the organization, we would connect to the VPN using the CAG plug-in. Then, using our browser, we can enter the correct URL; in our case, that would be:

```
http://ls.example.com:8082
```

This then will provide us access to the internal resource from wherever we connect in the world.

We are still on the computer with Internet connection, but we are able to access License Server on the internal network. The following screenshot shows the access of an internal website using the CAG plug-in:


Citrix License Administration Console - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Access Gateway Management
Citrix License Administration Console
ls.example.com:8082/dashboard?vendor=&licenseTab=&selected=
Google
License Administration Console
Help Log Out
CiTR
Dashboard Administratio
0 Critical

The license server is on the private network and DNS resolves from the private DNS server

Concurrent Licenses

Vendor Daemon: CITRIX

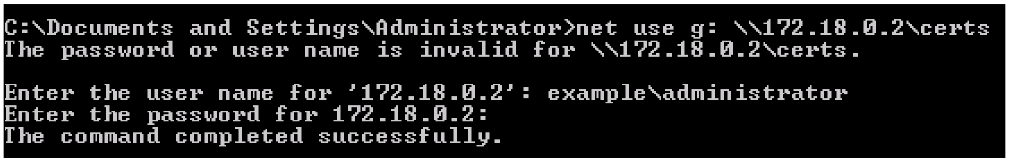
Product	SA Date	In Use (Available)	Expiration	License Type
▸ Citrix Access Gateway - Advanced Edition|Concurrent				
▸ Citrix Access Gateway - Basic Connection|Concurrent				
▸ Citrix Access Gateway - Basic Connection|Server				
▸ Citrix Access Gateway - Enterprise Edition|Concurrent				
▸ Citrix Access Gateway - Standard Edition|Concurrent				
▸ Citrix Start-up License|Server				
▸ Citrix XenApp (Presentation Server) Platinum|Concurrent User				

Another resource that we may need to access would be internal file shares. To connect to these, we could use Windows Explorer and choose **Map Network Drive** from the tools menu. We could also use the command line, and having a batch file on your desktop or start menu may make things a lot quicker. From the command line, we could issue something similar to this:

```
net use g: \\8222dc.example.com\certs /user:example\administrator
```

Ultimately, the way we access the share is not the point, just that we can access the share!

Using the command line and the IP address of an internal resource to map a drive from the remote device is shown in the following screenshot:



```
C:\Documents and Settings\Administrator>net use g: \\172.18.0.2\certs
The password or user name is invalid for \\172.18.0.2\certs.

Enter the user name for '172.18.0.2': example\administrator
Enter the password for 172.18.0.2:
The command completed successfully.
```

Of course, as the use of VPN and CAG grows, you will find more ways in which you can use the product as part of your Secure Remote Access toolset, but this gives you some ideas of how you can implement and start using SmartAccess logon points on your gateway server. I think we are ready to take a step back, admire our work, and accept another pat on the back for a job well done!

Summary

It has taken a long time in coming; however, in the previous section we have finally been able to use the remote access framework that we have been piecing together over the last few chapters. We have seen how the Endpoint Analysis Plug-in is used to assess the device prior to authentication, and then, upon success, pass us back to the CAG plug-in to prompt us for our credentials.

It does not take long from our being connected to be able to use the resources seamlessly from our remote device. The access methods that we use do not change from the local networks to remote networks. Resources can be accessed in the same manner from either network. We are provided access to the private DNS as a matter of course to ease this mechanism.

In the next chapter, we will start to investigate the logs on the server and how we can monitor CAG performance. The gateway can also be configured to monitor itself, to a degree, providing a high-availability solution to fail over to a second, or auxiliary, CAG if problems are detected for the master device. This, I am sure, is something that you will want to take a look at.

13
Monitoring the Citrix Access Gateway

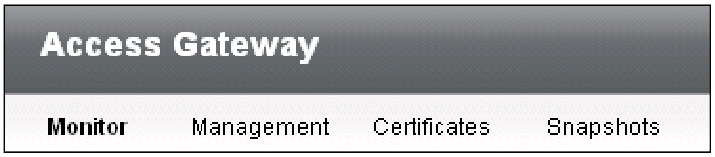
As we near the end of our journey with the CAG VPX, we need to ensure that we can understand the logs and help diagnose and prevent issues from becoming service outages. In addition to this proactive monitoring, as attentive administrators, we can provide levels of faulty tolerance by implementing appliance failover, utilizing an additional CAG. Appliance failover will allow for a virtual CAG to exist within a cluster of a maximum of three gateways. The virtual CAG is active on a single running device, but it can automatically failover to a partner in the event of a failure of the running device.

- Accessing and interpreting logfiles
- Logfile settings and remote log transfer
- Creating configuration snapshots and updating firmware
- Implementing appliance failover

Accessing and interpreting logfiles

For the vast majority of this book, we have focused on managing CAG and, as such, our time has been spent mainly on the **Management** tab in the web console. Now, just for a change, we will spend a little time on the **Monitor** tab to find out what goes on there along with the **Snapshot** tab, which we have not yet visited. Would you keep your excitement in check?

Logs can be viewed from the **Monitor** tab of the web management console, as shown in the following screenshot:



Now of course, we do know that we should check the logfile; this does not change, no matter what OS we are looking at. We also know that sometimes the logs will be useful and at other times not. However, we should always consider the logs, as a first port of call is diagnosing issues with the client and server. We then have real information that we can be working with, and not just perceived performance or errors that may be misinterpreted.

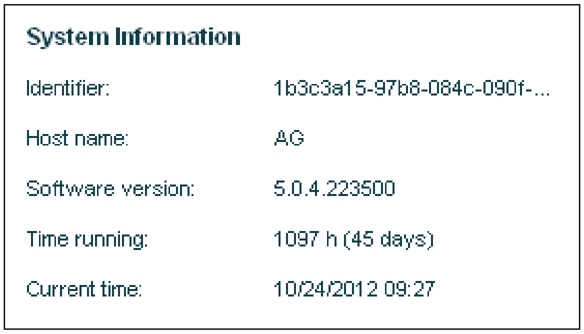
Before we delve straight into the logs, let's make sure we understand from the outset all of the information that is displayed on the **Monitor** tab.

System Information

One of the first items that we can see from the **Monitor** tab is the **System Information** wizard. From here we can verify the version of the CAG software and other information that may be useful, some examples of which are as follows:

- **Identifier**: This is the CAG unique identifier.
- **Hostname**: If this has not been changed, then it will be CAG. The hostname can be set in the **Networking** section of the **Management** tab.
- **Software version**: The version of the CAG software is displayed here.
- **Time running**: The CAG runs on a Linux OS; reboots are not usually required as we can only run software that ships with CAG, and that is, as you would expect, reliable. The time running though, does give you some idea if the machine perhaps has been recently turned off and access will have been affected but with the lack of availability.
- **Current time**: This does, as it says, show the date and time and can be used as an indication that you have set the correct time zone for the server and synchronization with NTP. This information can be set on the **Management** tab.

Following is the screenshot of the **System Information** box:



System Information

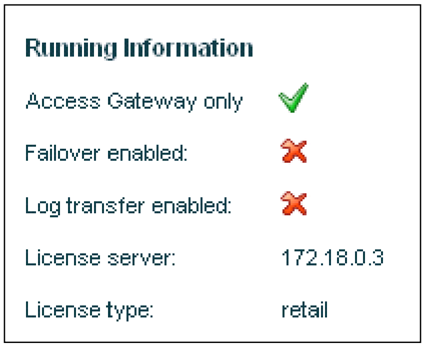
Identifier:	1b3c3a15-97b8-084c-090f-...
Host name:	AG
Software version:	5.0.4.223500
Time running:	1097 h (45 days)
Current time:	10/24/2012 09:27

Running Information

Directly below the **System Information** box, we can view the **Running Information** box, which can then detail how the server has been configured. It is really this information that we will be looking at in more detail later in this chapter, such as setting up our log transfer and appliance failover. Following are the options that appear on the **Running Information** box:

- **Access Gateway only**: We are using CAG in the **Standalone** mode, which allows for all that we have looked at in this book. It is possible if we are using the gateway specifically for access to XenApp or XenDesktop so that we could use it in conjunction with the Access Controller. CAG and Access Controller combined can then be used in tandem with Citrix Group Policy filters to better control the policies that are applied to user connections based on conditions read from the Access Controller.
- **Failover enabled**: We will set this up in this chapter; if this is enabled, then we have two CAGs that act together to ensure that at least one CAG is enabled at all times to increase the availability of the solution.
- **Log transfer enabled**: With this set, we will be able to archive logs on a remote server either using SCP or FTP. Again, we shall set this up in this chapter.
- **License server**: In License Server that we are using, either the name or the IP address will be shown, depending on how we entered the information in the first place.
- **License type**: The license type can be retail or express. Express denotes the free version that is renewed each year; retail denotes that the purchased version of the platform license should be sought out on the configured License Server.

The **Running information** wizard as viewed from the **Monitor** tab is displayed in the following screenshot:



Running Information

Access Gateway only ✓

Failover enabled: ✗

Log transfer enabled: ✗

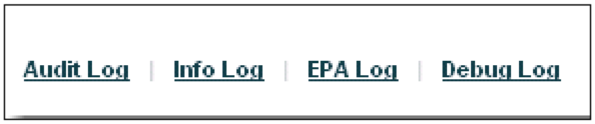
License server: 172.18.0.3

License type: retail

At the very bottom of this first column, we can access hyperlinks to view the logs. There are four logs that we can view on CAG:

- **Audit Log**: This log shows user-related activity; if we have enabled logging within a logon point, we can view the access from this log
- **Info Log**: This log shows system-related activity; it has more to do with the underlying operating system of CAG, such as network issues, but we are also able to see log transfer event here
- **EPA Log**: This log shows device profile activity for endpoint analysis
- **Debug Log**: This log shows more detailed technical information relating CAG activity

The following screenshot shows the logfile hyperlinks that are at the base of the **Monitor** tab:

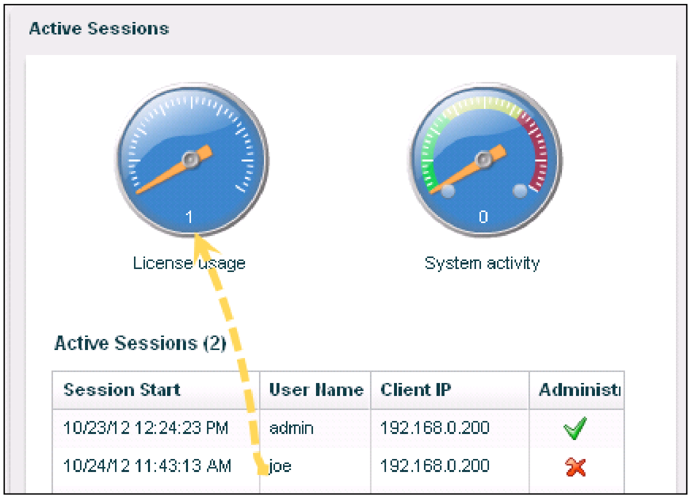


Audit Log | Info Log | EPA Log | Debug Log

Active Sessions

I am sure you can work out what is displayed on the **Active Sessions** box at the center of the **Monitor** tab. The two dials show system activity (CPU) and license usage. In the case of the following screenshot, we can see a single license in use; this will be a universal license issued to the user **joe**, who is currently connected to a SmartAccess logon point. Licenses are not used for basic logon points or for the administrator sessions running in the web console.

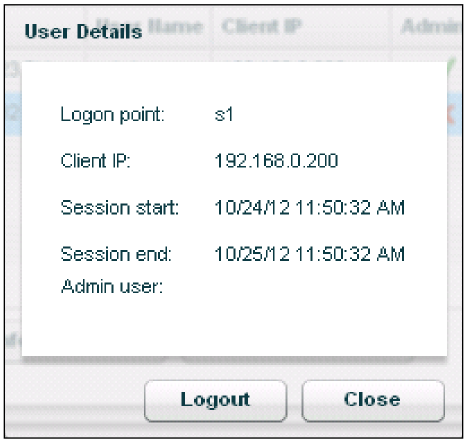
If licensing has not been set up, then CAG will still be in evaluation mode, and the license dial will show the number of hours that are left from the 48-hour evaluation period (96 hours in CAG Version 5.04). Following is the screenshot of the **Active Sessions** dialog:


Active Sessions

Active Sessions (2)

Session Start	User Name	Client IP	Administ
10/23/12 12:24:23 PM	admin	192.168.0.200	✓
10/24/12 11:43:13 AM	joe	192.168.0.200	✗

If we right-click on the **joe** user as displayed in the **Active Sessions** dialog, we can see the logon point and the client IP address that is in use. This means that even without referring to our logfiles, information is at hand from the dashboard. Right-clicking on the **joe** user will also allow you to disconnect users, should we need to bounce the server, perhaps when we need to perform urgent maintenance. Following is the screenshot of the **User Details** wizard:


User Details

Logon point: s1

Client IP: 192.168.0.200

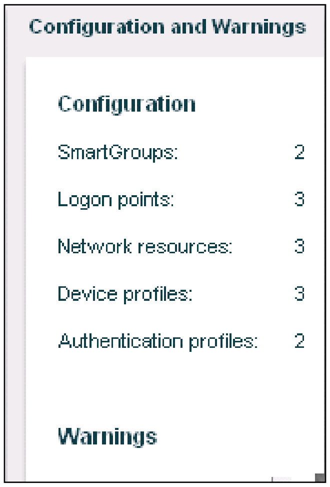
Session start: 10/24/12 11:50:32 AM

Session end: 10/25/12 11:50:32 AM

Admin user:

Configuration and Warnings

On the far right of the **Monitor** tab, we can see how many objects we have created– the amount of logon points, authentication profiles, and so on. As the book has grown, so has the list of configuration objects that we have set up. Warnings will display for licenses that are due to expire or certificate expiry dates when they near. Additionally, warnings will be shown when we have not created the initial components for basic logon points, STAs, and Access Lists for XenApp and XenDesktop. Following is the screenshot of the **Configurations and Warnings** wizard:



Configuration and Warnings

Configuration

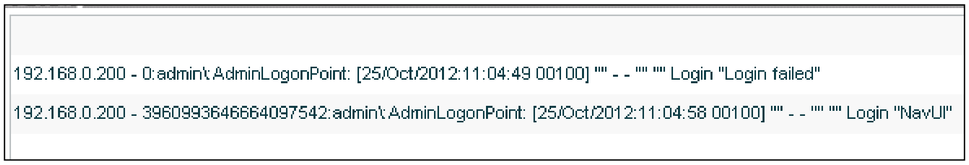
SmartGroups:	2
Logon points:	3
Network resources:	3
Device profiles:	3
Authentication profiles:	2

Warnings

Now that we have reviewed the contents of the **Monitor** page, we can begin to evaluate the contents of each of the logs that are presented and understand their content.

Audit Log

The audit log is able to track access to basic logon points and SmartGroups that have a home page. If **Log Access** is selected, then access information, both success and failure is written to the audit log. By default, access to the AdminLogonPoint is logged, as we can see in the next screenshot. We have a failed attempt followed by a successful logon. If we had multiple failed attempts, then we may assume someone is attempting to gain malicious access to the gateway. It is important to view these logs regularly. Following is the screenshot of the **Audit Log** wizard:

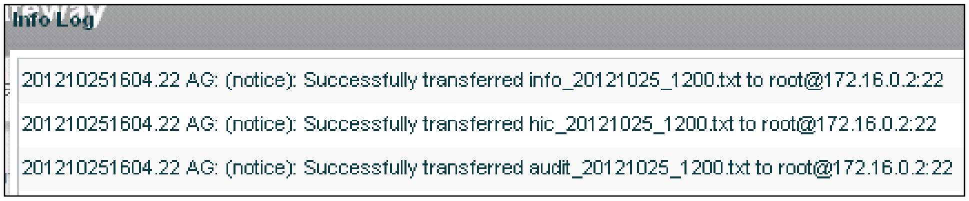


```
192.168.0.200 - 0:admin\AdminLogonPoint: [25/Oct/2012:11:04:49 00100] "" - - "" "" Login "Login failed"
192.168.0.200 - 3960993646664097542:admin\AdminLogonPoint: [25/Oct/2012:11:04:58 00100] "" - - "" "" Login "NavUI"
```

Info Log

These logs can contain system information relating to the underlying OS of CAG. If an IP address cannot be bound to an interface because of an address conflict, then errors will be shown here. If we do set up to transfer logs to a remote machine, those transfer events will be recorded in the info log.

Following is the screenshot of log transfers shown in the **Info Log** wizard:



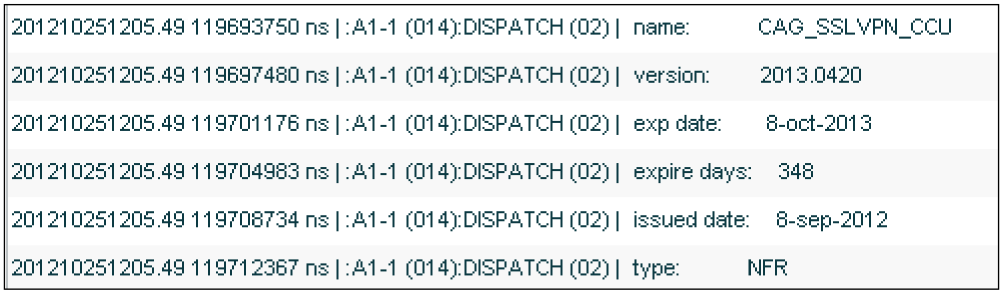
```
201210251604.22 AG: (notice): Successfully transferred info_20121025_1200.txt to root@172.16.0.2:22
201210251604.22 AG: (notice): Successfully transferred hic_20121025_1200.txt to root@172.16.0.2:22
201210251604.22 AG: (notice): Successfully transferred audit_20121025_1200.txt to root@172.16.0.2:22
```

EPA Log

Endpoint analysis of a device from configured device profiles will be shown in these logs; perhaps this indicates if we have an excess of devices not meeting a required level of health to be able to access the network.

Debug Log

In many respects, this is not quite as complex as the name may suggest. We can view information relating to licenses and license utilization that can help diagnose issues where users cannot connect. Additionally, from these logs we are able to view more complex details about the underlying processes that run with CAG, such as memory cleanup. From the following screenshot, we can see that the license was issued by Citrix on September 8, 2012 as a **Not for Resale** (**NFR**) license, and expires in 348 days:



```
201210251205.49 119693750 ns | :A1-1 (014):DISPATCH (02) |  name:         CAG_SSLVPN_CCU
201210251205.49 119697480 ns | :A1-1 (014):DISPATCH (02) |  version:      2013.0420
201210251205.49 119701176 ns | :A1-1 (014):DISPATCH (02) |  exp date:     8-oct-2013
201210251205.49 119704983 ns | :A1-1 (014):DISPATCH (02) |  expire days:  348
201210251205.49 119708734 ns | :A1-1 (014):DISPATCH (02) |  issued date:  8-sep-2012
201210251205.49 119712367 ns | :A1-1 (014):DISPATCH (02) |  type:         NFR
```

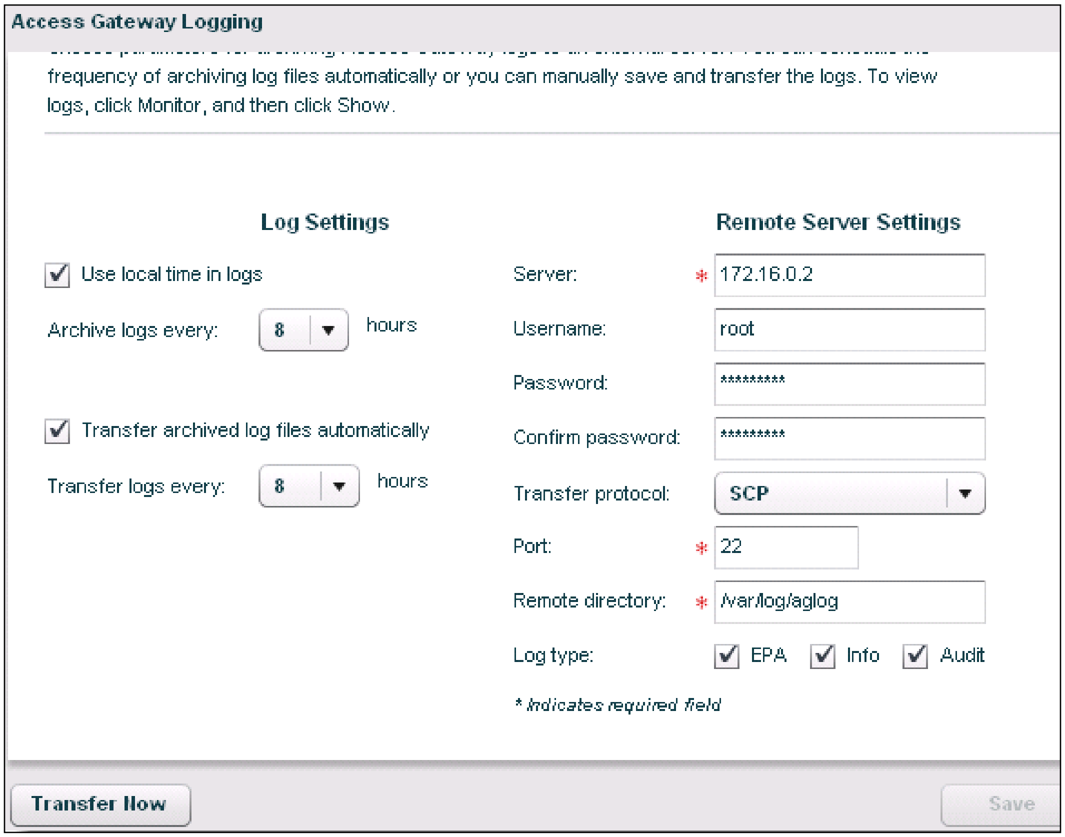
Reading from the debug log, we can notice in the previous screenshot that license expiry is included, as well as other license properties.

Logfile settings and log transfer

We have spent a little time on the **Monitor** tab; we will now return to our day job in the **Management** tab. I hope you enjoyed your brief excursion.

From the **Management** tab, we should be able to navigate to the **System Administration** and **Logging** panes.

The following screenshot illustrates the settings that are available for logging:



Access Gateway Logging

frequency of archiving log files automatically or you can manually save and transfer the logs. To view logs, click Monitor, and then click Show.

Log Settings

☑ Use local time in logs

Archive logs every: 8 ▼ hours

☑ Transfer archived log files automatically

Transfer logs every: 8 ▼ hours

Remote Server Settings

Server: * 172.16.0.2

Username: root

Password: *********

Confirm password: *********

Transfer protocol: SCP ▼

Port: * 22

Remote directory: * /var/log/aglog

Log type: ☑ EPA ☑ Info ☑ Audit

* Indicates required field

In the simplest form of the configuration, we would purely use the **Use local time in logs** and **Archive logs every** options. There is no requirement to transfer the logfiles.

The default will be to archive logs every 4 hours, but when servers are less busy, we can choose to archive every 8 hours. The available options are **4** and **8** hours. We can view only the current file, not the archived files. So choosing to transfer the files allows for retention of all logfiles as long as we need. If we do choose to transfer the files, we can transfer every 4, 8, or 16 hours to the remote server.

In many cases the remote server will be Linux; the transfer protocols being:

- **Secure Copy Program** (**SCP**) running on port 22
- **File Transfer Protocol** (**FTP**) running on port 21

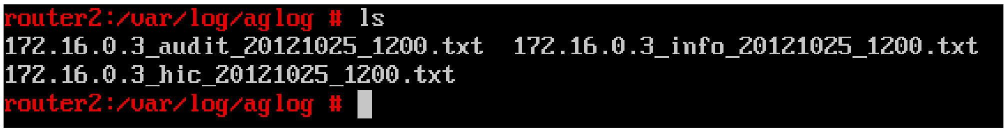
And, as you can see from the previous screenshot, you will be prompted to authenticate to the remote server, and select a directory to store the transferred logs. You can see that the gateway is configured to send the logs to the remote server using the root account, which may not be the best option, and store the logs in:

```
/var/log/aglog
```

Once the logs have been transferred, then it's our job to maintain them on the remote server; we may use logs to rotate within Linux to ensure we do not occupy too much disk resource on the Linux host. Your log-rotating plan would be based upon how often we read the logs and how many old copies we need to maintain. Keeping old logs may be required for compliance with certain agencies or certifications.

We can view the transferred log with any text viewer, and of course, they show in the directory that they were transferred to:

Directory listing after a single transfer on the remote host is shown in the following screenshot:



```
router2:/var/log/aglog # ls
172.16.0.3_audit_20121025_1200.txt  172.16.0.3_info_20121025_1200.txt
172.16.0.3_hic_20121025_1200.txt
router2:/var/log/aglog #
```

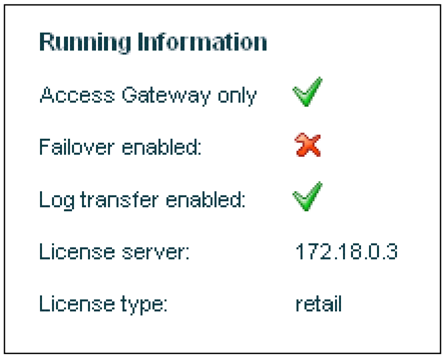
The logfile names include the following:

- IP address of CAG –`172.16.0.3`
- The log type – audit, info, and hic (EPA). The hic log displays information about the endpoint analysis results from clients
- Date as 2012/10/25 (YYYY/MM/DD)
- Time logfile started at 12 o'clock midday in this case. If we are rotating every 4 hours, then the times of the files will be as follows:
    - 0000
    - 0400
    - 0800
    - 1200

- After rotating the files every 8 hours, the files times will be:
  - 0000
  - 0800
  - 1600
  - 0000

Once we have configured with the log transfer and we are happy that it is working, we can view the **Monitor** tab under the running information that log transfer is enabled. It then becomes an easy task to note when this is enabled or disabled with the big red cross or big green tick.

Log transfer is now enabled, as shown in the following screenshot:



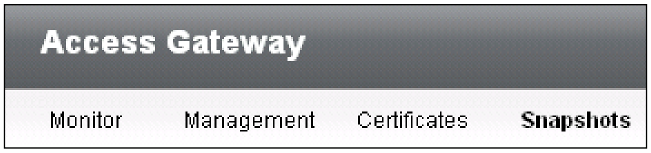
Running Information

Access Gateway only	✓
Failover enabled:	✗
Log transfer enabled:	✓
License server:	172.18.0.3
License type:	retail

Creating configuration snapshots and importing firmware updates

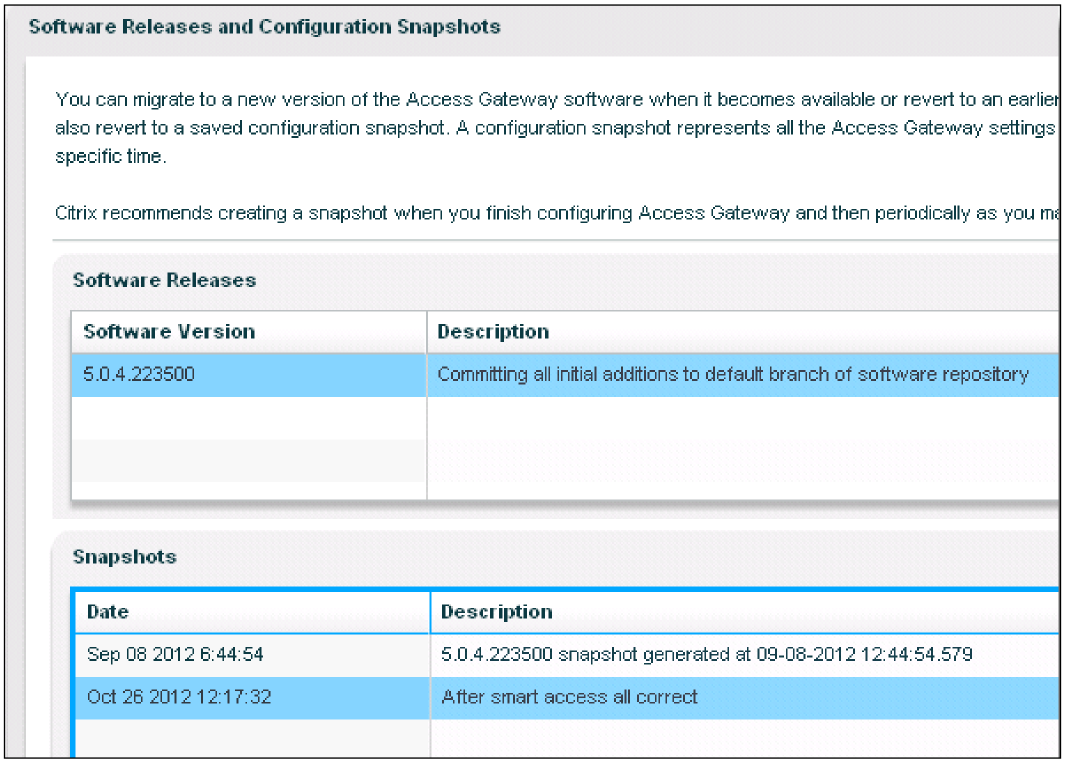
So far we have not spent much time, if any, on the **Snapshots** tab of the management console.

The **Snapshots** tab allows for import of new firmware and configuration snapshots. Refer to the following screenshot:



From here we can create configuration snapshots, saving the configuration, so we can roll back to a working configuration at any stage. We can also export snapshots, so we can import the configuration in another CAG. When you think about it, the configuration needs of one CAG will be similar to other CAGs within your organization. Being able to configure the settings on one gateway and import them to other devices saves the administration time hugely. Of course, there will be some adjustments needed to tune each CAG, such as the hostname, IP address timeouts, and so on. However, nowhere near the same work that is needed in creating the configuration from scratch each time. The suggestion would be to at least create your first snapshot, once you have configured CAG with its initial settings. As changes are needed, you can always create snapshots before any change and roll back to previous versions as required.

From the following screenshot, we can view snapshots and the CAG software version:



Software Releases and Configuration Snapshots

You can migrate to a new version of the Access Gateway software when it becomes available or revert to an earlier also revert to a saved configuration snapshot. A configuration snapshot represents all the Access Gateway settings specific time.

Citrix recommends creating a snapshot when you finish configuring Access Gateway and then periodically as you ma

Software Releases

Software Version	Description
5.0.4.223500	Committing all initial additions to default branch of software repository

Snapshots

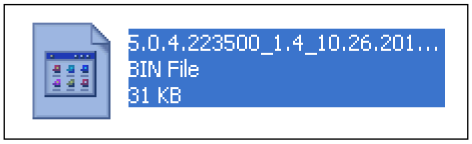
Date	Description
Sep 08 2012 6:44:54	5.0.4.223500 snapshot generated at 09-08-2012 12:44:54.579
Oct 26 2012 12:17:32	After smart access all correct

The upper window shows the software version that we are running. As new versions become available, it is possible to import the latest version after downloading it from Citrix. There is also an **Initialize** button, which will revert CAG to factory settings, essentially a factory reset of the device.

This would be the same as applying the initial snapshot that is created at the time of the virtual machine import. In the previous screenshot, the snapshot taken on September 8 represents the factory settings of CAG. Having now successfully tested SmartAccess, we have decided it pertinently to take a new snapshot representing the release that we, as administrators, are happy with representing our current environment.

We can also export the snapshot; it will be saved to the PC that we are using to access the web console as a `.BIN` file. This can then make part of our disaster recovery plan; in case we need to rebuild CAG from scratch, we have the current configuration, or we can build other CAGs with similar settings. The exported file includes the CAG version and date and time of the snapshot. The file should not be huge inside; it should just represent configuration data; a typical size would be 30 to 50 KB.

Following is the exported configuration screenshot in the Windows client filesystem:



5.0.4.223500_1.4_10.26.201...
BIN File
31 KB

Implementing appliance failover

Using the VPX edition of CAG, by its very nature, we have a level of high availability provided if we implement it at the hypervisor level; using the enterprise or platinum licenses of the Citrix XenServer will allow for high availability. If the host running CAG fails, then the virtual appliance will start on another XenServer host. It is possible to use HA or appliance failover with CAG itself, maybe because we are using a hardware NetScaler appliance or maybe just because we want to cater for actual appliance failures as well as hardware failures. Either way it is possible with CAG and will just need another platform licence for each slave device we implement.

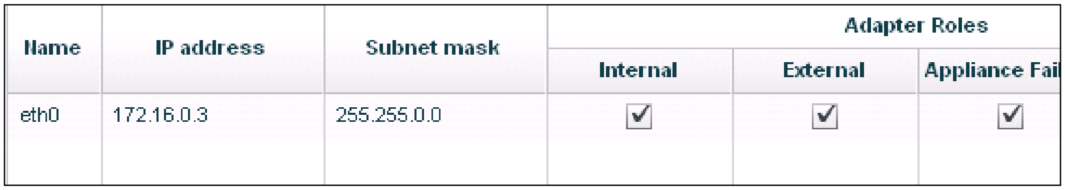
For correct operation, we will also need to ensure that we utilize the two network cards that ship with the VPX gateway; connect both `eth0` and `eth1`. This way we then have an interface for users to connect to on the Internet-facing network interface card and an internal management interface connected to the internal network. The heartbeat to test the availability of the failover master can occur on the internal management interface and can automate the failover from the master to the slave.

Like a virtual server, the master and slave CAG have their own IP address on both the internal and external networks. The IP address for the virtual CAG moves between the master and the slave depending on which CAG hosts the resource currently. The slave can detect the absence of the heartbeat and can then take over hosting of the virtual server until the master operation is resumed.

The heart beat operates on UDP port 694 and, of course, needs to be open between the primary and secondary devices; additionally, TCP port 5432 needs to be open for the secondary devices to be able to access the database and replicate the settings.

Configuring the master device

The first step in configuring failover is to select an interface to use for appliance failover. As mentioned earlier, we would normally expect to be using both interfaces on the gateway, `eth0` and `eth1`. The interface that we use for the internal management traffic can then be selected for the appliance failover role. Using the **Management** tab and selecting **System Administration and Networking**, we can select the interface to use for appliance failover. Following is the screenshot of network adaptor roles:

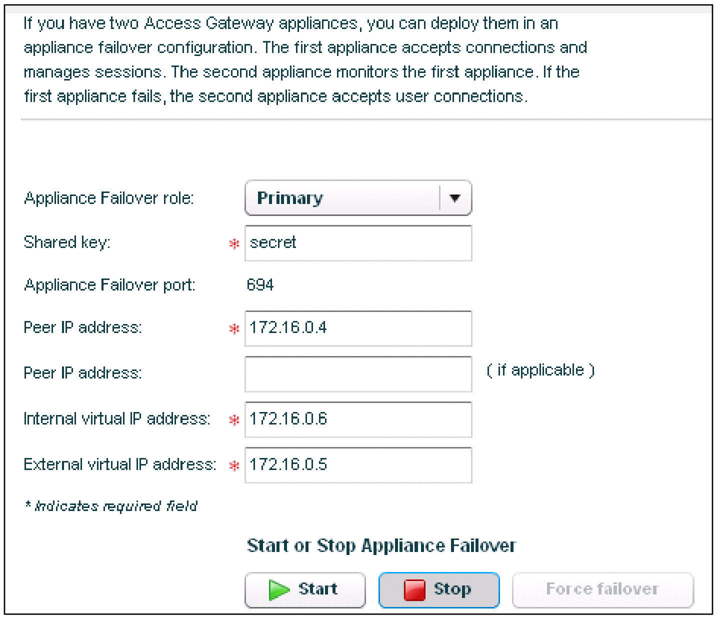


Name	IP address	Subnet mask	Adapter Roles		
			Internal	External	Appliance Fail
eth0	172.16.0.3	255.255.0.0	☑	☑	☑

With the selection made, we can move down to the **Appliance Failover** node. From here we can then set the settings for appliance failover. This includes:

- **Appliance role**: This will be primary on the master device.
- **Shared key**: This refers to the authentication credentials used between the master and slaves.
- **Peer IP address**: Up to two slave devices can be added into the configuration; one slave device would normally be adequate.
- **Internal/external IP address**: Once configured, we create a virtual CAG, the IP address of which is migrated between the master and slaves as required to maintain the running of CAG. It is the external address of the virtual CAG that clients connect to. The external address would normally be an address on the DMZ and the internal address on the internal private network. The address shown here is for demonstration only.

Configuring a failover on the master device in the cluster is shown in the following screenshot:



If you have two Access Gateway appliances, you can deploy them in an appliance failover configuration. The first appliance accepts connections and manages sessions. The second appliance monitors the first appliance. If the first appliance fails, the second appliance accepts user connections.

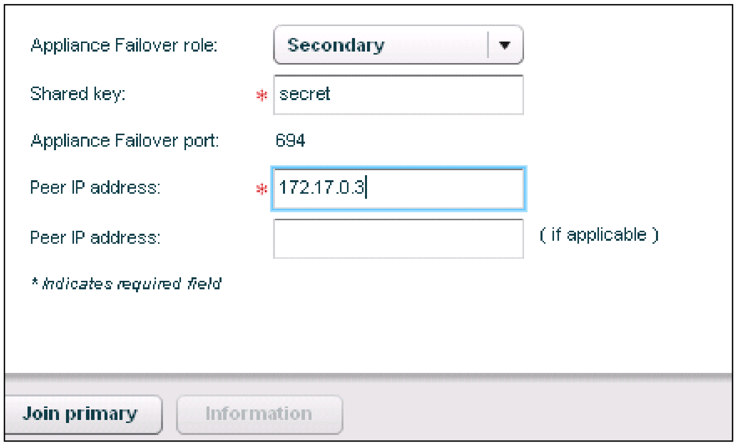
Appliance Failover role:	Primary ▾	
Shared key: *	secret	
Appliance Failover port:	694	
Peer IP address: *	172.16.0.4	
Peer IP address:		(if applicable)
Internal virtual IP address: *	172.16.0.6	
External virtual IP address: *	172.16.0.5	

* indicates required field

Start or Stop Appliance Failover

Configuring the slave device

Configuring the slave or a secondary device is a similar process. Enable the appliance failover role of the internal NIC, and then configure the appropriate settings on the **Appliance Failover** node. The configuration of the slave is shown in the following screenshot:

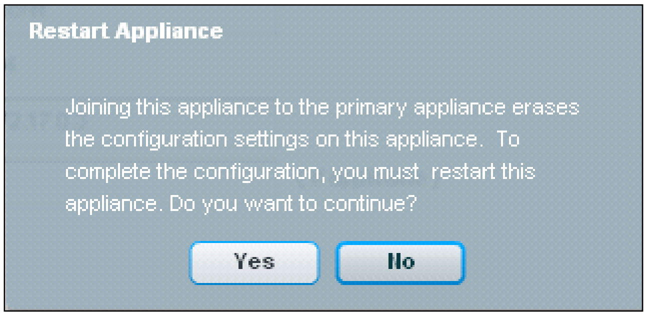


Appliance Failover role:	Secondary ▾	
Shared key: *	secret	
Appliance Failover port:	694	
Peer IP address: *	172.17.0.3	
Peer IP address:		(if applicable)

* indicates required field

Once set up, we can select the **Join Primary** button. We will be warned that we will lose any configuration on the secondary device and that we will need to restart the appliance once we have joined.

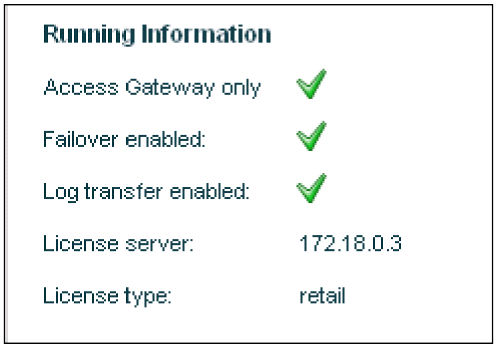
The mode of operation is master/slave. This is not load balancing; the complete configuration of logon points comes from the master device and the slave is only used in a failover event. The secondary device warning is shown in the following screenshot:



Restart Appliance

Joining this appliance to the primary appliance erases the configuration settings on this appliance. To complete the configuration, you must restart this appliance. Do you want to continue?

Both gateways, master and slave, need to reboot. We should ensure that the master device reboots first, so as not to cause a failover. We can confirm the running settings on the **Monitor** tab; now we will have the happy green tick indication that we have set up appliance failover. The setting up of appliance failover is shown in the following screenshot:



Running Information

Access Gateway only	✓
Failover enabled:	✓
Log transfer enabled:	✓
License server:	172.18.0.3
License type:	retail

If we need to test failover, rather than bringing the primary or master device down, we can force a failover. This can both test the failover action and provide us with a safe way of bringing down the master. After performing appliance failover, check it has worked, and then bring down the master for maintenance or whatever the need is. If we have used the **Force Failover** button from **Management | System Information | Appliance Failover**, then we can view the progress. Once complete, the running CAG is now on the secondary or slave device. The force failover is shown in the following screenshot:

Please Wait

Failover in progress...

Initializing...

Summary

Being able to manage CAG must include being able to effectively monitor and maintain access and performance; these areas of management are just as important as being able to create the logon points for user access. Being able to keep them available is down to effective monitoring and high availability services. To this end, we have now investigated the monitoring tools and logs that the web console makes available and transferred the logs to remote severs to ensure that historical logs are available. We have also seen how we can improve the availability of the gateway with appliance failover.

In the next chapter, we will finish the administration of the VPX edition of CAG by looking at the command line tools available from the console of the server or via SSH.

14
Command Line Management of the Citrix Access Gateway

In this final chapter we take a look at how we can manage CAG from the command line, both locally on the server or remotely using SSH. In this chapter we'll see:

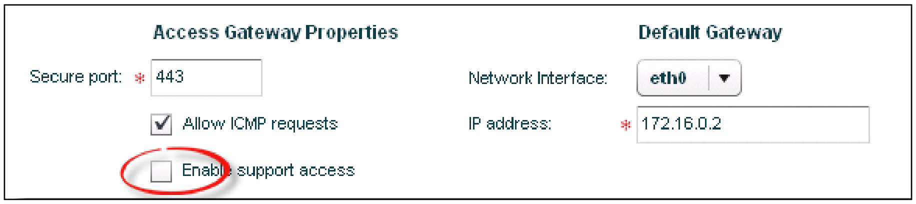
- Enabling SSH access to the command line
- Managing CAG from the command line

Enabling SSH access to the command line

In the early stages of this book, we visited the command line in order to run the Express Setup as part of our initial configuration of CAG. This enabled us to set an IP address suitable for the network we are attached to (CAG ships with the IP address of `10.20.30.40`). We of course can always access the server's command line from the hypervisor tools such as XenCenter; however, direct access to the server's command line via SSH is quicker and more desirable.

To enable SSH (it is a little obscure), use the **Enable support access** option on the **Management** tab and **Networking** section. This is disabled by default and needs to be ticked to allow SSH access.

To enable SSH, select the **Enable support access** checkbox as shown in the following screenshot:



Access Gateway Properties

Secure port: * 443

☑ Allow ICMP requests

□ Enable support access

Default Gateway

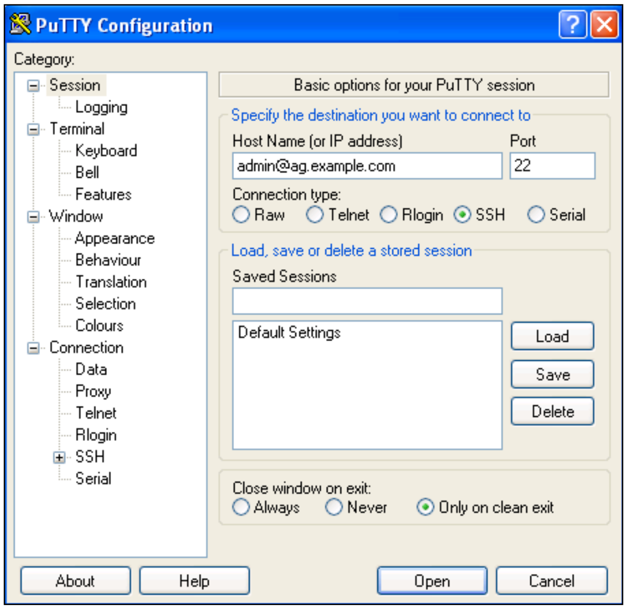
Network Interface: eth0

IP address: * 172.16.0.2

Once we have enabled SSH through this option, we can use tools such as PuTTY, a freely downloadable software to connect to the command line of our server. We will still connect as the user `admin` with the password that we have set. This is the same username and password that we use to access the AdminLogonPoint of the web-based console.

> You can download PuTTY from`http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html`.

In our case, the connection will be made to `admin@ag.example.com` to ensure that the username is passed with the connection to the server. We then just need to confirm the username and type in the password once we have connected, as shown in the following screenshot:



Host Name (or IP address): admin@ag.example.com

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

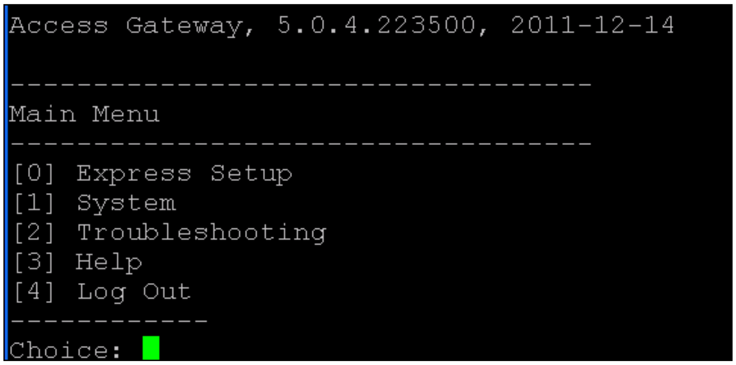
Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Establishing a connection to CAG using SSH is in no way different to connecting to the console on the actual virtual machine; in that we only have access to the menu that is provided and not to the shell itself. Hence, the OS itself is more secure as we only have access to the menu. Using SSH just makes connection to the console easier and works direct from your workstation.

Managing the Citrix Access Gateway from the command line

Once we gain console access, either via SSH or using the console on XenCenter, we are limited by the menu as to what changes we can effect. We first saw the menu with the initial setup of CAG when we set the IP address. Following is the screenshot of the command-line menu:



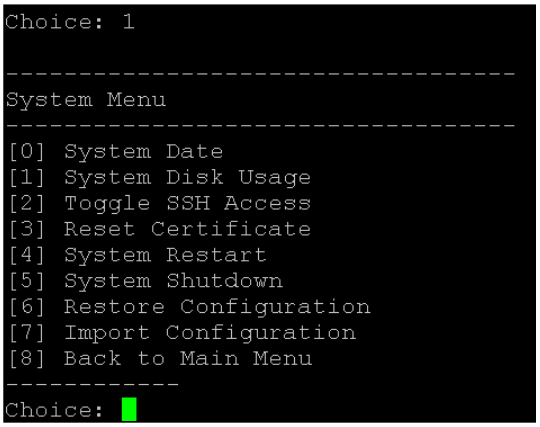
```
Access Gateway, 5.0.4.223500, 2011-12-14

-----------------------------------
Main Menu
-----------------------------------
[0] Express Setup
[1] System
[2] Troubleshooting
[3] Help
[4] Log Out
------------
Choice:
```

Express Setup

This is the menu item that we visited before, during the initial configuration. We do not need to revisit this once we have connectivity. Our networking settings can be managed via the web console. So we will leave that from this section.

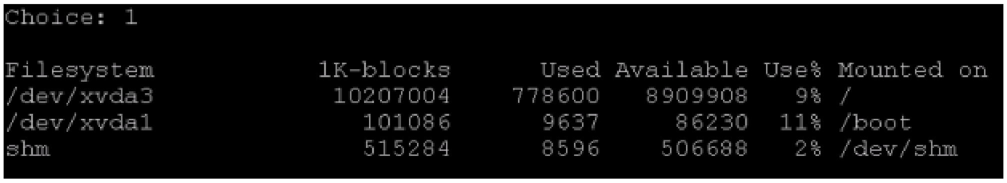
System

Choosing `[1]` from the `Main Menu` mode will take us to the **System** submenu. From here we can see the date, disk usage, reboot the gateway, and restore settings. The following screenshot shows the system menu:



```
Choice: 1

-----------------------------------
System Menu
-----------------------------------
[0] System Date
[1] System Disk Usage
[2] Toggle SSH Access
[3] Reset Certificate
[4] System Restart
[5] System Shutdown
[6] Restore Configuration
[7] Import Configuration
[8] Back to Main Menu
------------
Choice:
```

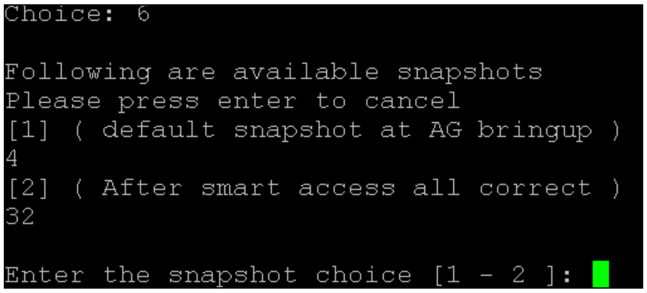
- Selecting option `[0]`just displays the system date issuing the command date on the console.
- Selecting option `[1]` shows the disk space in use by using the command `df`. The usage is shown in `1K-blocks`, so it isn't the easiest to read. The percentage of disk use is useful and we should look only for the root partition; in the case of XenServer-based appliances, this will be `/dev/xvda3`. In the following screenshot, we can see that in selection option `[1]`, we are shown the disk utilization:



```
Choice: 1

Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/xvda3            10207004    778600   8909908   9% /
/dev/xvda1              101086      9637     86230  11% /boot
shm                     515284      8596    506688   2% /dev/shm
```

- Selecting option `[2]`allows us to turn SSH on and off.
- Selecting option `[3]`resets the SSL certificates to the factory-supplied certificates.
- Selecting option `[4]` and `[5]`are obvious stop and restart options, respectively.

- Selecting option `[6]` restores configuration, allows you to revert to a snapshot that has been created. In the monitoring chapter of the book, we saw how it was possible to save the configuration as a snapshot. Here, we can revert to them. The initial CAG start is always available if we want to clear the complete configuration of the device. From option `[6]`, we can see that we are presented with a choice of previously created snapshots or configurations to revert to:

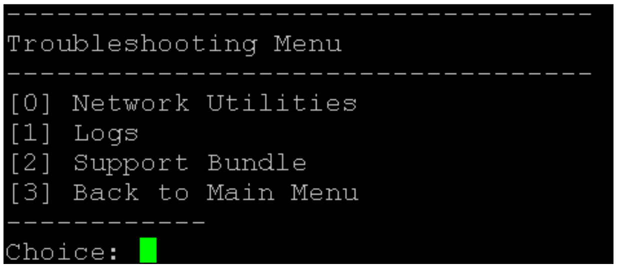


```
Choice: 6

Following are available snapshots
Please press enter to cancel
[1] ( default snapshot at AG bringup )
4
[2] ( After smart access all correct )
32

Enter the snapshot choice [1 - 2 ]:
```

- Selecting option `[7]` allows us to import a configuration from an FTP or SCP server.
- Selecting option `[8]` allows us to return to the main menu.

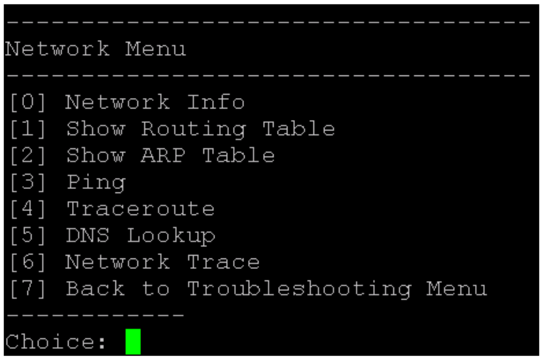
Troubleshooting

The `Troubleshooting Menu` mode allows you access to some simple tools such as ping and access to the logs from the console of CAG. Following is the screenshot of the `Troubleshooting Menu` mode:



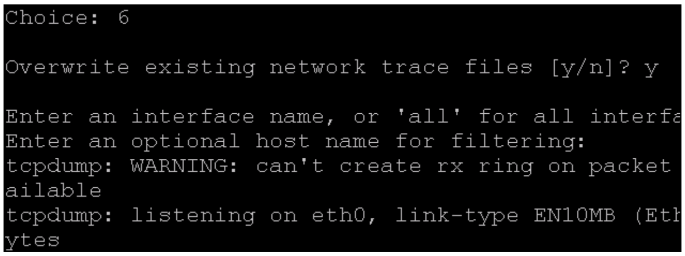
```
-----------------------------------
Troubleshooting Menu
-----------------------------------
[0] Network Utilities
[1] Logs
[2] Support Bundle
[3] Back to Main Menu
------------
Choice:
```

Selecting option `[0]`, the `Networking Utilities` option, will show another sub-menu, as shown in the following screenshot:



```
-----------------------------------
Network Menu
-----------------------------------
[0] Network Info
[1] Show Routing Table
[2] Show ARP Table
[3] Ping
[4] Traceroute
[5] DNS Lookup
[6] Network Trace
[7] Back to Troubleshooting Menu
------------
Choice: 
```

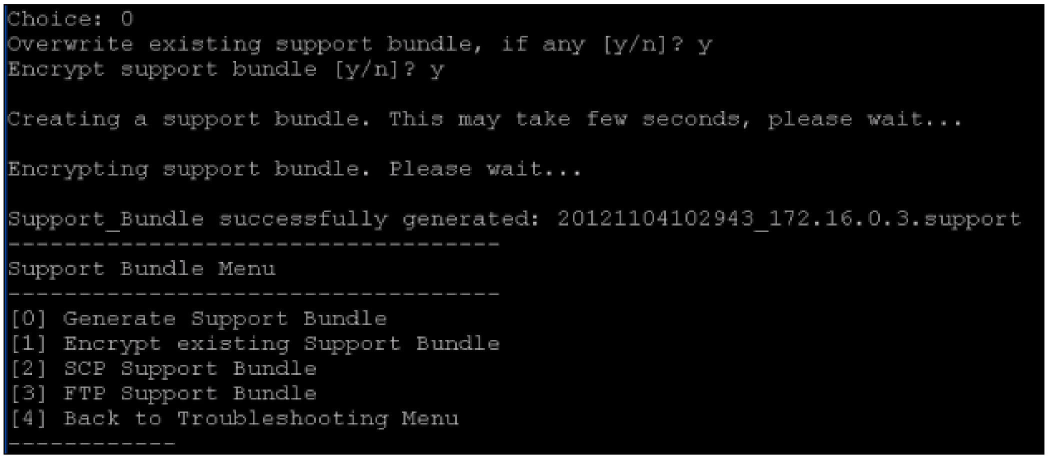
The option from the `Networking Menu` mode, as you can see, allows you access to your standard tools for investigating communication issues. `Networking Info` shows the IP addresses, and then moving down to the route table, arp cache, ping, trace route, and nslookup. The last option, `[6]`, `Network Trace`, is actually using `tcpdump`, the Linux command line packet analyzer to run packet captures from the device and is illustrated in the following screenshot:



```
Choice: 6

Overwrite existing network trace files [y/n]? y

Enter an interface name, or 'all' for all interfa
Enter an optional host name for filtering:
tcpdump: WARNING: can't create rx ring on packet
ailable
tcpdump: listening on eth0, link-type EN10MB (Eth
ytes
```

- Selecting option `[1]` from the `Troubleshooting Menu` mode allows us to view and manage the logs from the command line, although not log transfer. So, I still feel the GUI tools become the answer to this and transfer the logs to another machine for viewing.

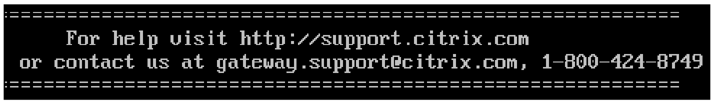
- Selecting option `[2]` allows us to create a support bundle that allows us to transfer information about our gateway to Citrix for advanced diagnostics. From the `Support Bundle Menu` mode, we can choose to create a new support bundle that then can be copied to Citrix Technical Support. The creation of support bundle is shown in the following screenshot:



```
Choice: 0
Overwrite existing support bundle, if any [y/n]? y
Encrypt support bundle [y/n]? y

Creating a support bundle. This may take few seconds, please wait...

Encrypting support bundle. Please wait...

Support_Bundle successfully generated: 20121104102943_172.16.0.3.support
-----------------------------------
Support Bundle Menu
-----------------------------------
[0] Generate Support Bundle
[1] Encrypt existing Support Bundle
[2] SCP Support Bundle
[3] FTP Support Bundle
[4] Back to Troubleshooting Menu
------------
```

Help

Selecting option `[3]` from the `Main Menu` mode does not do a whole lot, giving a web URL, e-mail, and a US number to call for support. As shown in the following screenshot, option `[3]` does not show too much:



```
==========================================================
    For help visit http://support.citrix.com
 or contact us at gateway.support@citrix.com, 1-800-424-8749
==========================================================
```

Summary

We will close the book now having taken you through the complete management lifecycle of the CAG VPX edition. In this final section, we enabled SSH access to the server console.This enabled us to investigate the management options that are available via the command line interface of CAG. These commands can be accessed remotely using SSH or directly on the console itself.

This now concludes the book and we have completed the journey, where we began by setting up licensing. We then discussed about the MYCITRIX website, importing the VPX into our virtualization environment. Soon we learned the two types of logon point we can create:

- Basic, which uses the platform license only and provides ICA-Proxy only to XenApp and XenDesktop
- SmartAccess, which uses the universal licenses and enables full VPN access to your network, along with all the elements such as endpoint analysis that go hand in hand with SmartAccess

With these in place, we had to then consider how we maintained our logfiles and high availability, closing with this section on the command-line access. I hope you have found the book useful and you return to Packt Publishing soon for your next book.

Index

Symbols

.NET 3.5.x 26
.XVA extension 39

A

accelerated orchestration
- about 152
- Adaptive Compression 152
- Adaptive Protocol Acceleration 152
- adaptive TCP flow control 152
- Traffic Prioritization and Quality of Service 152

access
- auditing, to CAG 78, 79

Access Gateway 5 (NetScaler 2010) 21
Access Gateway 5.x 15
Access Gateway 9.2 Enterprise Edition
- about 14
- benefits 14

Access Gateway 9.3 Enterprise Edition 14
Access Gateway 10
- about 13
- organizational benefits 13

Access Gateway basic logon point
- configuring 65, 66

Access Gateway Milestones 12
Access Gateway plug-in
- distributing, with Merchandising Server 112
- integrating, with Citrix Receiver 111

Access Gateway Plug-in. *See* **CAG plug-in**
Access Gateway setup
- inititating, from command line 40-43

Active Directory sAMAccountName
- used, for authentication 92

Active Directory userPrincipalName
- used, for authentication 93

Active Sessions, Monitor tab 190
Adaptive Compression 152
Adaptive Protocol Acceleration 152
Adaptive TCP flow control 152
address pools
- creating 119-122
- License Server, accessing 125
- resource, verifying 123
- VPN connection, establishing 122
- welcome page, accessing on web server 123, 124

address pools option, System Administration 128
admin password
- setting 45

Adobe Flash 44
advanced properties, group settings
- about 172
- authenticate after network interruption 172
- authenticate after system resume 172
- close existing connections 172
- enable single sign-on to Windows 173
- enable split DNS 173
- enable split tunneling 172
- override session time-out 173
- override user inactivity time-out 173
- override user network time-out 173

appliance failover
- appliance role 199
- implementing 198, 199
- internal/external IP address 199
- master device, configuring 199
- Peer IP address 199

settings 199
shared key 199
slave device, configuring 200, 201
appliance failover option, System Administration 127
Audit Log wizard, Monitor tab 192
authentication 20
with Active Directory sAMAccountName 92
with Active Directory userPrincipalName 93
authentication profiles
about 82
LDAP 82
RADIUS 82-86
RSA SecurID 82, 88, 89
authentication profiles, SmartAccess logon points
using 158
authentication, SmartAccess logon points
about 158
authorization, enabling 158
authorization profiles, SmartAccess logon points
about 158
profile properties 159
using 158

B

basic logon point
about 22
extending, for internal web-based resources access 73-78

C

CAG
about 8, 37
access, auditing to 78, 79
address pools, creating 119
as remote access solution 56, 57
Citrix Web Interface site, configuring with 57, 58
device profiles 131
endpoint analysis plug-in, installing 138
features 15
hardware 10
importing, into VMware 39
importing, into XenServer 39, 40
licensing 21, 22, 47, 48
logon point, branding 161
managing, from command line 205
monitoring 52, 54, 187
network resources 143
plug-in, installing 104-106
plug-in, obtaining 105
plug-in properties, configuring 107-110
Remote Access Solutions, addressing 8, 9
security, addressing 8, 9
SmartAccess logon points 155
SSH access, enabling to command line 203-205
SSL certificates, adding 48-51
two-factor authentication, implementing on 100-102
universal licenses, adding 103, 104
used, for resolving remote access 19
versions 12
XenApp Server farms, accessing with 72
CAG logon page
customizing 96-98
CAG management options
express setup 205
help menu 209
system menu 206
troubleshooting menu 207, 208
CAG, monitoring
about 187
appliance failover, implementing 198
configuration snapshots, creating 196, 197
firmware updates, importing 198
logfiles, accessing 187
logfile settings 194
logfiles, interpreting 188
log transfer 194, 196
CAG plug-in
about 151, 177
client plug-in, managing 182, 183
configuring 180-182
connection properties 182
delivering, from SmartAccess logon point 177-179
used, for accessing resources on private network 184, 185

CAG VPX Edition 15, 16
certificate authority (CA) 48
certificate signing request (CSR) 48
CIFS (Common Internet File System) 151
Citrix
  about 8
  virtual appliance, downloading from 38
Citrix Access Gateway. *See* **CAG**
Citrix Access Gateway Express 23, 24
Citrix Access Gateway plug-in. *See* **CAG plug-in**
Citrix Branch Repeater 150
Citrix Branch Repeater plug-in 151
Citrix Endpoint Analysis plug-in 151
Citrix Receiver
  Access Gateway plug-in, integrating with 111
Citrix Secure Gateway (CSG) 8
Citrix Web Interface site
  configuring, with CAG 57, 58
Citrix XenServer
  about 28
  License Server VPX, importing into 28-30
client plug-in
  managing 182
command line
  Access Gateway setup, initiating from 40-43
configuration, Access Gateway basic logon point 65, 66
configuration, Protiva 86
configuration, SafeWord 87, 88
Configurations and Warnings wizard, Monitor tab 192
configuration snapshots
  creating 196-198
connection properties, CAG plug-in
  about 182
  change passwords 183
  connection log 182
  connection status 182
  disconnect 183

D

dashboard
  securing 34
date and time option, System Administration 129
debug log, Monitor tab 193
deliveries
  configuring, with Merchandising Server 114-116
deployment mode option, System Administration 128
device profiles
  about 131
  configuring 132
  creating 132
  effective scan expression, building 137
  file scan 133
  Operating System scan 135
  Ports scan 136
  process scan 133
  registry scan 134
  used, for controlling access to network 141

E

EdgeSight 24
eDOCS 24
effective scan expression, device profiles
  building 137
electronic software distribution (ESD) 112
encrypted MAPI 151
endpoint analysis plug-in
  accessing 178
  download link 138
  installing 138-140
EPA Log, Monitor tab 193
express setup menu 205

F

features, CAG 15
features, platform license 23
file scan type, device profiles 133
File Transfer Protocol(FTP) 195
firmware updates
  importing 196-198

G

Gemalto Protiva. *See* **Provita**
General Information, SmartGroups 164

General Properties, SmartAccess logon points 157
Group Criteria section, SmartGroups
- about 166
- device profiles 166
- group membership 167-169
- logon points 166

Group Settings section, SmartGroups
- about 169
- address pools 171
- advanced properties 172
- network resources 169, 170

H

hardware, CAG
- NetScaler Model 2010 Appliance 10
- NetScaler Model MPX 5500 Appliance 11

HDX WAN optimization protocol 152
help menu 209
home page, SmartGroups 165
HTTP 151
HTTPS
- about 151
- License Server, securing with 35, 36

I

ICA 9
ICA Proxy
- used, for accessing XenApp 18
- used, for accessing XenDesktop 18

ICMP 149
Info Log wizard, Monitor tab 193
initial configuration
- admin password, setting 45
- completing, from web portal 44
- static route, adding to private network 45-47

installation, License Server 11.10 26, 27
installation, Merchandising Server 112
internal web-based resources access
- basic logon point, extending to 73-78

Internet Control Message Protocol. *See* **ICMP**

L

LDAP authentication profiles
- creating, to Linux openLDAP 95, 96
- creating, to Microsoft's Active Directory 90-92
- creating, to Novell's eDirectory Directory 94

LDAP authorization, SmartAccess logon points
- about 159
- group membership attributes 159

LDAPS 90
License Grace Period 22
licenses
- importing 30-33
- obtaining 25

License Server
- about 125
- options 24, 25
- securing, with HTTPS 35, 36
- URL 125

License Server 11.10
- installing 26, 27

License Server Administration
- about 33
- dashboard, securing 34

License Server VPX
- importing, into Citrix XenServer 28-30

license types, CAG
- platform 22, 23
- universal 22, 23

licensing, CAG
- about 21, 47, 48
- concurrent connections 23
- License Grace Period 22

Licensing option, System Administration 129
Linux openLDAP
- LDAP authentication profiles, creating to 95, 96

logfiles
- accessing 187
- interpreting 188

logfile settings 194
logging option, System Administration 129
logon page
- user passwords, modifying on 98, 100

logon point

branding 161
creating 66-69
Logon Point Visibility
defining 160
log transfer 194, 195

M

MAPI (Mail Application Programming Interface) 151
master device, appliance failover
configuring 199
Merchandising Server
Access Gateway plug-in, distributing with 112
deliveries, configuring with 114-116
importing, into XenServer 113, 114
installing 112
Microsoft's Active Directory
LDAP authentication profiles, creating to 90-92
Microsoft Windows Server
deploying 25
Monitor tab
about 188
Active Sessions dialog 190
Audit Log wizard 192
Configurations and Warnings wizard 192
debug log 193
EPA Log 193
Info Log wizard 193
Running Information wizard 189, 190
System Information wizard 188
multiple logon points 20
Multi-stream ICA 13
MyCitrix
URL 25

N

name service providers option, System Administration 127
NAT (network address translation) 56
NetScaler 9
NetScaler Model 2010 Appliance 10
NetScaler Model MPX 5500 Appliance 11
netstat command 123
network access
controlling, device profiles used 141
network architecture 37, 38
networking options, System Administration 127
network resources
about 143
access, controlling via SmartGroups 147
audit access 144
defining 144
defining, on single server 145, 146
general properties 149
network lists 148
protocols and port ranges 149
Not for Resale(NFR)license 193
Novell's eDirectory Directory
LDAP authentication profiles, creating to 94

O

Open Virtual Format (OVA) 39
Operating System scan type, device profiles 135

P

password option, System Administration 128
PKI Certificates 20
platform license
about 22
features 23
plug-in
installing 105, 106
obtaining 105
plug-in properties
configuring 107-110
Ports scan type, device profiles 136
private network
static route, adding to 45-47
process scan type, device profiles 133, 134
Protiva
about 86
configuring 86
guidelines, for configuration 86
protocols and ports, network resources
enabling 149
ICMP (Internet Control Message Protocol)

149
Repeater 150
TCP (Transport Control Protocol) 149
UDP (User Datagram Protocol) 149
PuTTY
about 204
download link 204

Q

quality of service (QoS) 13

R

RADIUS authentication profile
creating 83-86
RADUIS 83
registry scan type, device profiles 134
Remote Access Dial In User Service. *See* **RADIUS**
remote access issues
resolving, CAG used 19
Remote Access solution
designing 17
Remote Authentication and Dial-In User Service (RADIUS) 20
remote users
website, configuring for 59-61
Repeater 150
resources
accessing, on private network with CAG plug-in 184, 185
RSA SecurID authentication profiles
creating 88, 89
Running information wizard, Monitor tab
about 190
options 189

S

SafeWord
configuring 87, 88
Secure Access method
modifying 62-65
Secure Copy Program(SCP) 195
Secure Sockets Layer (SSL) 22
Secure Ticket Authorities (STAs) 54, 63, 71
Service-level agreements (SLAs) 13
Session Reliability 70
SG2 SmartGroup 174
signed SMBv1/v2 151
slave device, appliance failover
configuring 200, 201
SmartAccess login points 104
SmartAccess logon points 66
about 23, 166
authentication 158
defining 155, 156
demonstrating 125
General Properties 157
Logon Point Visibility, defining 160
SmartGroup priority
defining 174, 175
SmartGroups
about 163
defining 164
General Information 164
Group Criteria section 166
Group Settings section 169
home page 165, 166
SmartGroup SG1 174
SMBv2 151
SSH access
enabling, to command line 203, 204
SSL certificates
about 48
adding, to CAG 48-51
static route
adding, to private network 45-47
static routes option, System Administration 128
System Administration options
about 126
address pools 128
Appliance failover 127
date and time 129
deployment mode 128
licensing 129
logging 129
name service providers 127
networking 127
password 128
static routes 128
System Information wizard, Monitor tab 188

system menu 206, 207

T

TCP 149, 151
TCP port 2598 9
Traffic Prioritization and Quality of Service 152
Transport Control Protocol. *See* TCP
troubleshooting menu 207, 208
two-factor authentication
  implementing, on CAG 100-102

U

UDP 149
universal licenses
  about 22, 23
  adding 103, 104
user access
  tracking 94
User Datagram Protocol. *See* UDP
users
  passwords, modifying on logon page 98, 100

V

versions, CAG
  about 12
  Access Gateway 5.x 15
  Access Gateway 9.2 Enterprise Edition 14
  Access Gateway 9.3 Enterprise Edition 14
  Access Gateway 10 13
  Access Gateway Milestones 12
virtual appliance
  downloading, from Citrix 38
virtual private network (VPN) 8
VMW 28
VMware
  CAG, importing into 39
VPN access 20
VPX Access Gateway 5 21
VPX Express 21
VPX License Server
  deploying 25

W

Web Interface placement 58
Web Interface (WI) 57
web portal
  initial configuration, completing from 44
website
  configuring, for remote users 59-61

X

xe command 40
XenApp
  about 25, 151
  accessing, ICA Proxy used 18
XenApp access controls 70
XenApp Server farms
  accessing, with CAG 72
XenDesktop
  about 25, 151
  accessing, ICA Proxy used 18
XenDesktop access controls 70
XenServer
  CAG, importing into 39, 40
  Merchandising Server, importing into 113, 114

Z

zypper command 83

Thank you for buying

Citrix Access Gateway VPX 5.04 Essentials

About Packt Publishing

Packt, pronounced 'packed', published its first book "Mastering phpMyAdmin for Effective MySQL Management" in April 2004 and subsequently continued to specialize in publishing highly focused books on specific technologies and solutions.

Our books and publications share the experiences of your fellow IT professionals in adapting and customizing today's systems, applications, and frameworks. Our solution based books give you the knowledge and power to customize the software and technologies you're using to get the job done. Packt books are more specific and less general than the IT books you have seen in the past. Our unique business model allows us to bring you more focused information, giving you more of what you need to know, and less of what you don't.

Packt is a modern, yet unique publishing company, which focuses on producing quality, cutting-edge books for communities of developers, administrators, and newbies alike. For more information, please visit our website: www.packtpub.com.

About Packt Enterprise

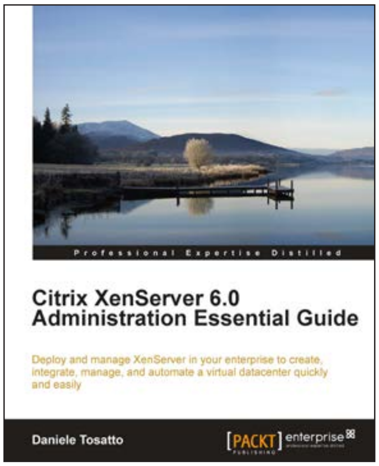
In 2010, Packt launched two new brands, Packt Enterprise and Packt Open Source, in order to continue its focus on specialization. This book is part of the Packt Enterprise brand, home to books published on enterprise software – software created by major vendors, including (but not limited to) IBM, Microsoft and Oracle, often for use in other corporations. Its titles will offer information relevant to a range of users of this software, including administrators, developers, architects, and end users.

Writing for Packt

We welcome all inquiries from people who are interested in authoring. Book proposals should be sent to author@packtpub.com. If your book idea is still at an early stage and you would like to discuss it first before writing a formal book proposal, contact us; one of our commissioning editors will get in touch with you.

We're not just looking for published authors; if you have strong technical skills but no writing experience, our experienced editors can help you develop a writing career, or simply get some additional reward for your expertise.

[PACKT] enterprise
PUBLISHING
professional expertise distilled


Professional Expertise Distilled
Citrix XenServer 6.0 Administration Essential Guide
Deploy and manage XenServer in your enterprise to create, integrate, manage, and automate a virtual datacenter quickly and easily
Daniele Tosatto
[PACKT] enterprise

Citrix XenServer 6.0 Administration Essential Guide

ISBN: 978-1-84968-616-7 Paperback: 364 pages

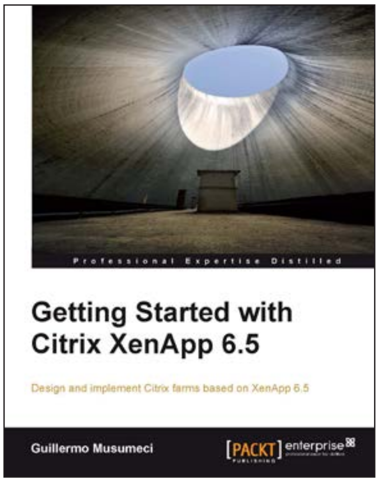
Deploy and manage XenServer in your enterprise to create, integrate, manage, and automate a virtual datacenter quickly and easily

1. This book and eBook will take you through deploying XenServer in your enterprise, and teach you how to create and maintain your datacenter

2. Manage XenServer and virtual machines using Citrix management tools and the command line

3. Organize secure access to your infrastructure using role-based access control

---


Professional Expertise Distilled
Getting Started with Citrix XenApp 6.5
Design and implement Citrix farms based on XenApp 6.5
Guillermo Musumeci
[PACKT] enterprise

Getting Started with Citrix XenApp 6.5

ISBN: 978-1-84968-666-2 Paperback: 478 pages

Design and implement Citrix farms based on XenApp 6.5

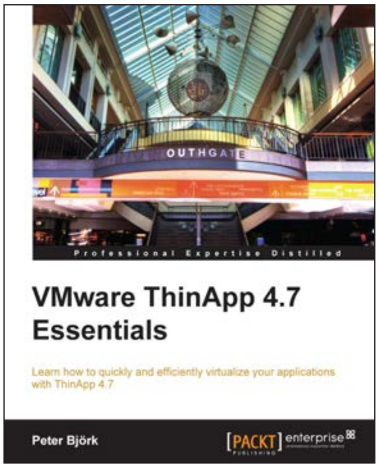
1. Use Citrix management tools to publish applications and resources on client devices with this book and eBook

2. Deploy and optimize XenApp 6.5 on Citrix XenServer, VMware ESX, and Microsoft Hyper-V virtual machines and physical servers

3. Understand new features included in XenApp 6.5 including a brand new chapter on advanced XenApp deployment covering topics such as unattended install of XenApp 6.5, using dynamic data center provisioning, and more

Please check **www.PacktPub.com** for information on our titles

[PACKT] enterprise
professional expertise distilled
PUBLISHING

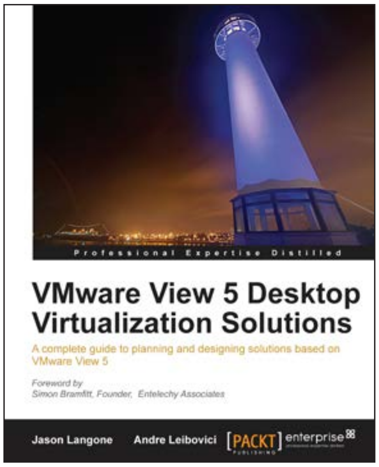

Professional Expertise Distilled
VMware ThinApp 4.7 Essentials
Learn how to quickly and efficiently virtualize your applications with ThinApp 4.7
Peter Björk
[PACKT] enterprise

VMware ThinApp 4.7 Essentials

ISBN: 978-1-84968-628-0 Paperback: 256 pages

Learn how to quickly and efficiently virtualize your applications with ThinApp 4.7

1. Practical book which provides the essentials of application virtualization with ThinApp 4.7
2. Learn the various methods and best practices of application packaging and deployment
3. Save money and time on your projects with this book by learning how to create portable applications


Professional Expertise Distilled
VMware View 5 Desktop Virtualization Solutions
A complete guide to planning and designing solutions based on VMware View 5
Foreword by
Simon Bramfitt, Founder, Entelechy Associates
Jason Langone
Andre Leibovici
[PACKT] enterprise

VMware View 5 Desktop Virtualization Solutions

ISBN: 978-1-84968-112-4 Paperback: 288 pages

A complete guide to planning and designing solutions based on VMware View 5

1. Written by VMware experts Jason Langone and Andre Leibovici, this book is a complete guide to planning and designing a solution based on VMware View 5
2. Secure your Visual Desktop Infrastructure (VDI) by having firewalls, antivirus, virtual enclaves, USB redirection and filtering and smart card authentication
3. Analyze the strategies and techniques used to migrate a user population from a physical desktop environment to a virtual desktop solution

Please check **www.PacktPub.com** for information on our titles