

extentrix



Extentrix

Smart Detectors Scan Package

User's Guide

NOTICE

Extentrix Systems, FZE makes no representations or warranties with respect to the contents or use of this publication. Extentrix specifically disclaims any express or implied warranties, merchantability, or fitness for any particular purpose. Extentrix reserves the right to make any changes in specifications and other information contained in this publication without prior notice and without obligation to notify any person or entity of such revisions or changes.

© Copyright 2008-2009 All Rights Reserved

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information and retrieval systems, for any purpose other than the purchase’s personal use, without express written permission of:

Extentrix Systems, FZE

P.O.Box 4404

Dubai, UAE

<http://www.extentrix.com>

The following marks are service marks, trademarks or registered trademarks of their respective owners:

Mark	Owner
Citrix®, ICA®, Presentation Server 4.0®, Web Interface®, WinFrame®, Program Neighborhood®, Citrix Developer Network™, Citrix Alliance Partners™	Citrix Systems, Inc.

TABLE OF CONTENTS

NOTICE..... 1

TABLE OF CONTENTS 2

INTRODUCTION 4

SCANS INCLUDED INSIDE EXTENTRIX SMART DETECTORS SCAN PACKAGE 5

1. EXTENTRIX ANTIVIRUS SCAN 5

Scan description 5

Installation and configuration..... 6

 Importing scan packages..... 6

 Installing the scan package 10

2. EXTENTRIX FIREWALL SCAN 18

Scan description 18

Installation and configuration..... 19

 Importing scan packages 19

 Installing the scan package 23

3. EXTENTRIX USER OPTION AV SCAN 30

Scan description 30

Installation and configuration..... 32

 Importing scan packages 32

 Installing the scan package 36

4. EXTENTRIX USER OPTION FW SCAN 47

Scan description 47

Installation and configuration..... 48

 Importing scan packages 48

- Installing the scan package 52
- 5. EXTENTRIX ANTI SPYWARE SCAN..... 62
 - Scan description* 62
 - Installation and configuration*..... 63
 - Importing scan packages..... 63
 - Installing the scan package* 67
- 6. EXTENTRIX USER OPTION AS SCAN..... 74
 - Scan description* 74
 - Installation and configuration*..... 75
 - Importing scan packages* 75
 - Installing the scan package* 79
- SUPPORT..... 90**
- GLOSSARY 91**
- INDEX..... 92**
- ABOUT EXTENTRIX 93**

INTRODUCTION

Extentrix Smart Detectors Scan Package is specialized in offering the most powerful Scans that detect the existence of Anti-viruses and firewalls on User's devices before granting them the permission to access corporations' resources. It includes a comprehensive set of scans for Ant viruses, Antispyware and Firewalls that also provide real-time protection environment.

This package will give the administrator the power to restrict the user to run only the AVs the company trusts to offer the ultimate security. With this feature, Administrators are given the ability to scan for more than one AV at the same time and limit them to what they believe it the AV software they want the user to use.

While Extentrix is increasing the number of AV list supported it is trying to ensure that the administrator will have the upper hand to decide which AVs to check for.

Extentrix Smart Detectors Scan Package extends administrators' ability to check for an antivirus, antispyware or/and a firewall, make sure of the last update date for the antivirus and check whether the firewall is enabled or not on the client machine. It consists of:

1. Distributed File:

- EPAClient.exe/EPAPugin.exe
- Append.txt

2. Scan Packages:

- Extentrix Antivirus Scan
- Extentrix Firewall Scan
- Extentrix Antispyware Scan
- Extentrix User Option AV Scan
- Extentrix User Option FW Scan
- Extentrix User Option AS Scan

SCANS INCLUDED INSIDE EXTENTRIX SMART DETECTORS SCAN PACKAGE

Extentrix Smart Detectors Scan Package contains many Scans inside. They are:

1. EXTENTRIX ANTIVIRUS SCAN

SCAN DESCRIPTION

Scan Name: Extentrix AV Scan.

Description: It allows the administrator to check if the client machine has Antivirus installed and supported by Extentrix Anti viruses list and ensure that the installed antivirus is up to date.

Parameters:

- Show/Hide Dialog – a Boolean value which allows administrators to show (true) or hide (false) the progress dialog to the client while scanning his/her machine. To see how the progress bar looks like, refer to page 12.
- Time Allowed – an integer value which presents the numbers of days that will be allowed since last update time.

Scan Output:

- Allow Access - a Boolean output which indicates whether the client has an antivirus with allowed update period or not.

TRUE – indicates that the client has one of Extentrix supported AV installed, enable and running.

FALSE – indicates that the client doesn't have one of Extentrix supported AV installed, enable and running.
- License Status- a String output which indicates whether the scan is licensed or not.

TRIAL LICENSE – indicates that the scan has a trial license.

INVALID LICENSE – indicates that the scan hasn't a license.

VALID LICENSE – indicates that the scan is licensed.

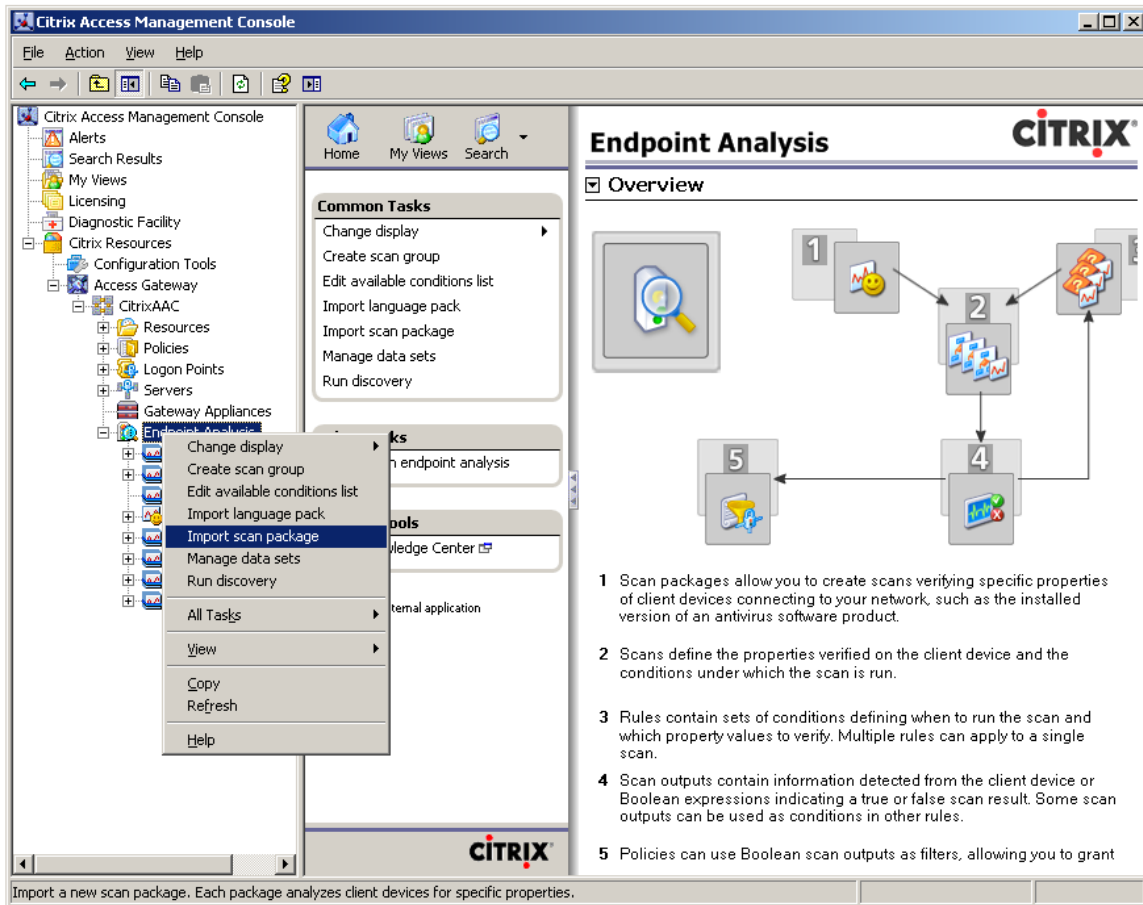
Note: If the License Status has an Invalid License value, the Allow Access will be false.

INSTALLATION AND CONFIGURATION

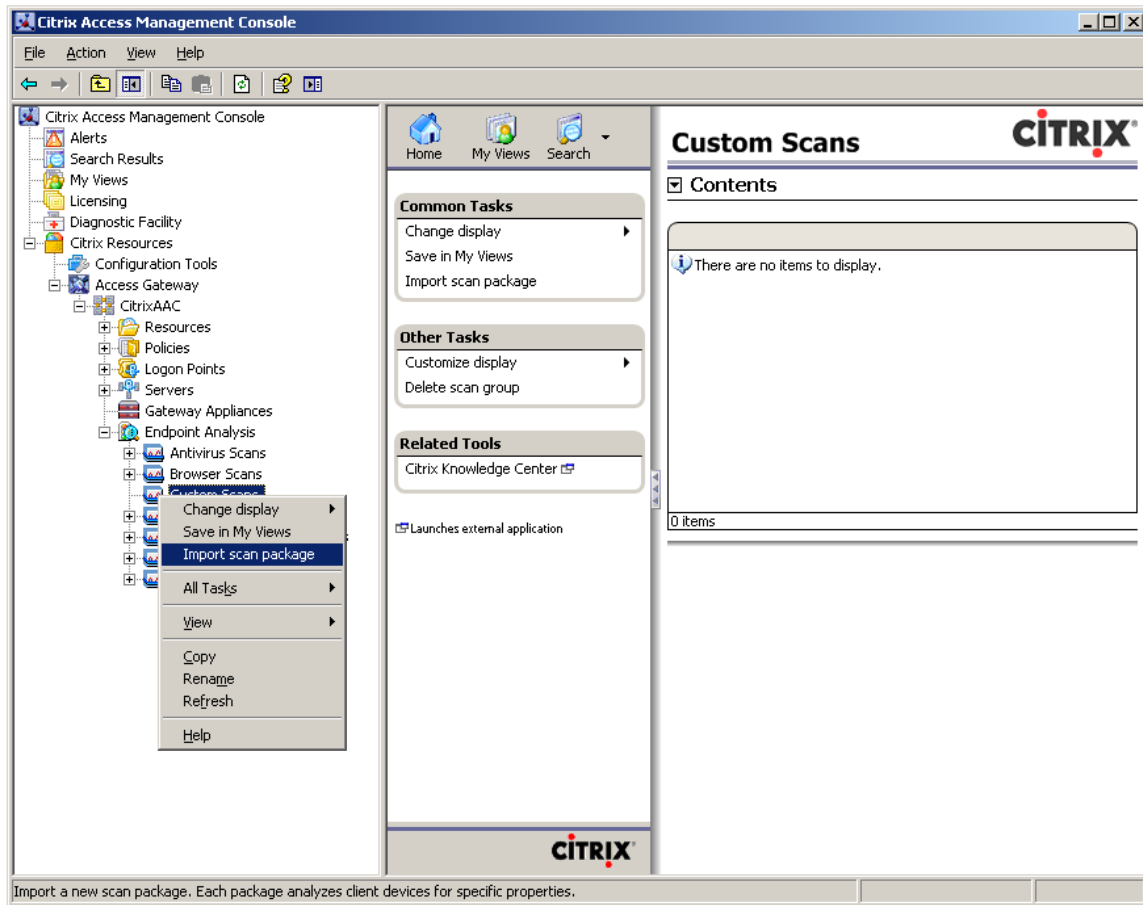
IMPORTING SCAN PACKAGES

To install a custom end point analysis scan package follow the following steps:

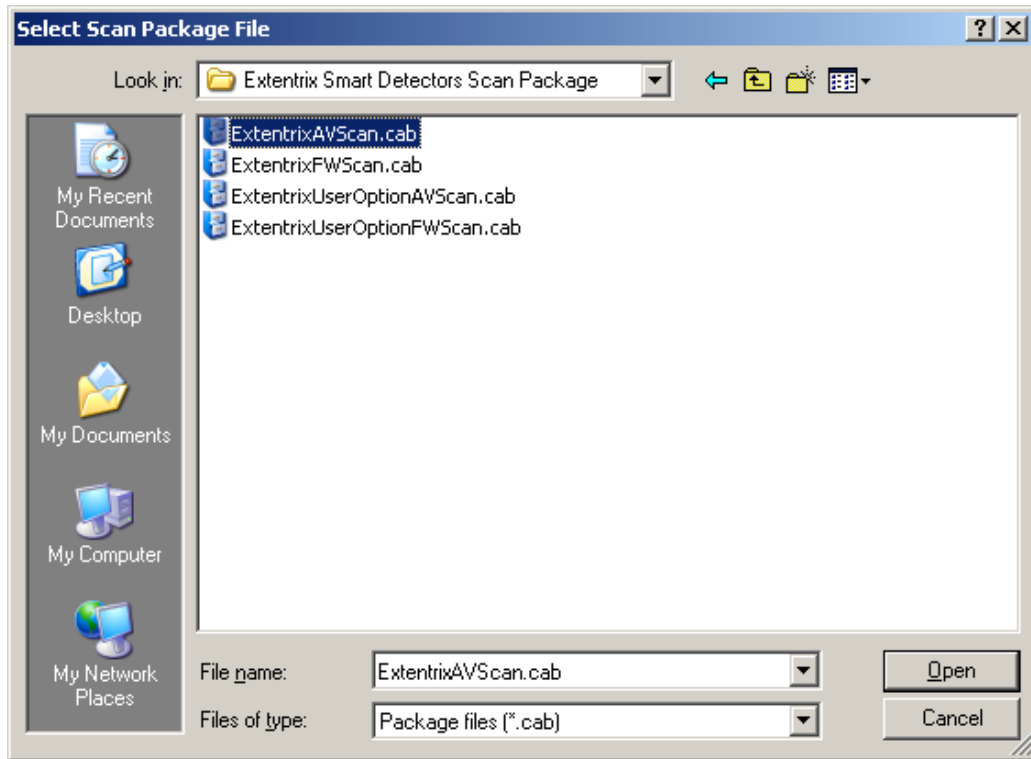
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



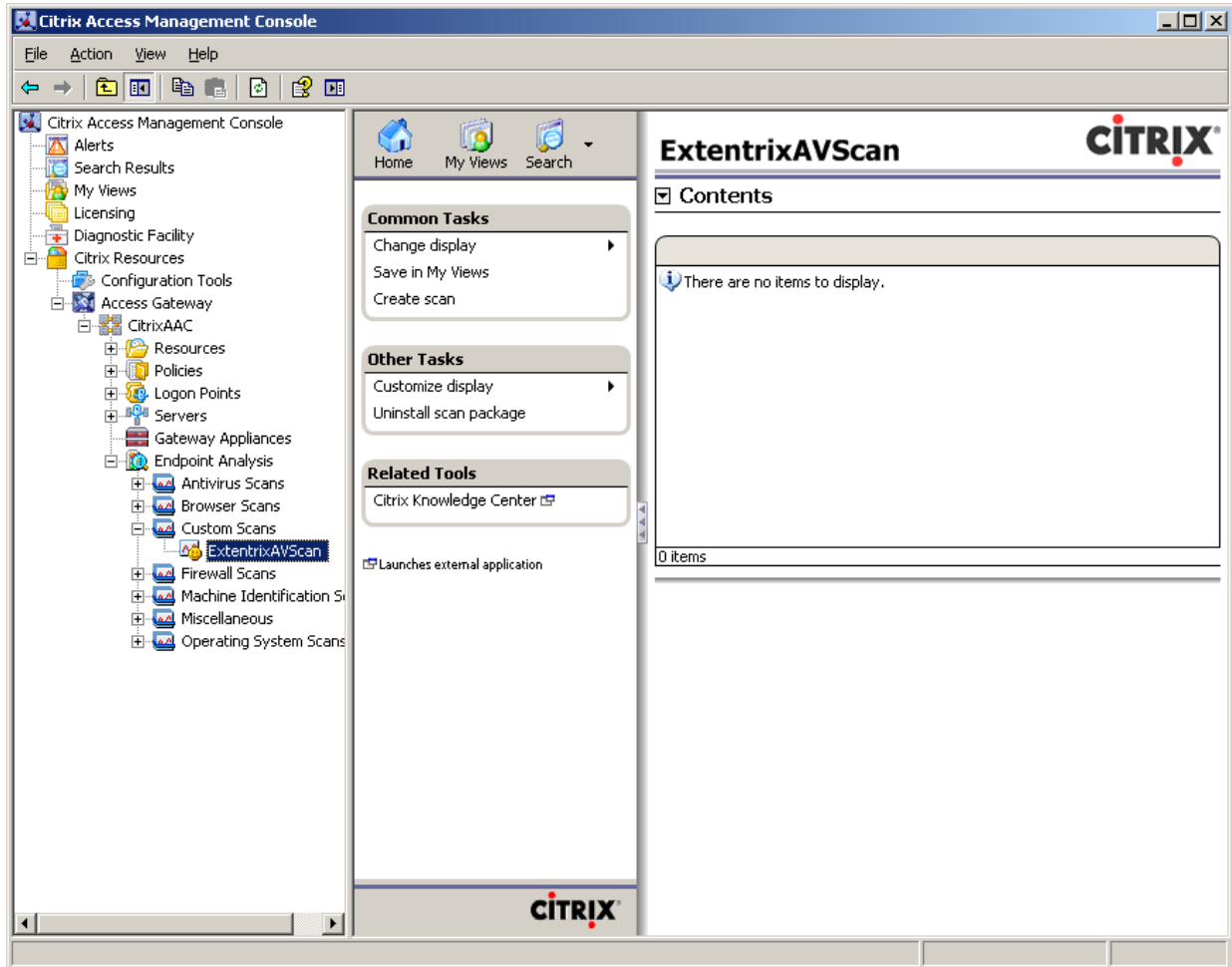
Also you can choose to insert the scan package to a specific scan package group as shown in the following picture:



3. A dialog box named **“Select Scan Package File”** will appear. Double click on the (.cab) file which contains the Scan.



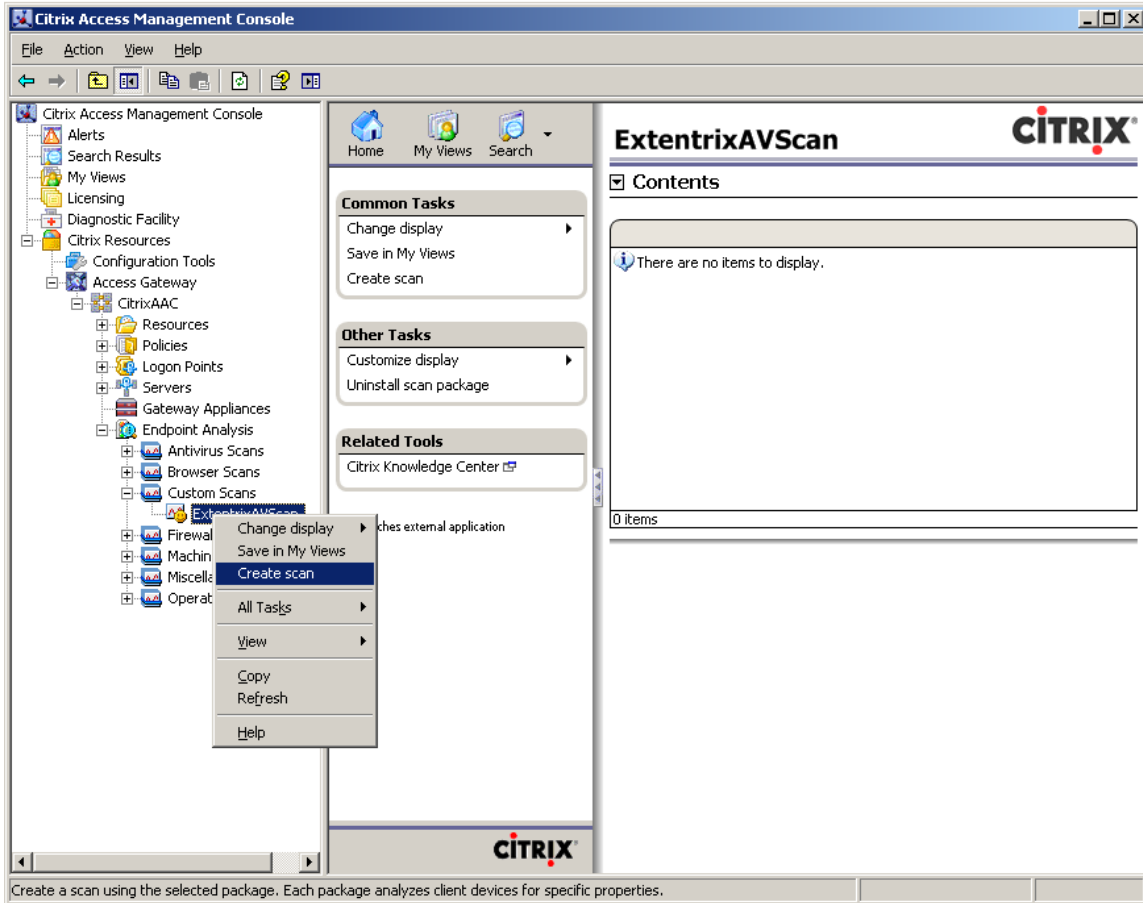
The package will be displayed in the console as shown in the following picture:



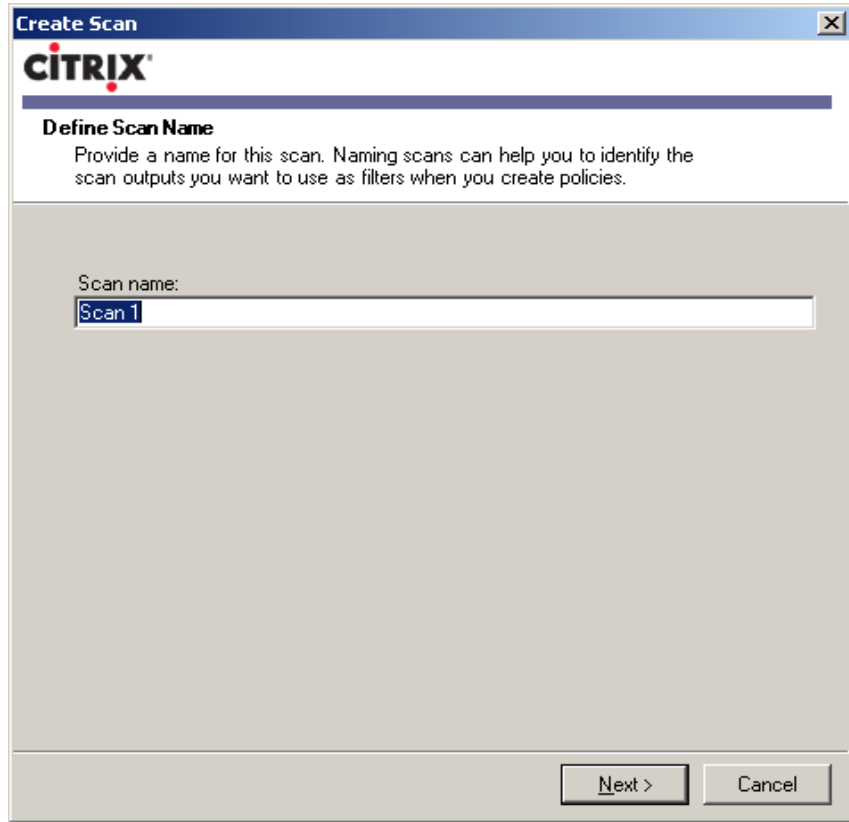
INSTALLING THE SCAN PACKAGE

Please follow the steps below to create scans and rules for the **Extentrix AV Scan**.

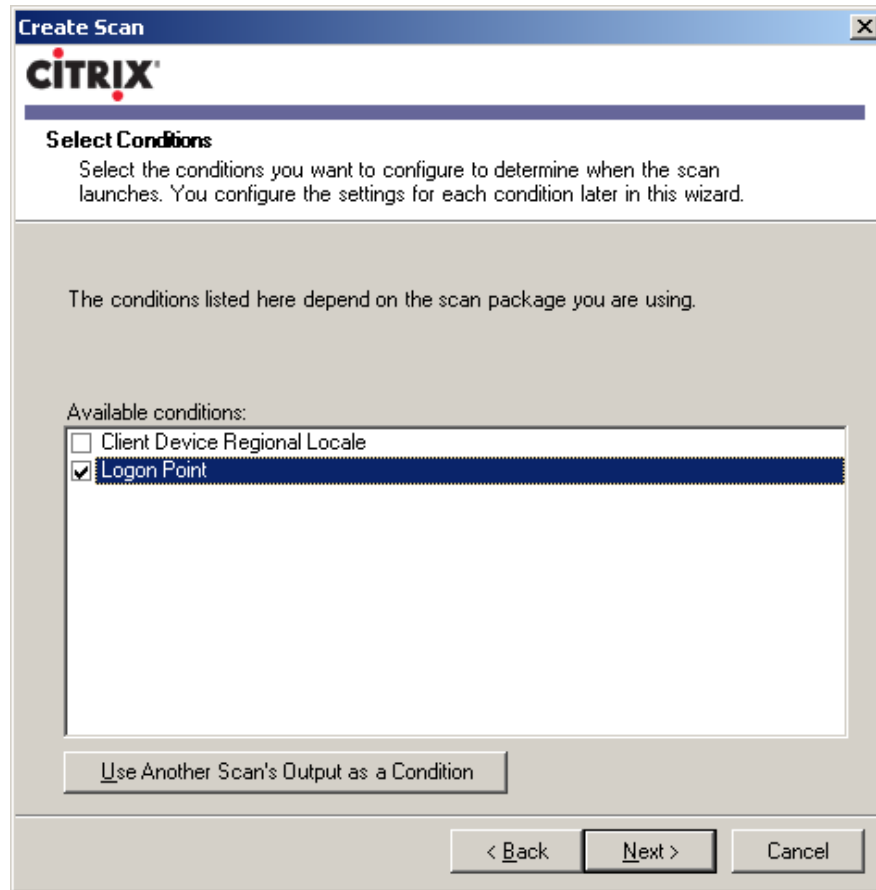
1. Select **ExtentrixAVScan** to create scan for it, right click the icon and choose **Create Scan**.



2. Type a name for the scan:



3. Set the scan conditions:



4. Type rule name and set rule conditions:

Create Scan

CITRIX

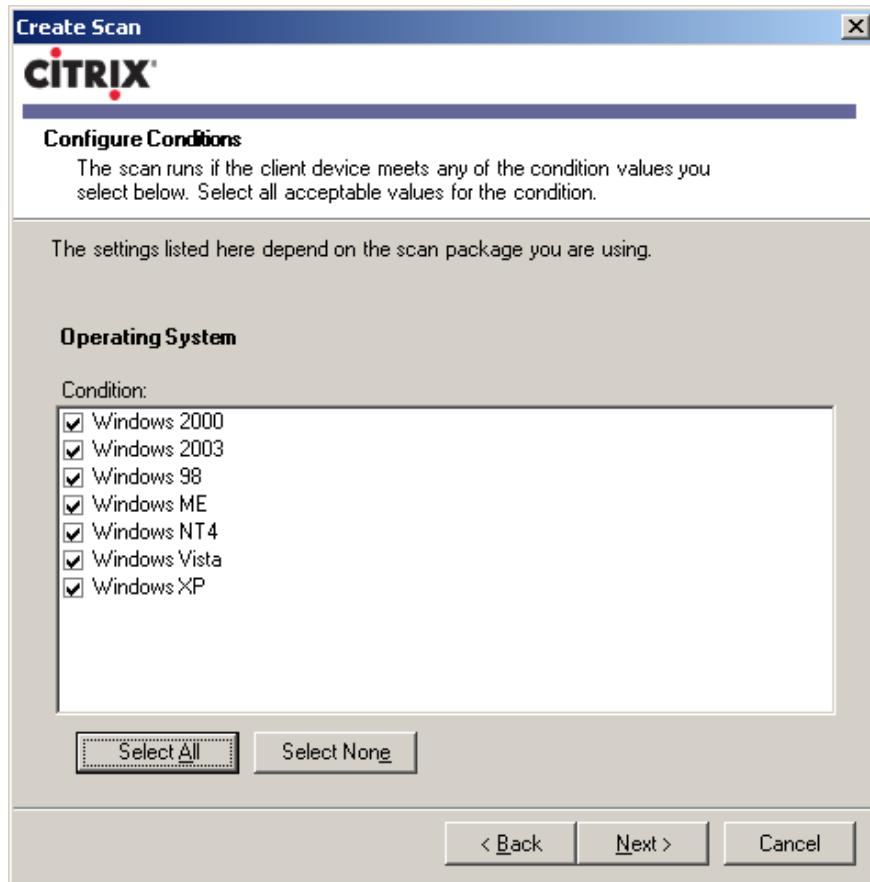
Define Rule
Rules are a combined set of conditions under which a scan is run.

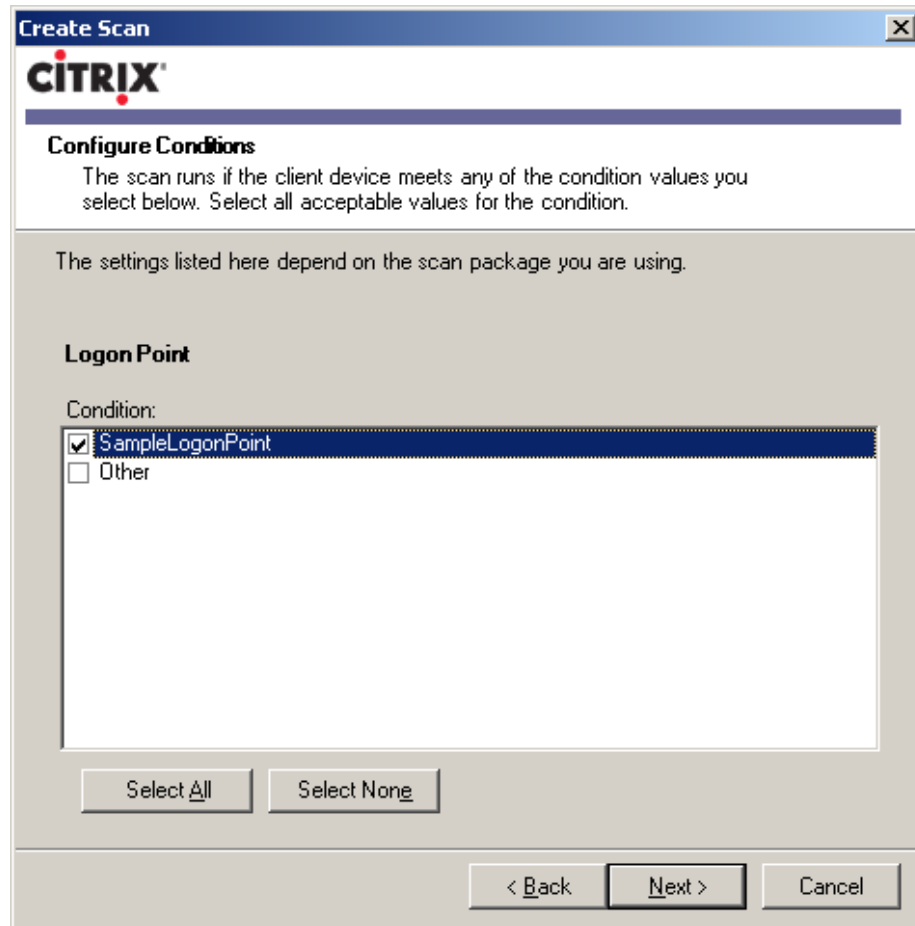
For example, your rule might be to use Scan X when the client device is running Operating System Y and Browser Version Z.

You can create multiple rules for any scan.

Rule name:

< Back Next > Cancel





5. Type the name in **Property Value**.

Create Scan

CITRIX

Define Property to Verify
The scan checks the client device for the property settings you configure below. The settings listed here depend on the scan package you are using.

Enter a whole number for this property.

Scan package:
ExtentrixAVScan

Property description:
Define the maximum time which is allowed to elapse from update date to access request date.

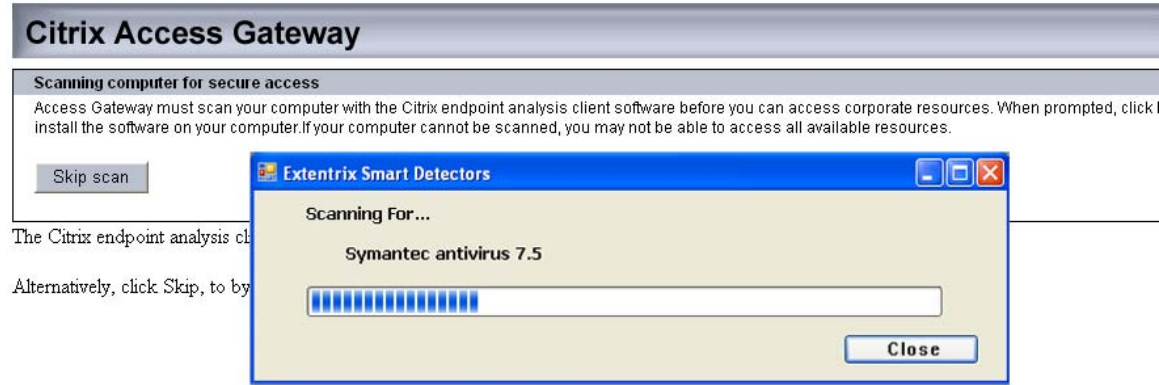
Property value:
30

Map to Scan Output

< Back Finish Cancel

6. When you are done, click **Finish**.

In the other side, when clients attempt to connect to the server that deploys this scan package, an active X control will be installed and it will perform the scanning operation. During this process, a progress bar will be shown to inform the clients about the scan progress as shown below:



2. EXTENTRIX FIREWALL SCAN

SCAN DESCRIPTION

Scan Name: Extentrix FW Scan.

Description: It allows the administrator to check if the client machine has Firewall installed and supported by Extentrix Firewalls list and ensure it is enabled and running on the client machine.

Parameters:

- Show/Hide Dialog – a Boolean value which allows administrators to show (true) or hide (false) the progress dialog to the client while scanning his/her machine. To see how the progress bar looks like, refer to page 21.
- Both Checks: a Boolean value which indicates whether check if a firewall is installed or/and enabled.

TRUE – indicates Checking for both conditions: installed and enabled.

FALSE – indicates Checking just for installed condition.

Scan Output:

- Allow Access - a Boolean output which indicates whether the client has an firewall installed and/or enable.
TRUE – indicates that the client's machine has at least one firewall installed and/or enabled.
FALSE – indicates that the client's machine doesn't have any of Extentrix Firewalls supported list or is not enabled.
- License Status- a String output which indicates whether the scan is licensed or not.
TRIAL LICENSE – indicates that the scan has a trial license.
INVALID LICENSE – indicates that the scan hasn't a license.
VALID LICENSE – indicates that the scan is licensed.

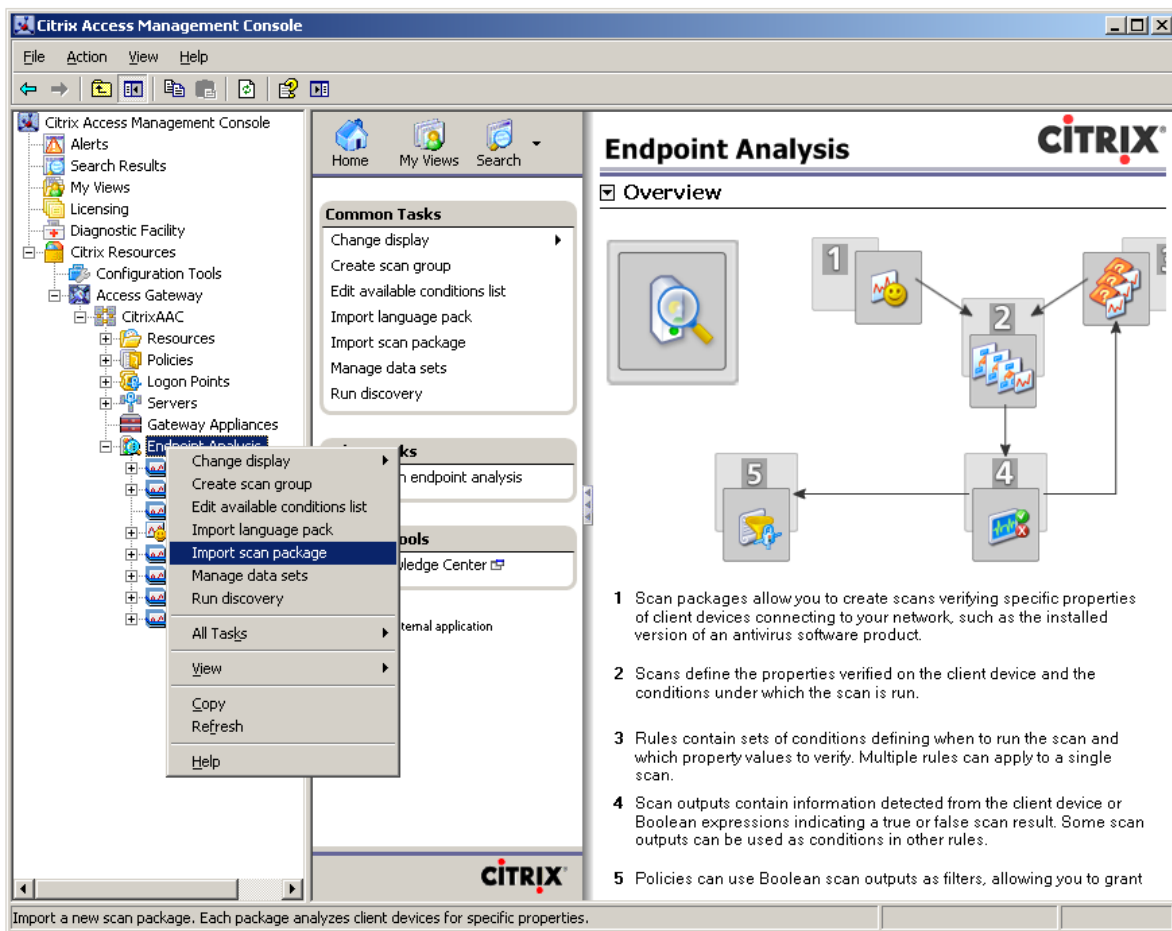
Note: If the License Status has an Invalid License value, the Allow Access will be false.

INSTALLATION AND CONFIGURATION

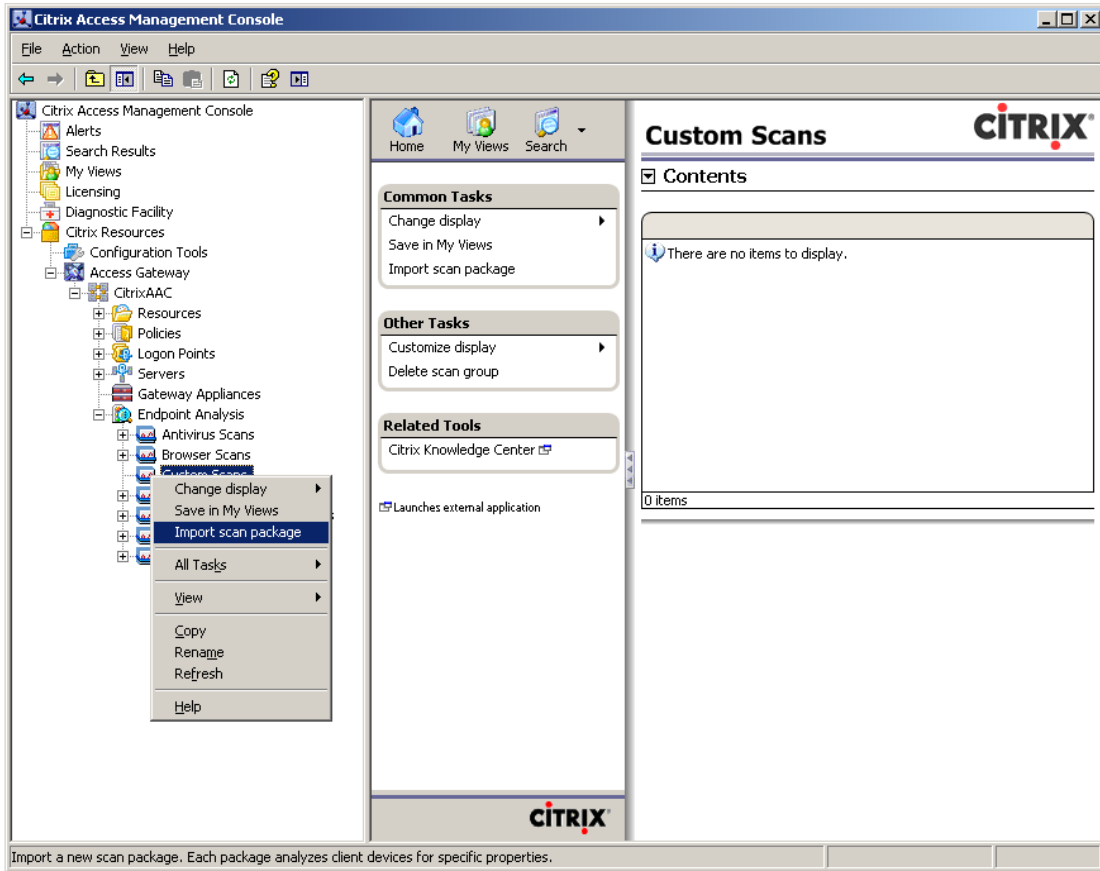
IMPORTING SCAN PACKAGES

To install a custom end point analysis scan package follow the following steps:

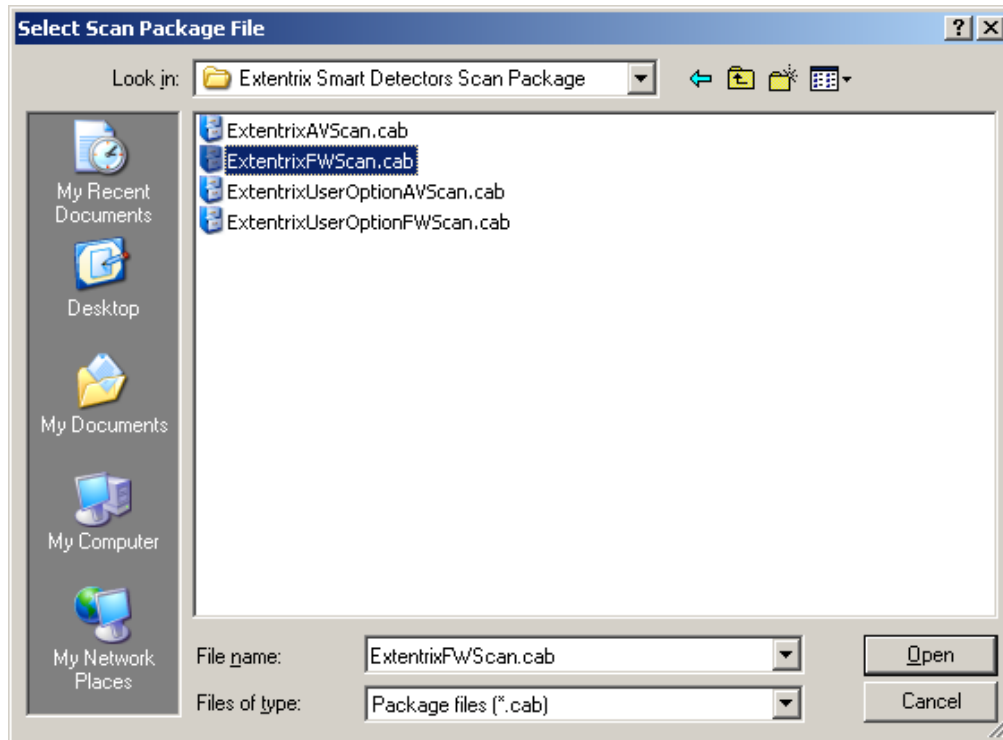
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



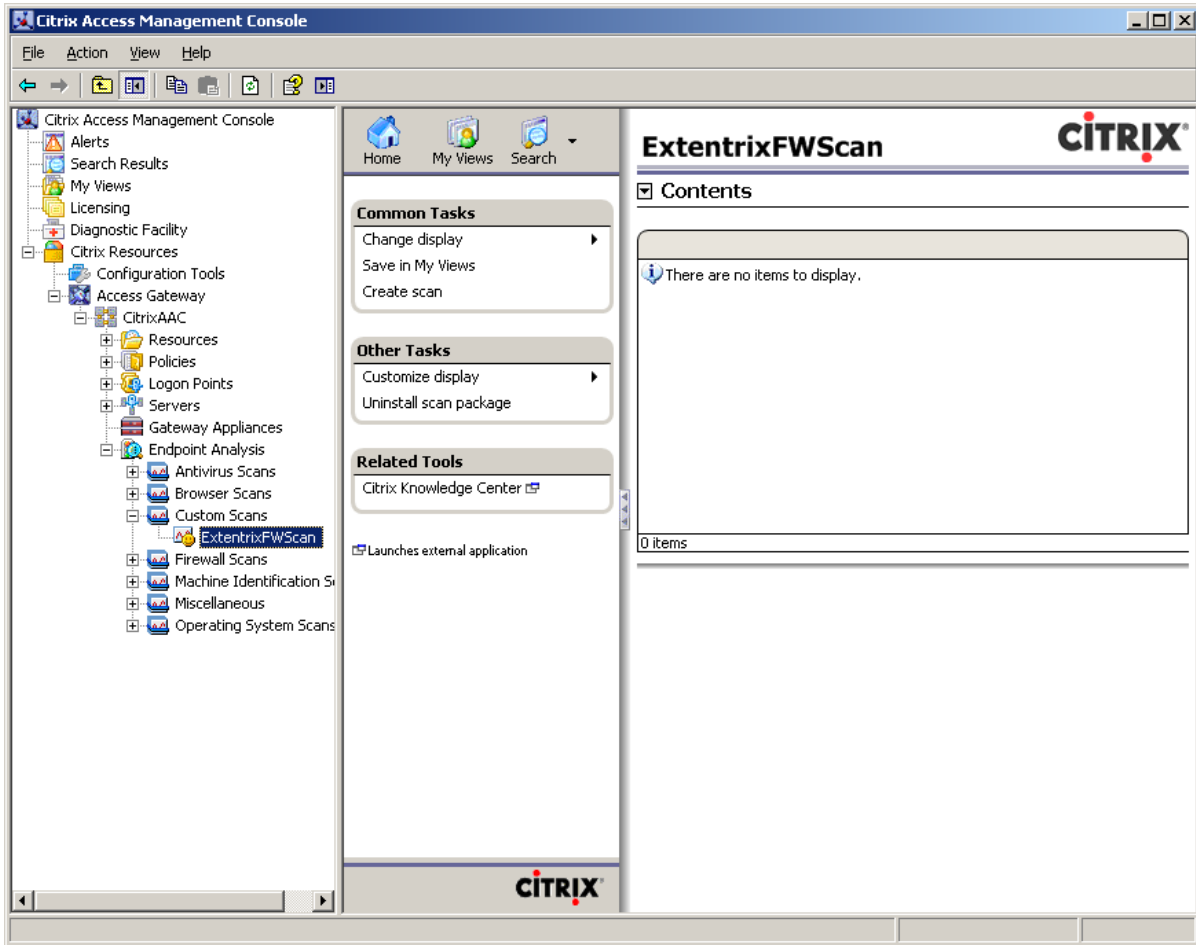
Also you can choose to insert the scan package to any scan category listed in the tree as shown in the following picture:



3. A dialog box named **“Select Scan Package File”** will appear. Double click on the (.cab) file which contains the Scan.



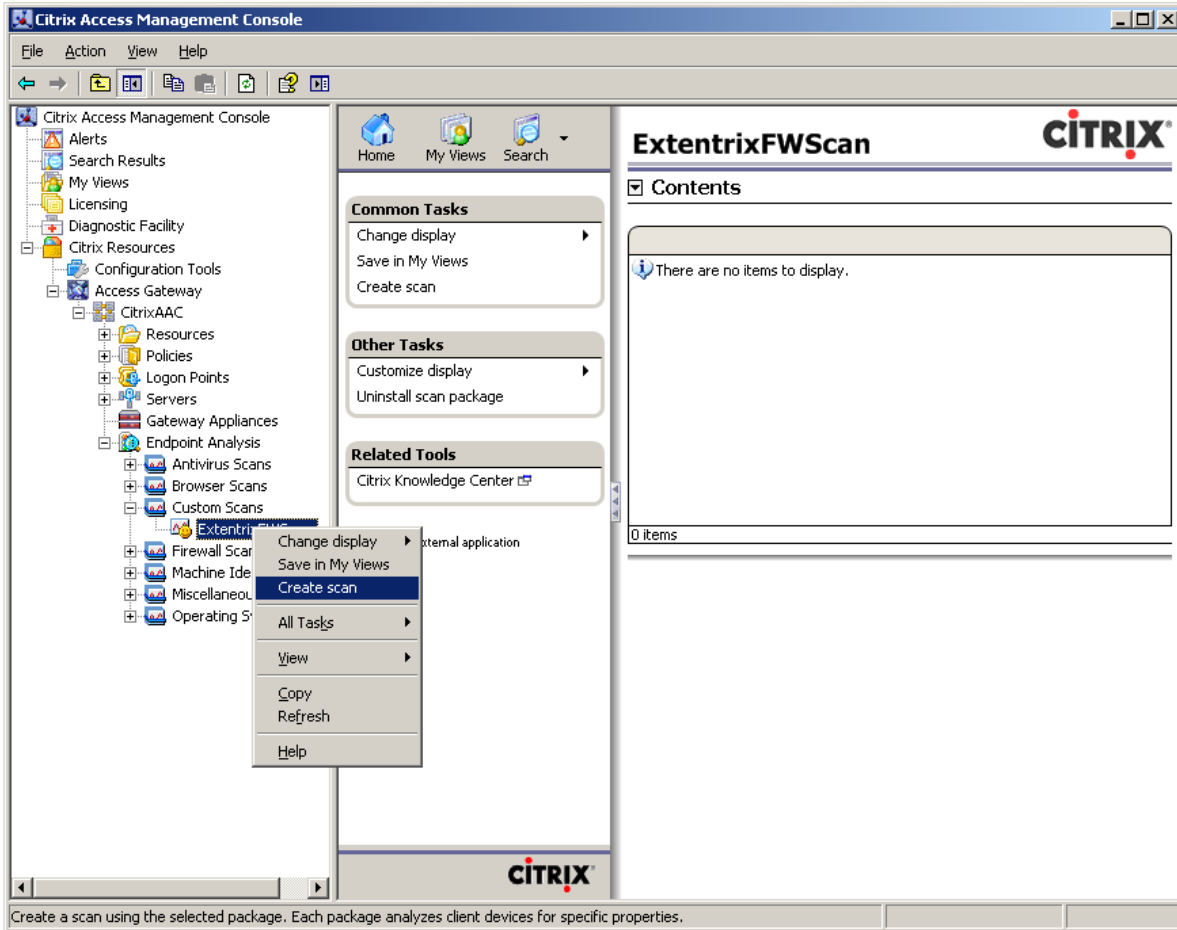
The package will be displayed in the console as shown in the following picture:



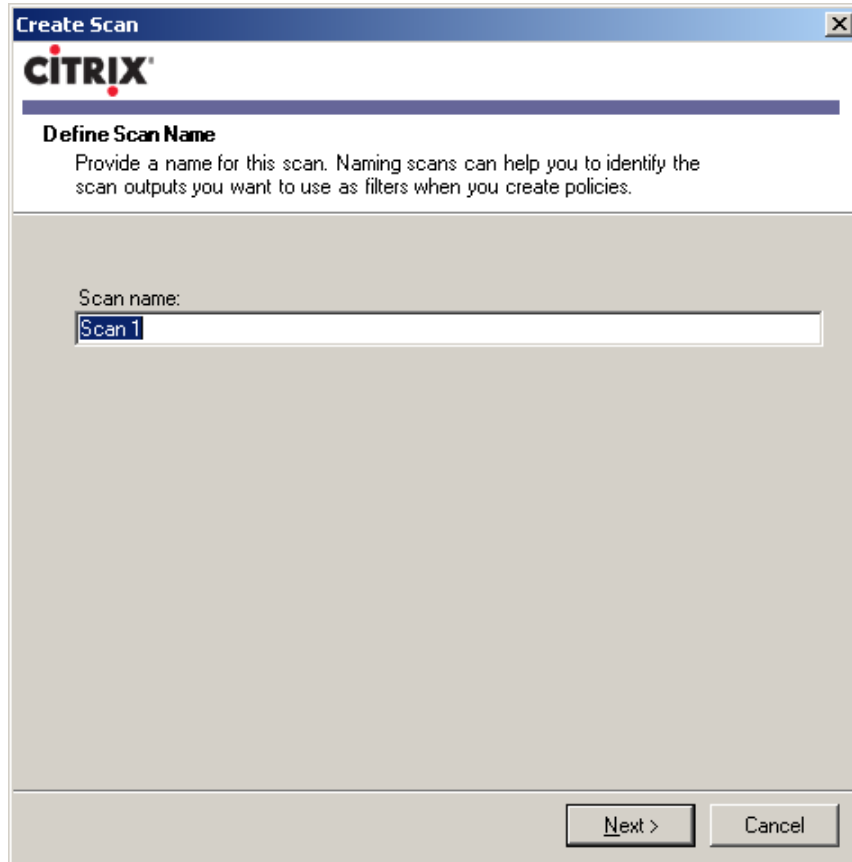
INSTALLING THE SCAN PACKAGE

Please follow the steps below to create scans and rules for the **Extentrix Firewall Scan**.

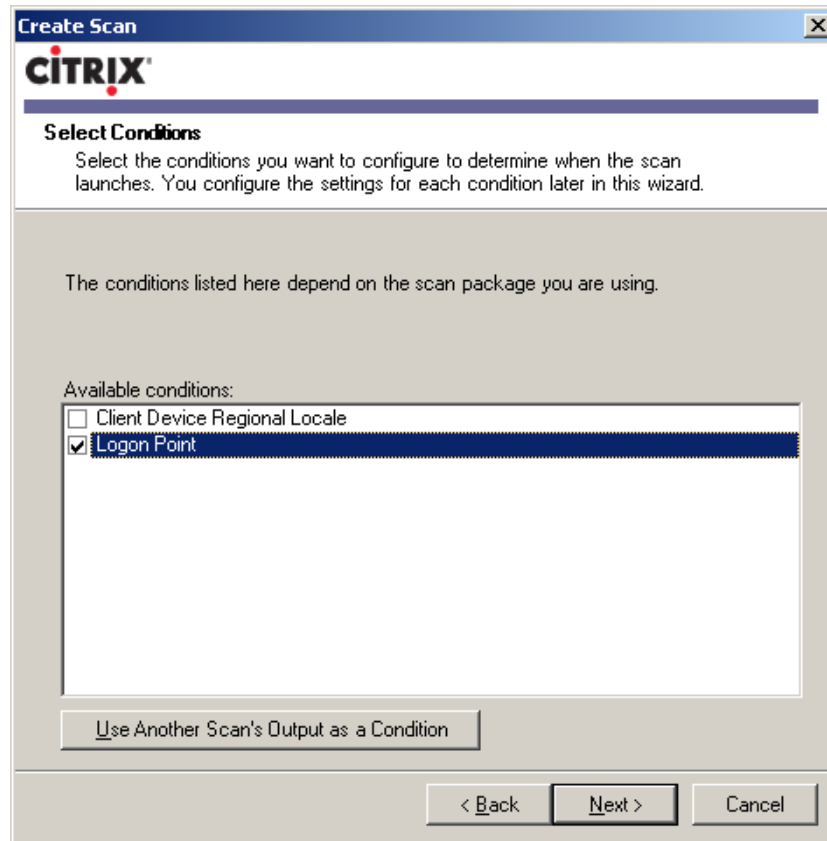
1. Select **ExtentrixFWScan** to create scan for it, right click the icon and choose **Create Scan**.



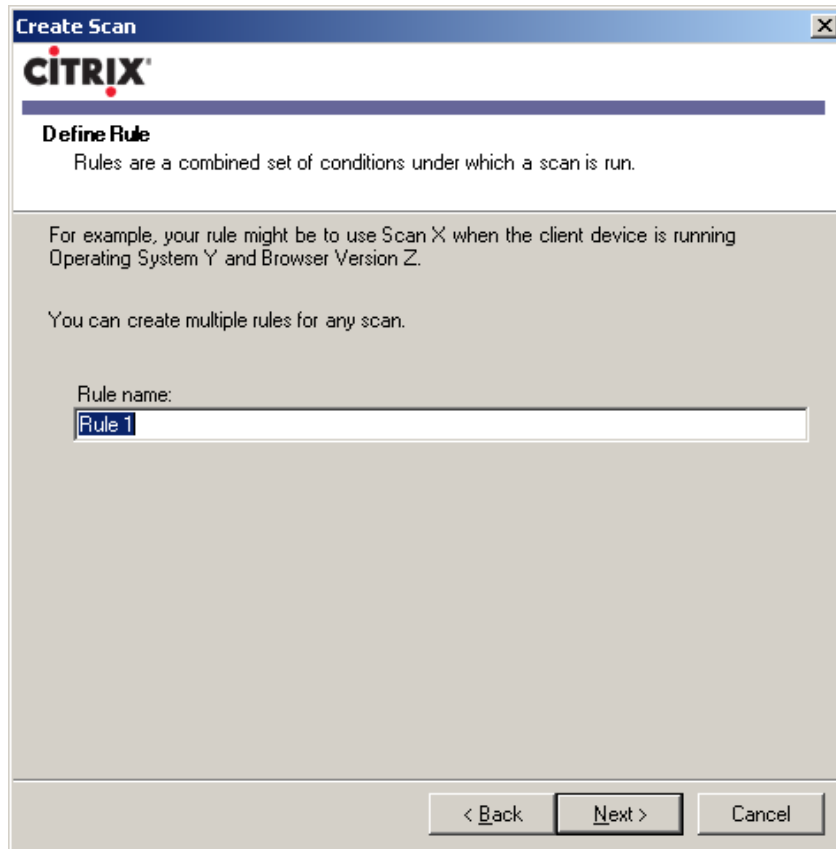
2. Type a name for the scan:

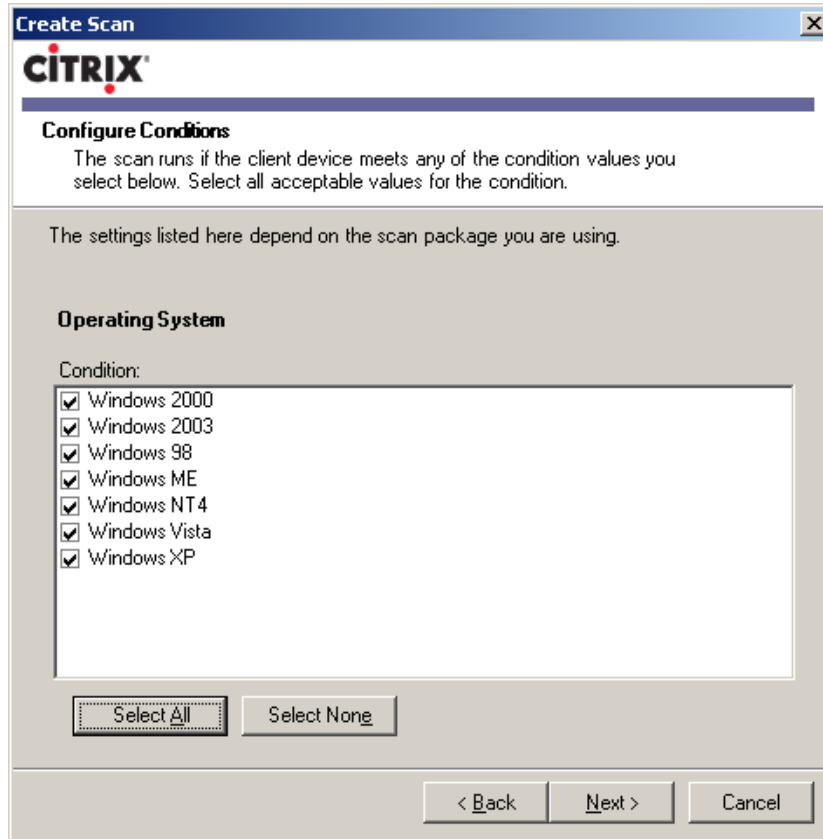


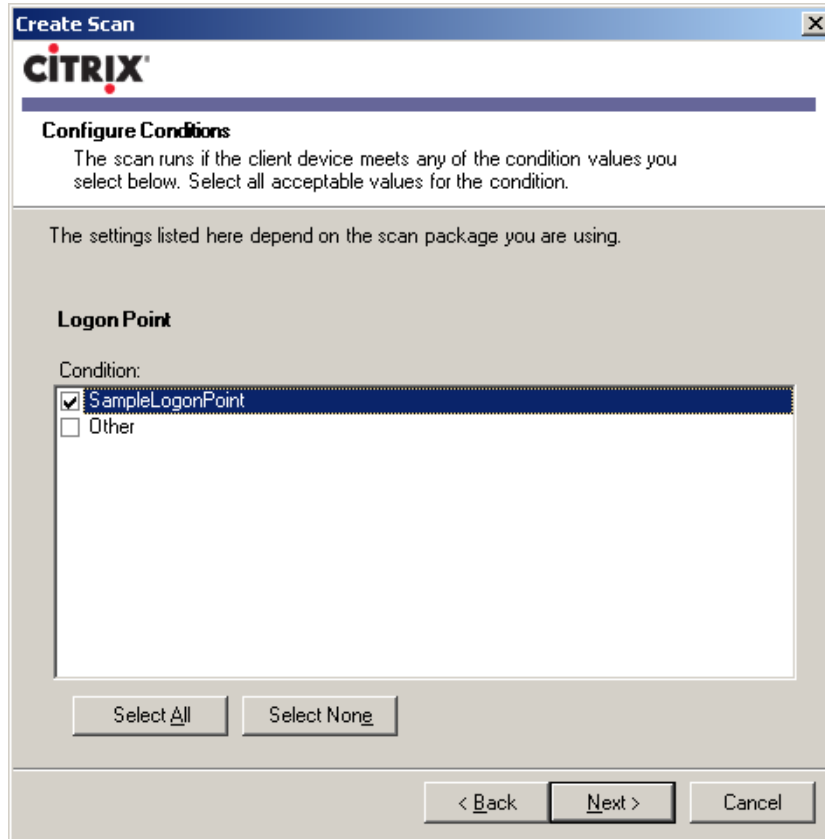
3. Set the scan conditions:



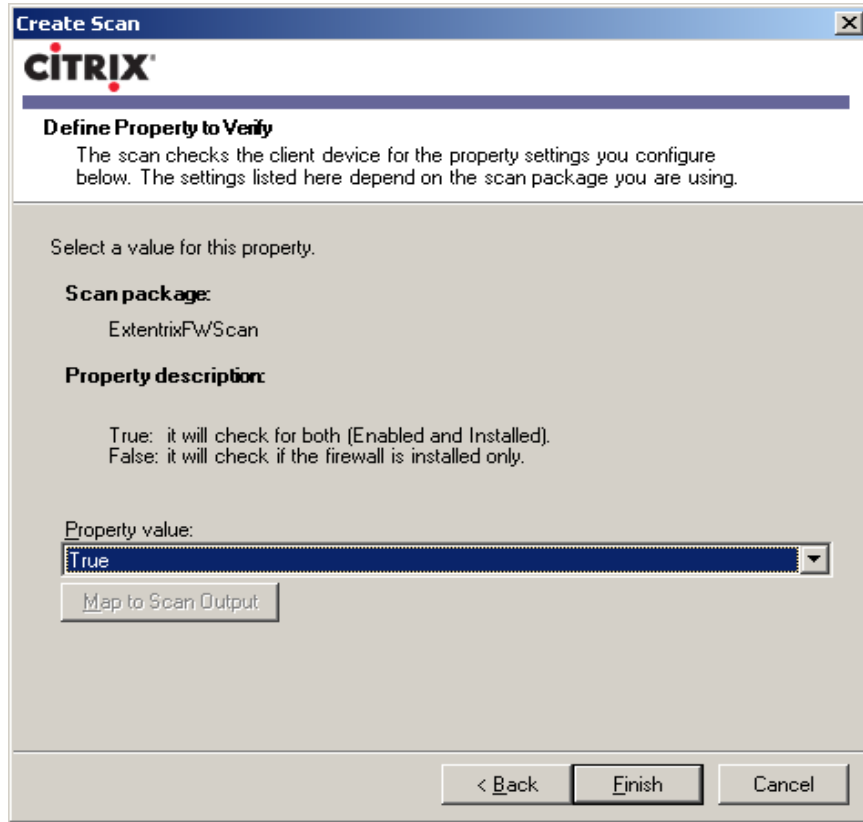
4. Type rule name and set rule conditions:







5. Type the name in **Property Value**.



6. When you are done, click **Finish**.

In the other side, when clients attempt to connect to the server that deploys this scan package, an active X control will be installed and it will perform the scanning operation. During this process, a progress bar will be shown to inform the clients about the scan progress as shown below:



3. EXTENTRIX USER OPTION AV SCAN

SCAN DESCRIPTION

Scan Name: Extentrix User Option AV Scan.

Description: This scan will check each Antivirus defined in Extentrix Antiviruses supported list, if it exists in the client machine, up to date and running. It makes sure of:

- Existence of the AV.
- Real time protection.
- Last update virus definition files.

Parameters:

- Show/Hide Dialog – a Boolean value which allows administrators to show (true) or hide (false) the progress dialog to the client while scanning his/her machine. To see how the progress bar looks like, refer to page 32.
- AV Map – a double-columned data set, each one of its records has an Antivirus name and time allowed pair. Antivirus name is a string value as named on <http://www.extentrix.com/EPA/AVsFWs.htm> and the time allowed is a string value that defines number of days of last update time allowed to the AV.

Scan Output:

- Allow Access - a Boolean output which indicates whether the client has an antivirus with allowed update period or not.

TRUE – indicates that the client has one of supported administrator AV list (list created by administrator using Extentrix supported list) installed, enable and running.

FALSE – indicates that the client doesn't have one of supported administrator AV list (list created by administrator using Extentrix supported list) installed, enable and running.
- License Status- a String output which indicates whether the scan is licensed or not.

TRIAL LICENSE – indicates that the scan has a trial license.

INVALID LICENSE – indicates that the scan hasn't a license.

VALID LICENSE – indicates that the scan is licensed.

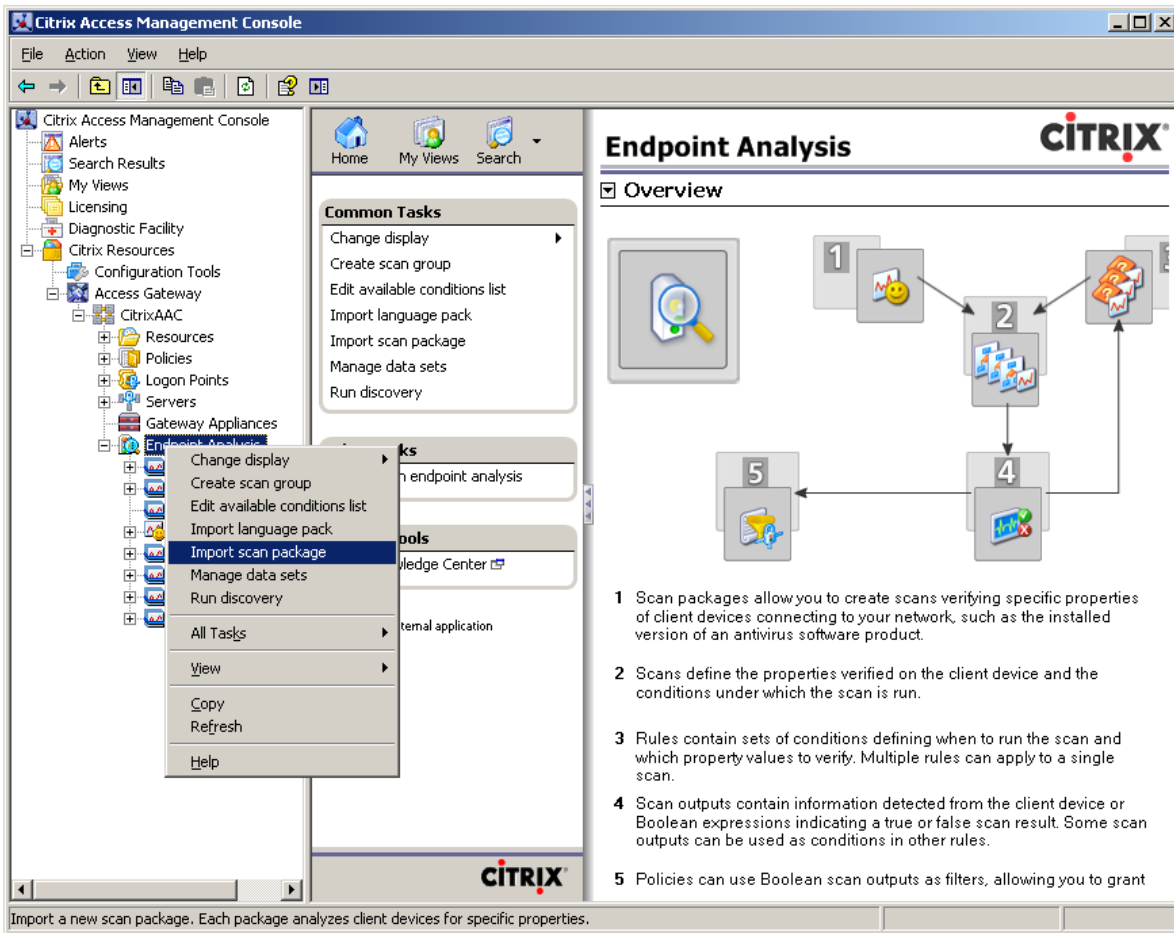
Note: If the License Status has an Invalid License value, the Allow Access will be false.

INSTALLATION AND CONFIGURATION

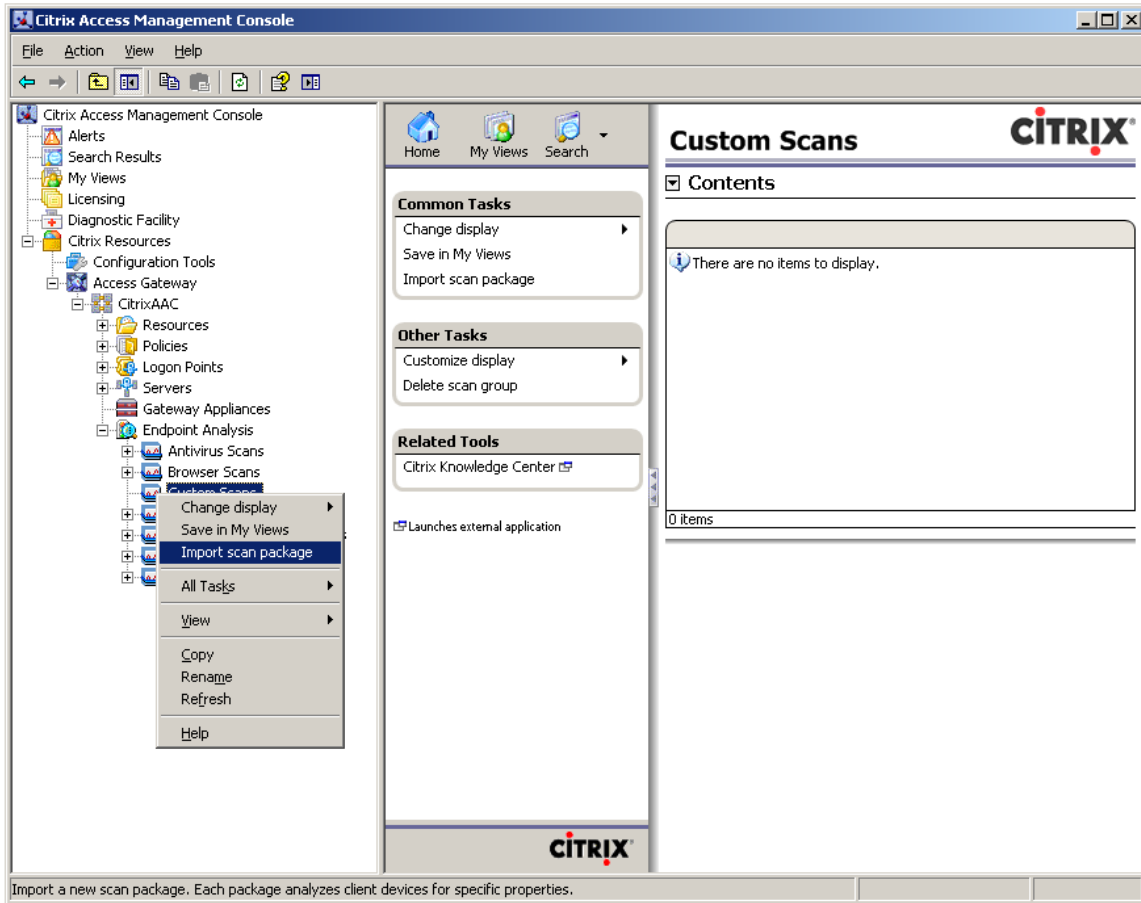
IMPORTING SCAN PACKAGES

To install a custom end point analysis scan package follow the following steps:

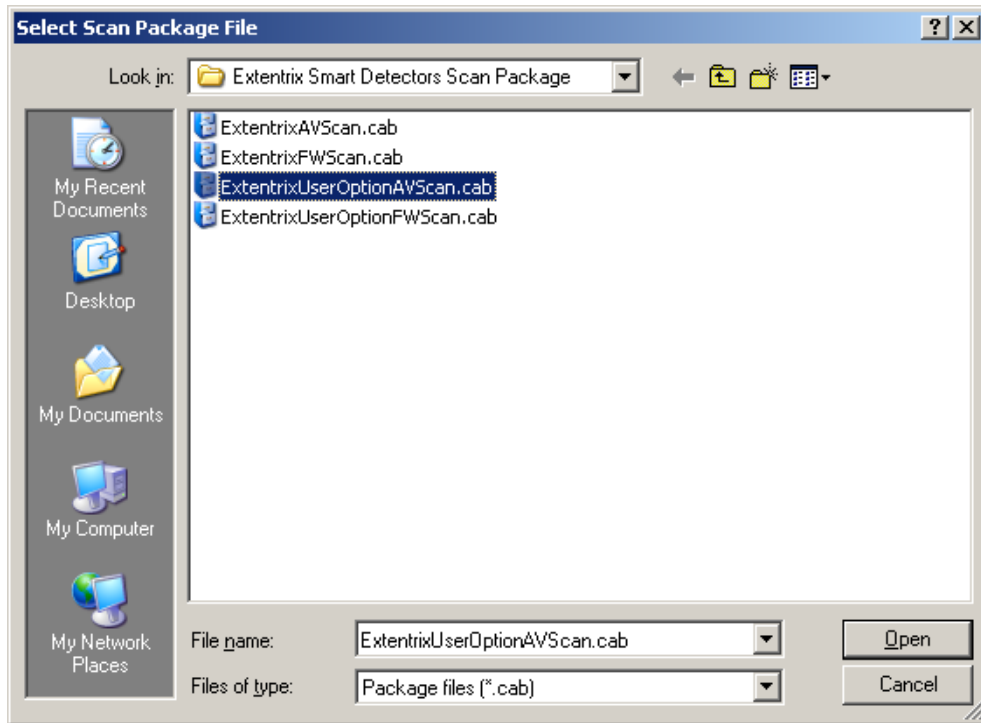
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



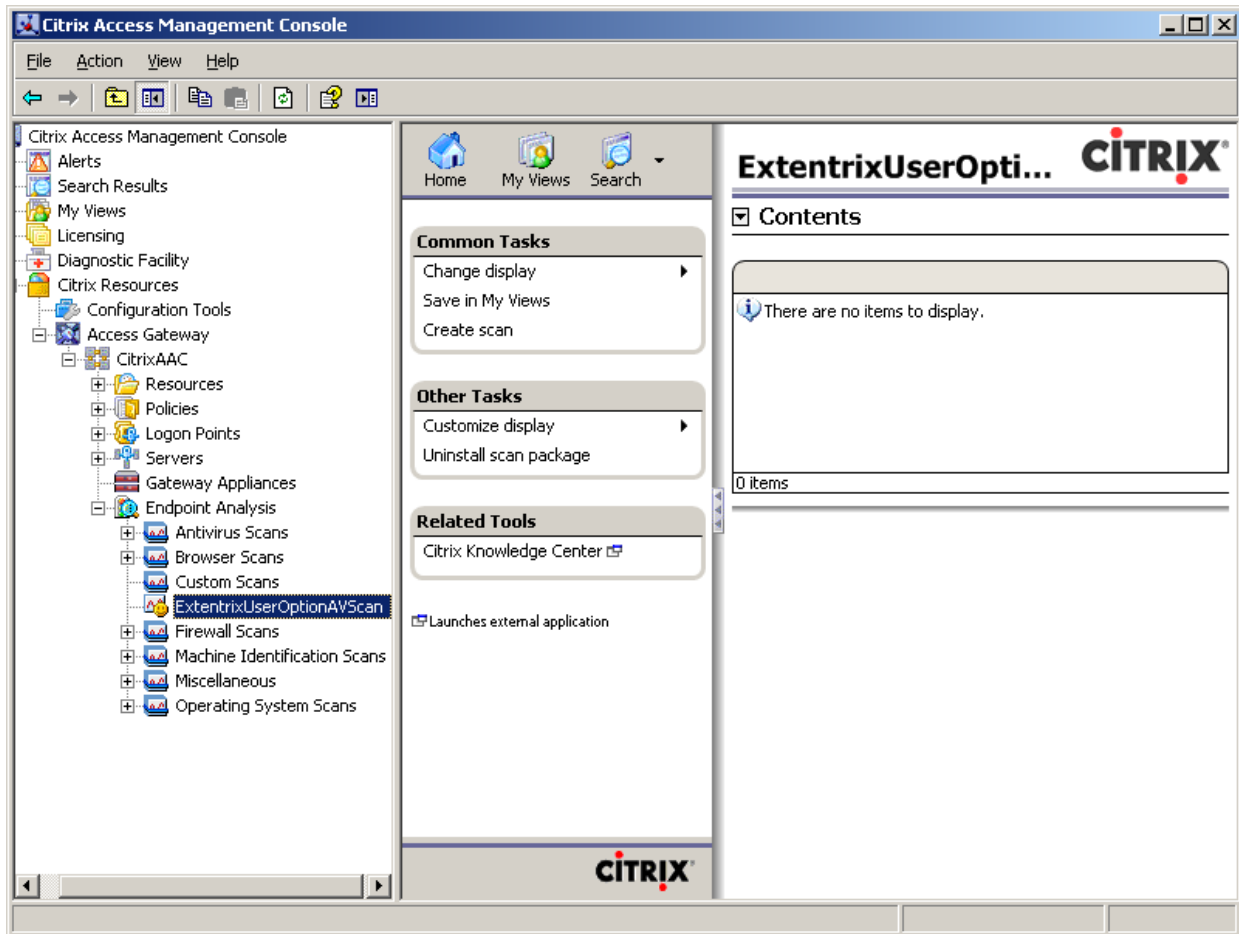
Also you can choose to insert the scan package to a specific scan package group as shown in the following picture:



3. A dialog box named **“Select Scan Package File”** will appear. Double click on the (.cab) file which contains the Scan.



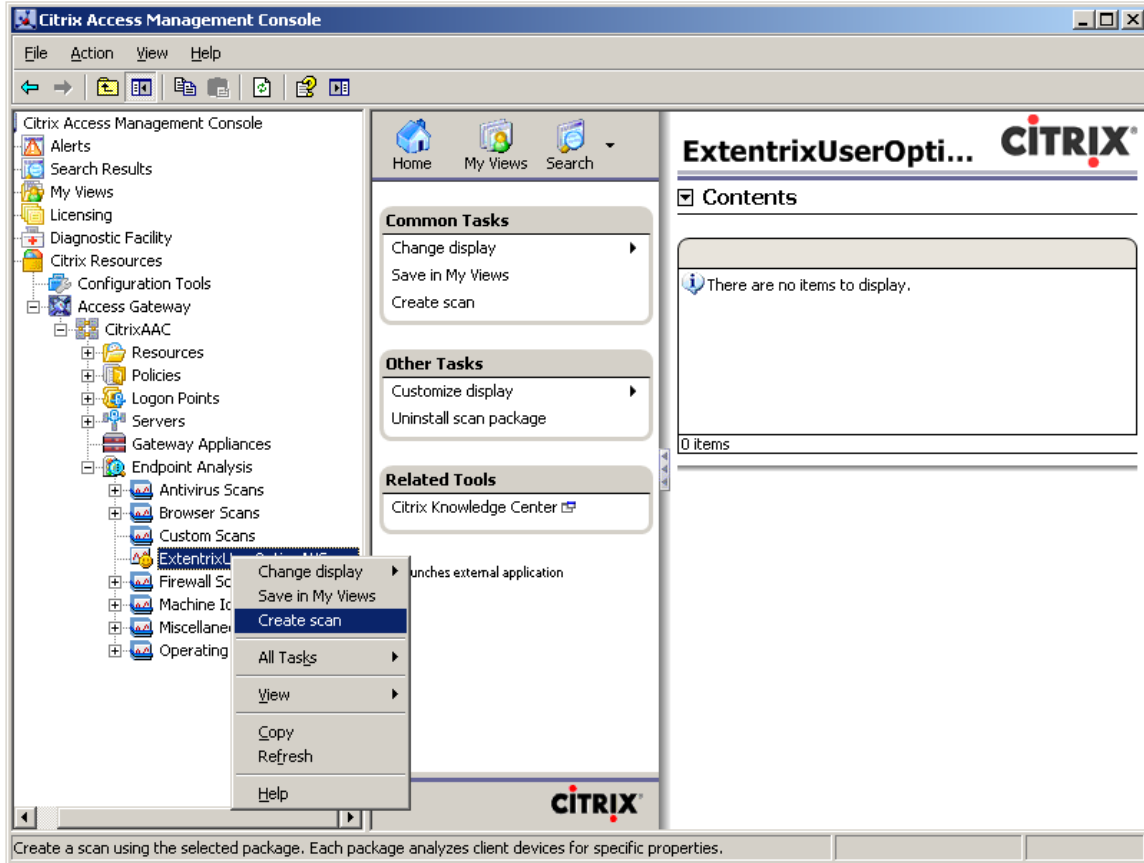
The package will be displayed in the console as shown in the following picture:



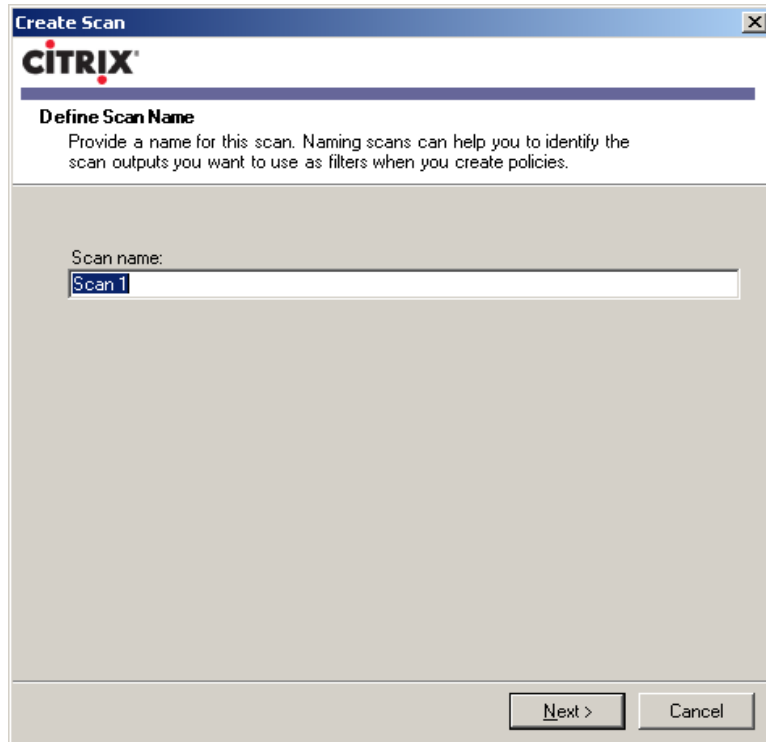
INSTALLING THE SCAN PACKAGE

Please follow the steps below to create scans and rules for the **Extentrix User Option AV Scan**.

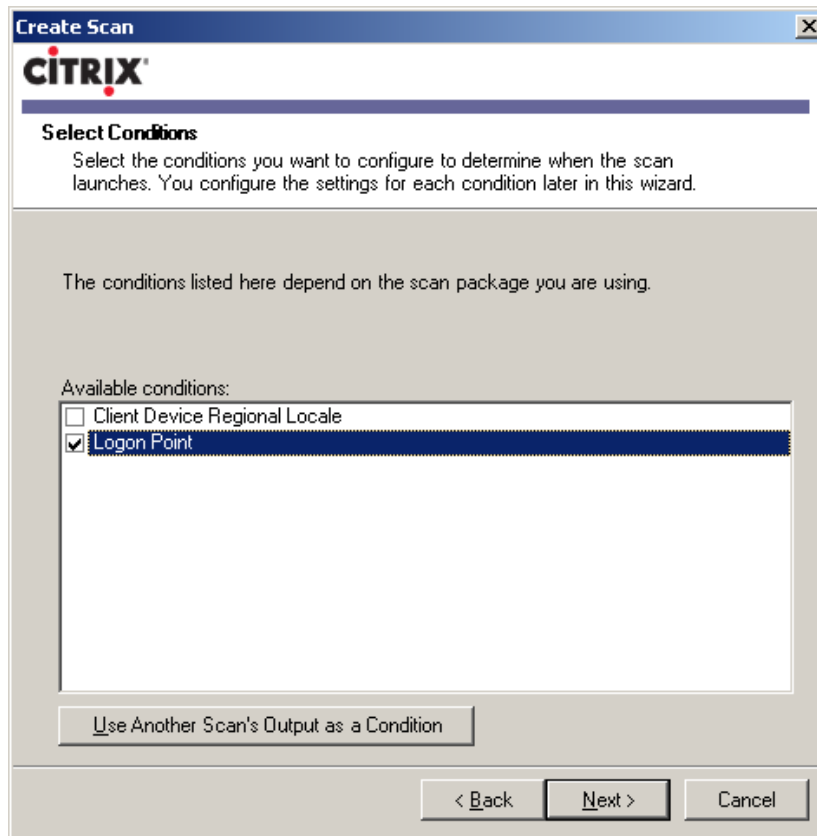
1. Select **ExtentrixUserOptionAVScan** to create scan for it, right click the icon and choose **Create Scan**.



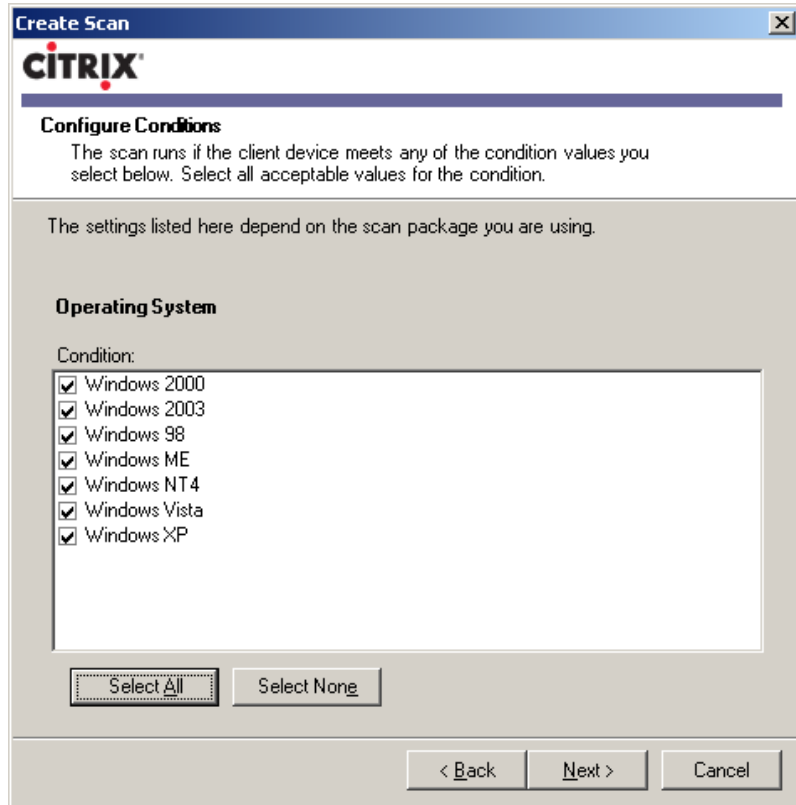
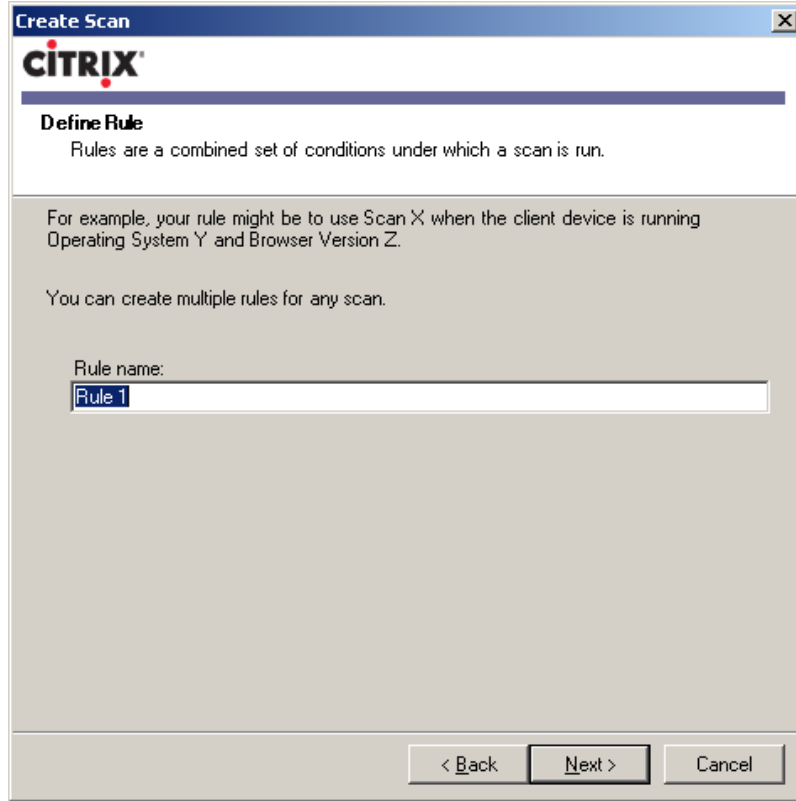
2. Type a name for the scan:

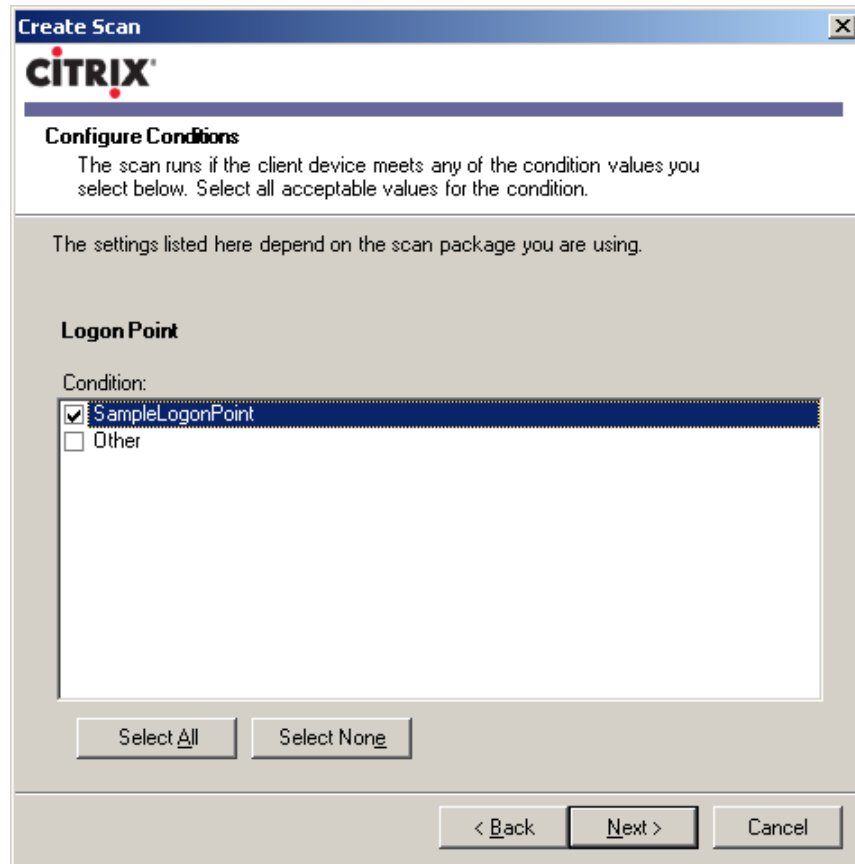


3. Set the scan conditions:

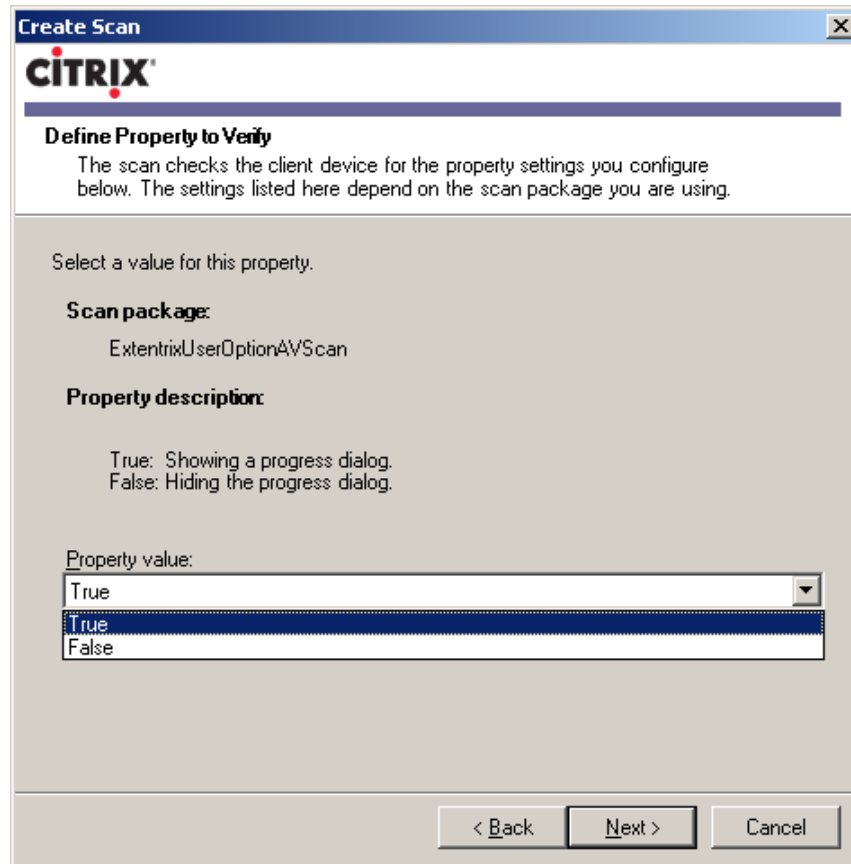


4. Type rule name and set rule conditions:

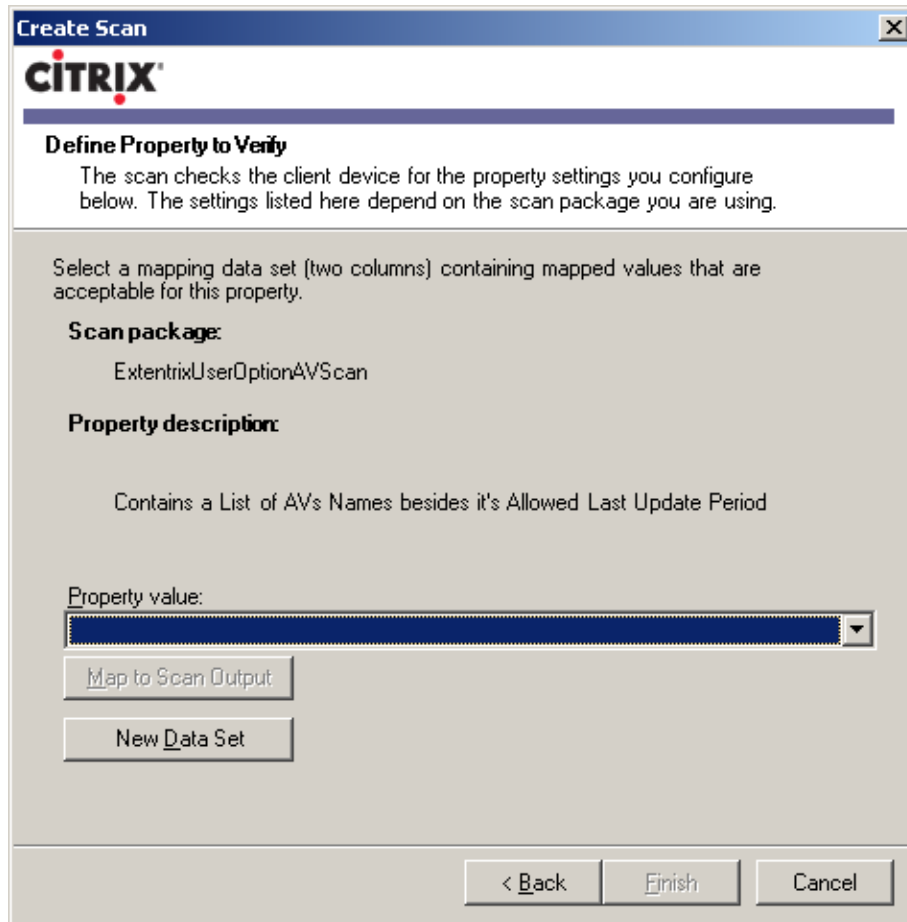




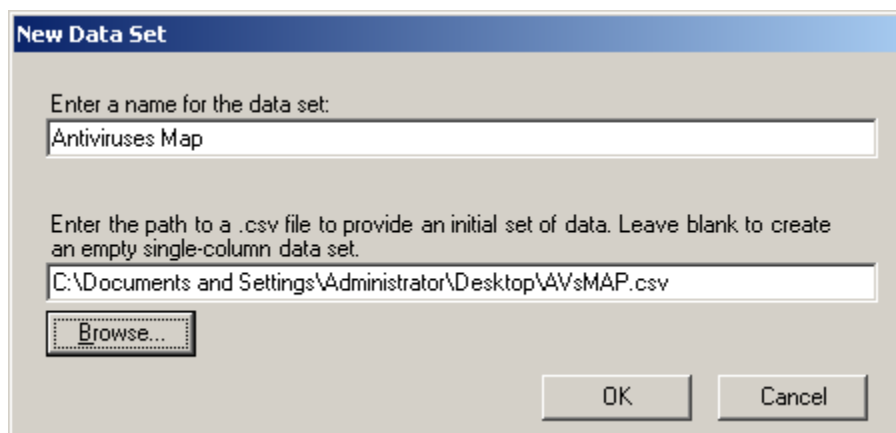
5. Type the name in **Property Value**.



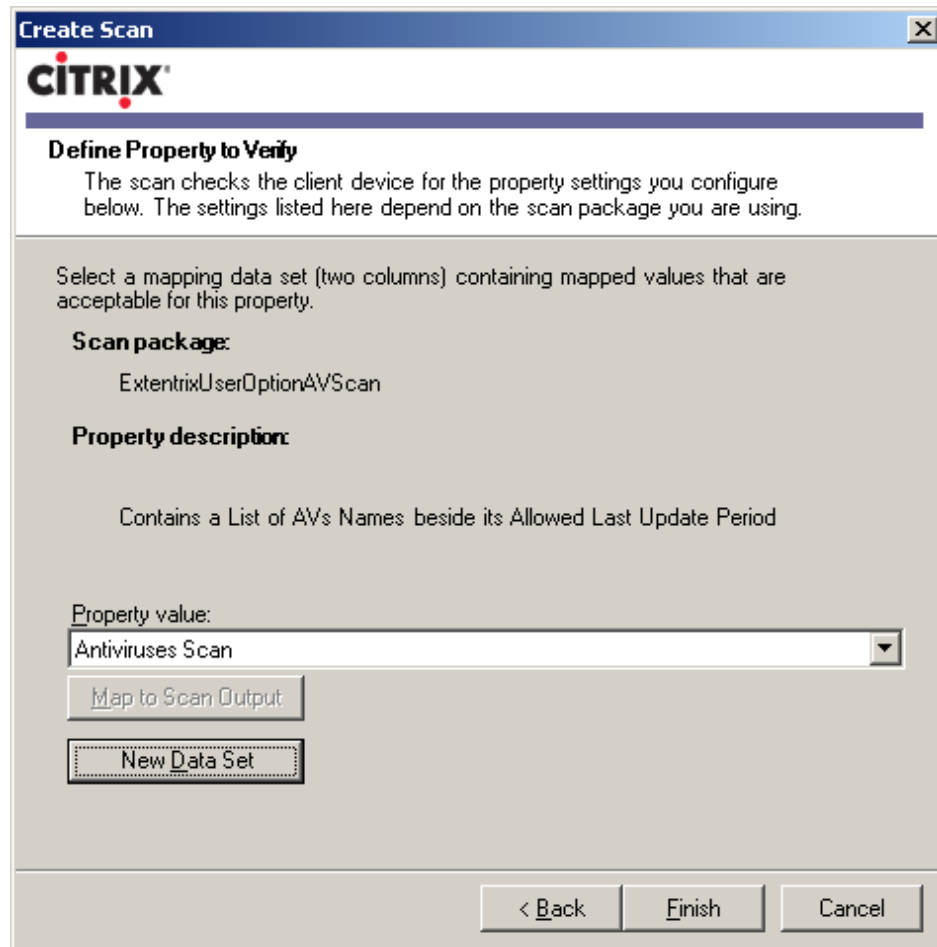
6. Define a data set (map) using a comma delimited .csv file. To do that, click on **New Data Set** to import the file. The file will have a list of Antivirus names and its desired time allowed.



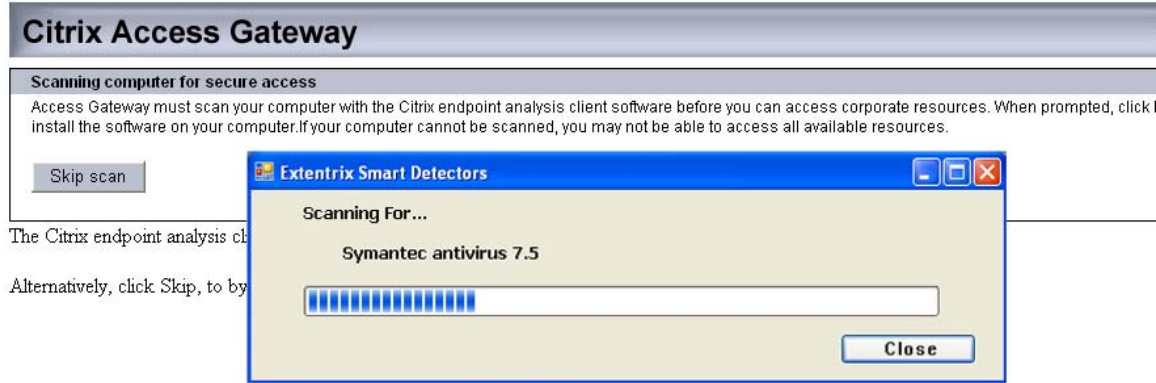
7. A dialog box named **“New Data Set”** will appear. Type a name for the new data set and use **Browse** to enter the path of the .csv file.



- When you are done, click **Finish**.

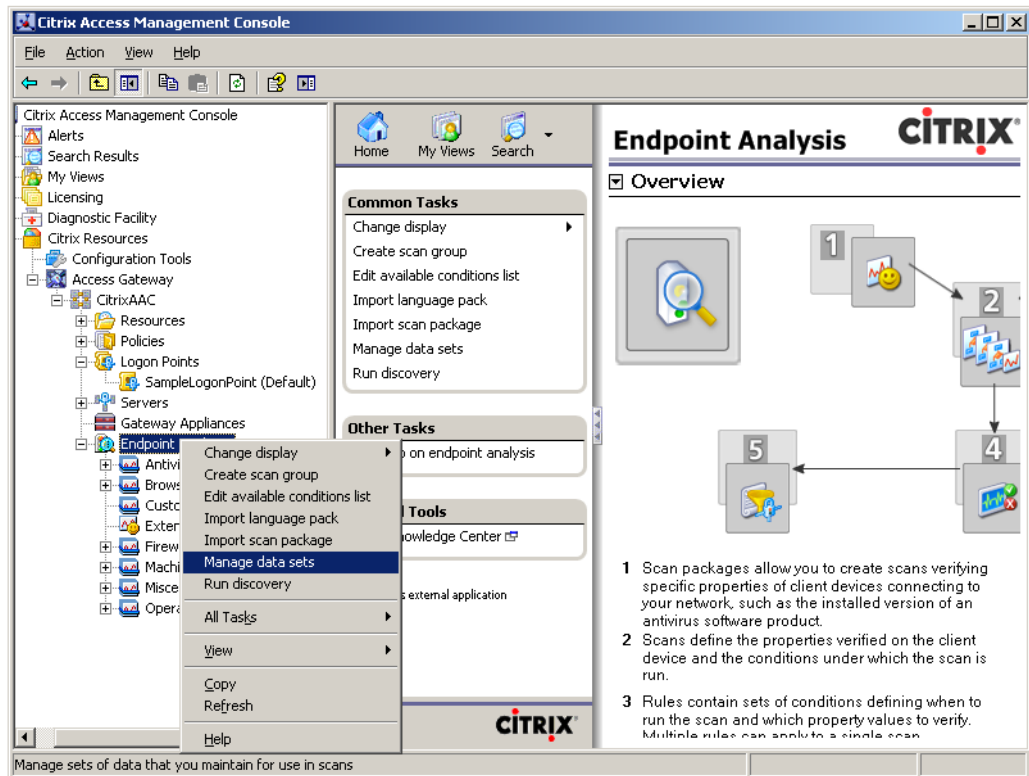


In the other side, when clients attempt to connect to the server that deploys this scan package, an active X control will be installed and it will perform the scanning operation. During this process, a progress bar will be shown to inform the clients about the scan progress as shown below:

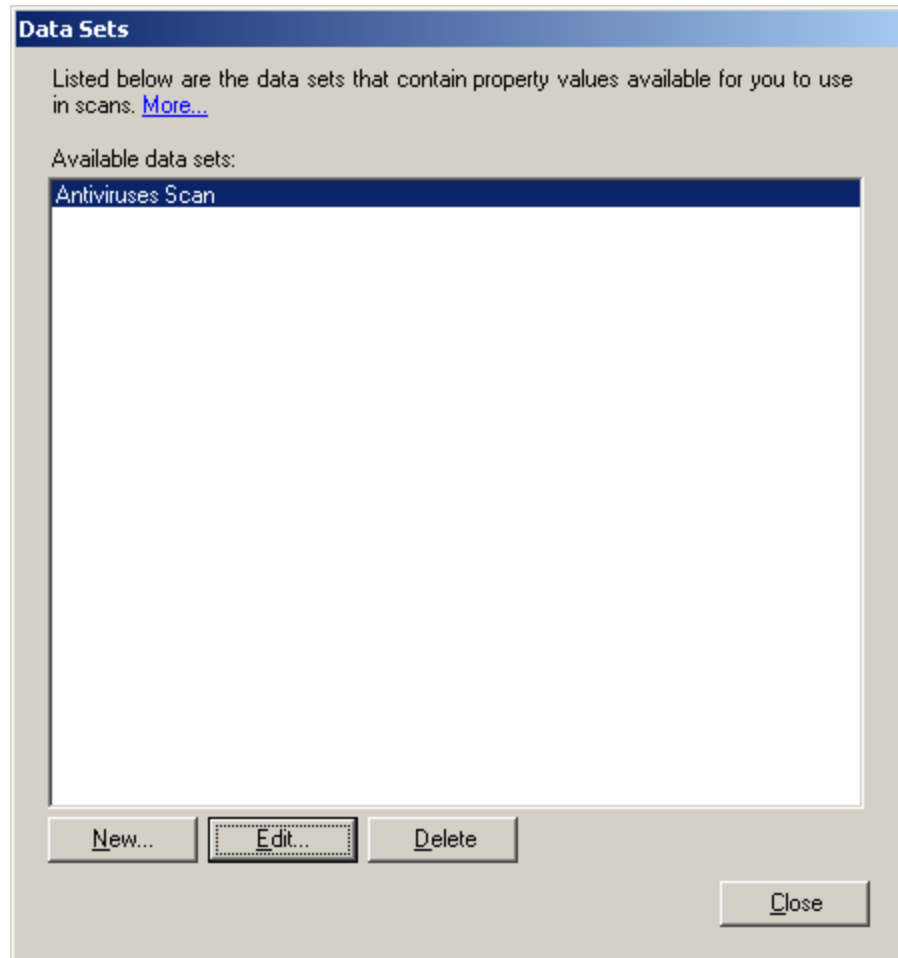


Note: You can edit the value later after you create the data set. To edit the data set:

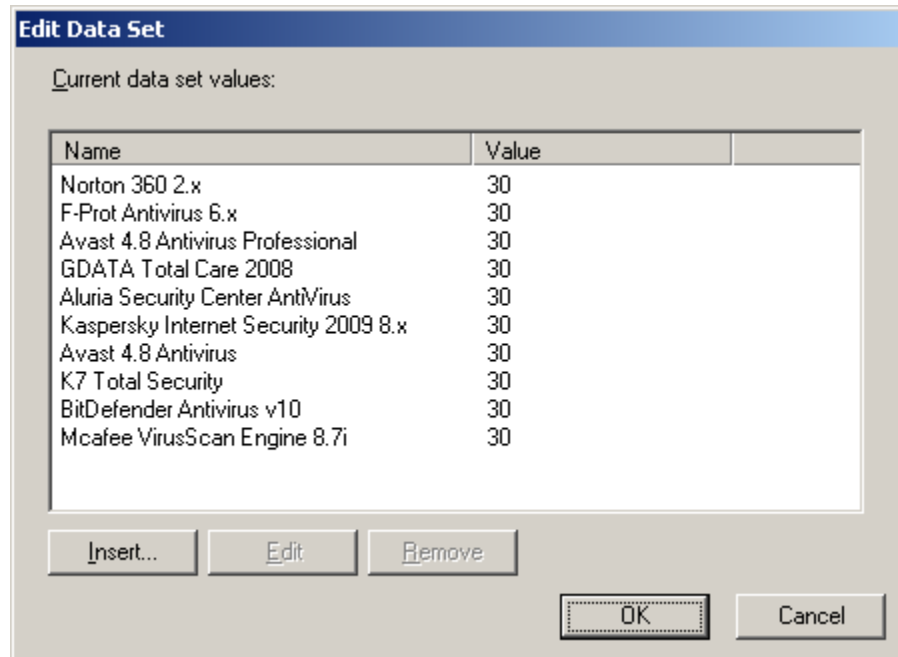
- Right click **Endpoint Analysis** in the console tree and select **Manage Data Set** from the action menu.



- A window named **“Data Sets”** will appear. Click the data set for which you want to make editing then click **Edit**.



- A window named **“Edit Data Set”** will appear.



- Make the editing you want (whether inserting new values, Editing or removing existing values). When you are done, click **OK**.

4. EXTENTRIX USER OPTION FW SCAN

SCAN DESCRIPTION

Scan Name: Extentrix User Option FW Scan.

Description: This scan will check each firewalls defined in Extentrix firewalls supported list, if it exists in the client machine and running. It makes sure of:

- Existence of the Firewall.
- Status of the Firewall Enable/Disable.

Parameters:

- Show/Hide Dialog – a Boolean value which allows administrators to show (true) or hide (false) the progress dialog to the client while scanning his/her machine. To see how the progress bar looks like, refer to page 44.
- FW Map – a double-columned data set, each one of its records has a Firewall name and status pair. Firewall name is a string value as named on <http://www.extentrix.com/EPA/AVsFWs.htm> and the status is a string value True for enable and False for disable.

Scan Output:

- Allow Access - a Boolean output which indicates whether the type is matched or not.

TRUE – indicates that the client’s machine has at least one of Extentrix Firewall supported list installed and/or enabled.

FALSE – indicates that the client’s machine doesn’t have any of Extentrix Firewalls supported list or is not enabled.
- License Status- a String output which indicates whether the scan is licensed or not.

TRIAL LICENSE – indicates that the scan has a trial license.

INVALID LICENSE – indicates that the scan hasn’t a license.

VALID LICENSE – indicates that the scan is licensed.

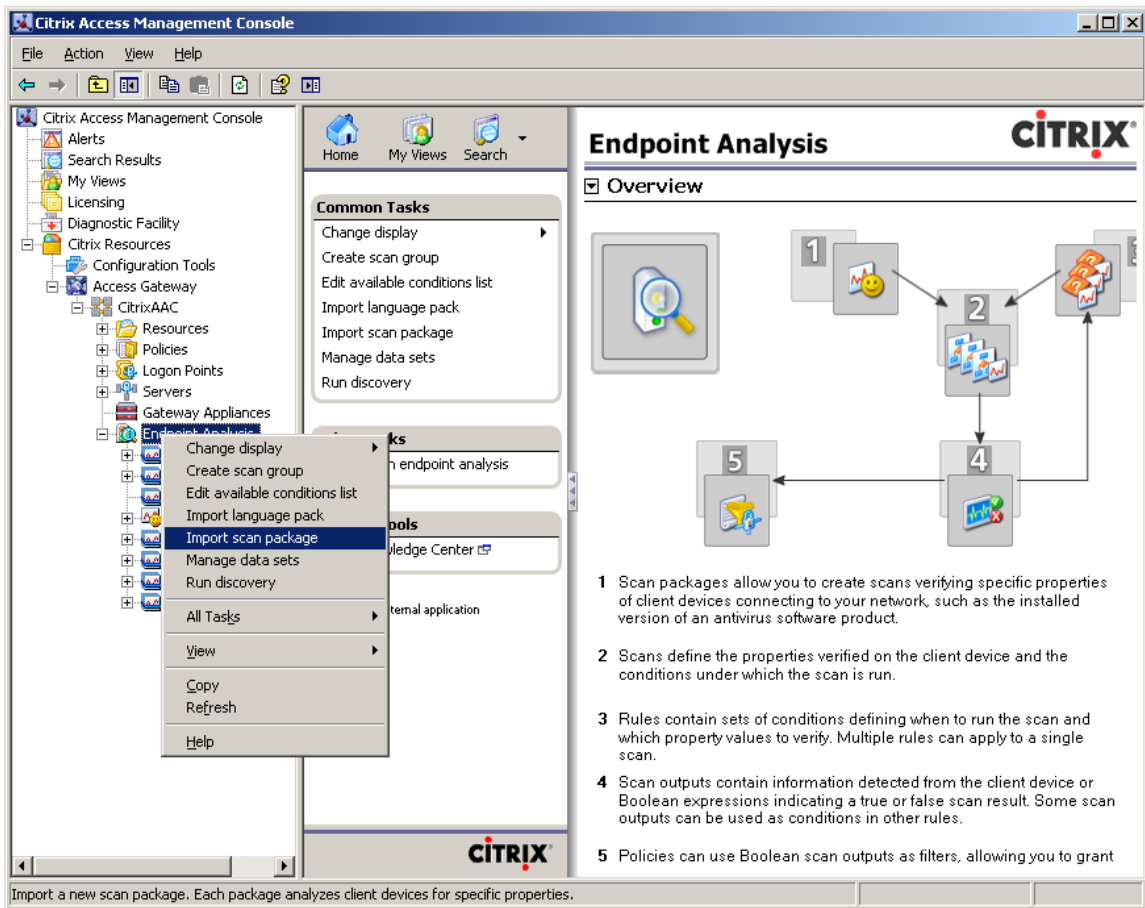
Note: If the License Status has an Invalid License value, the Allow Access will be false.

INSTALLATION AND CONFIGURATION

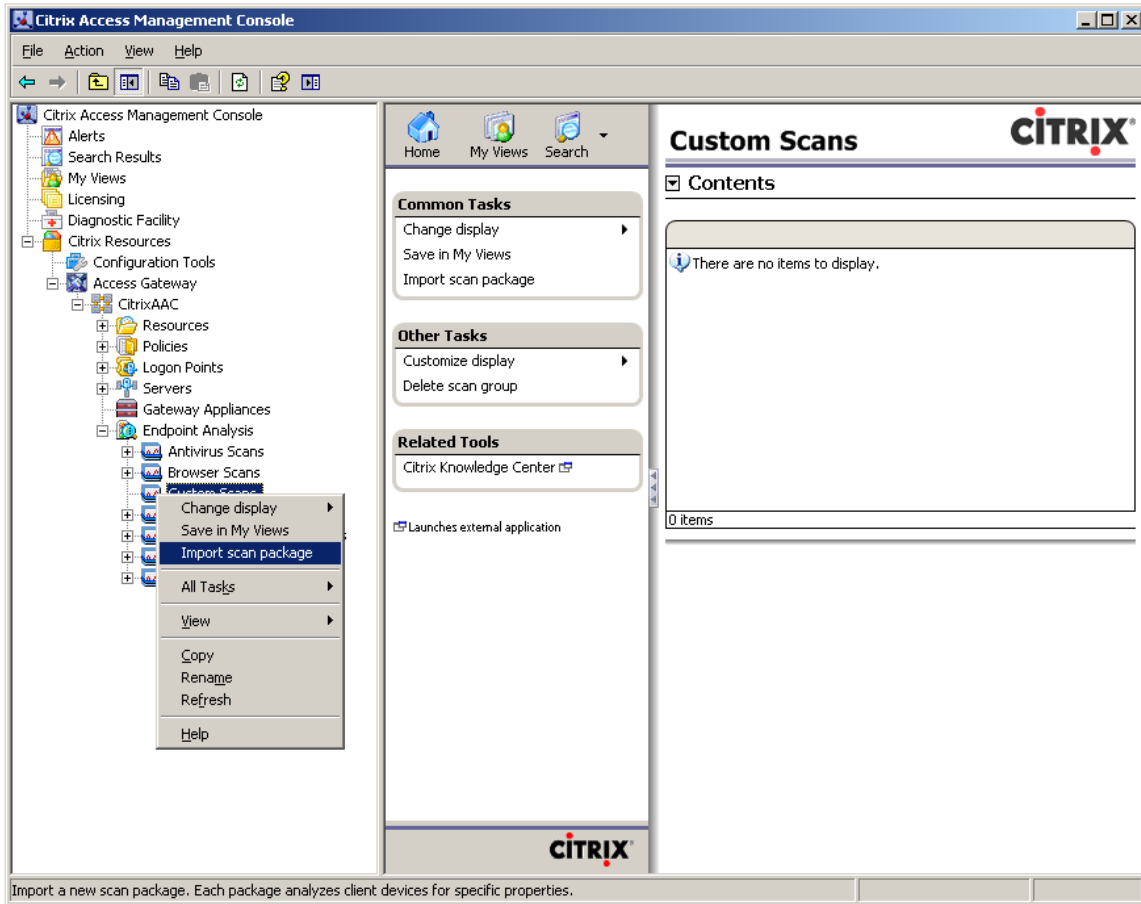
IMPORTING SCAN PACKAGES

To install a custom end point analysis scan package follow the following steps:

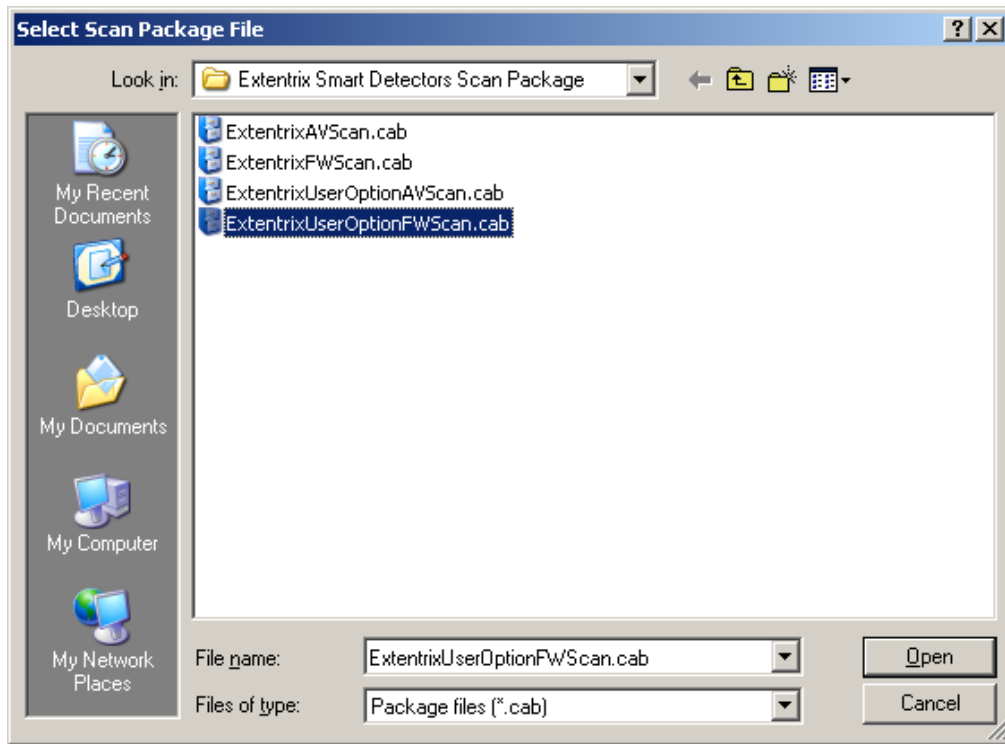
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



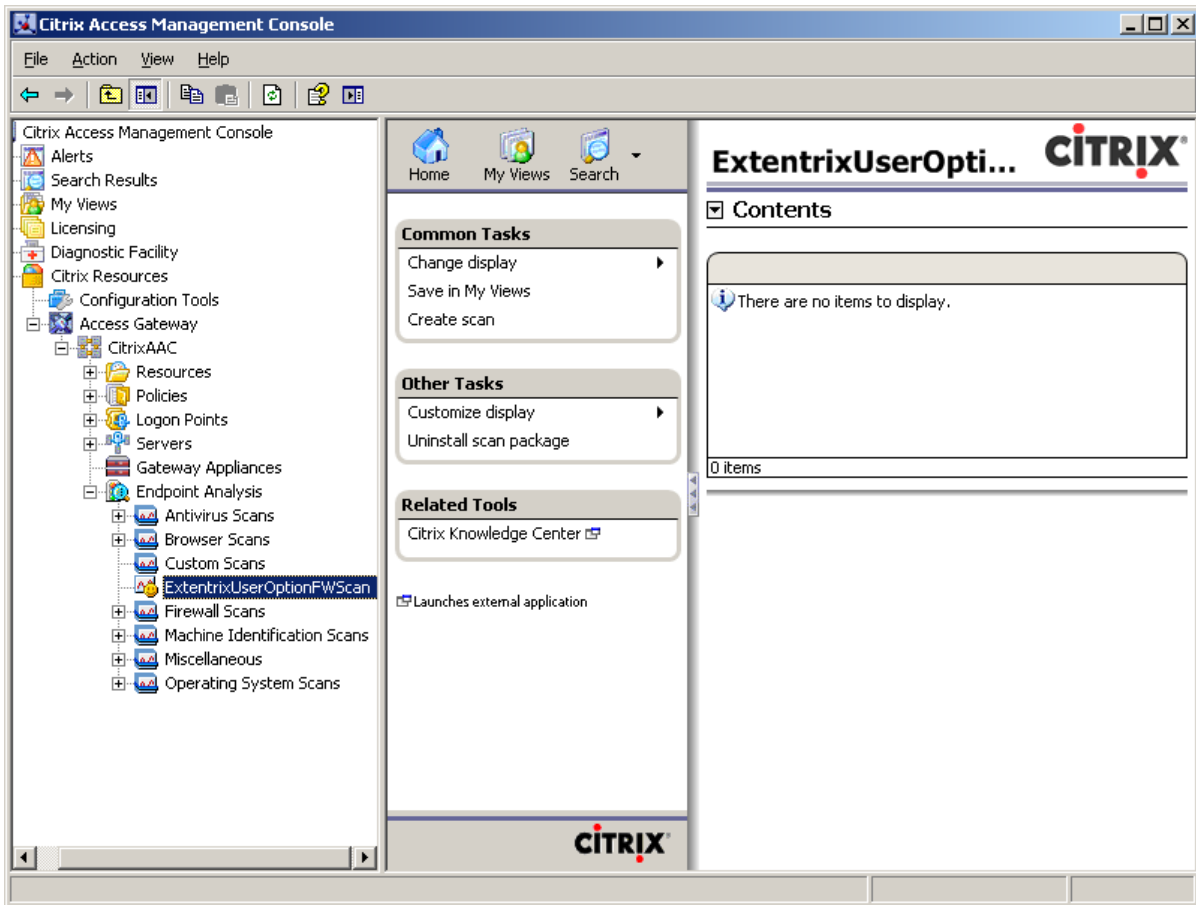
Also you can choose to insert the scan package to any scan category listed in the tree as shown in the following picture:



3. A dialog box named **“Select Scan Package File”** will appear. Double click on the (.cab) file which contains the Scan.



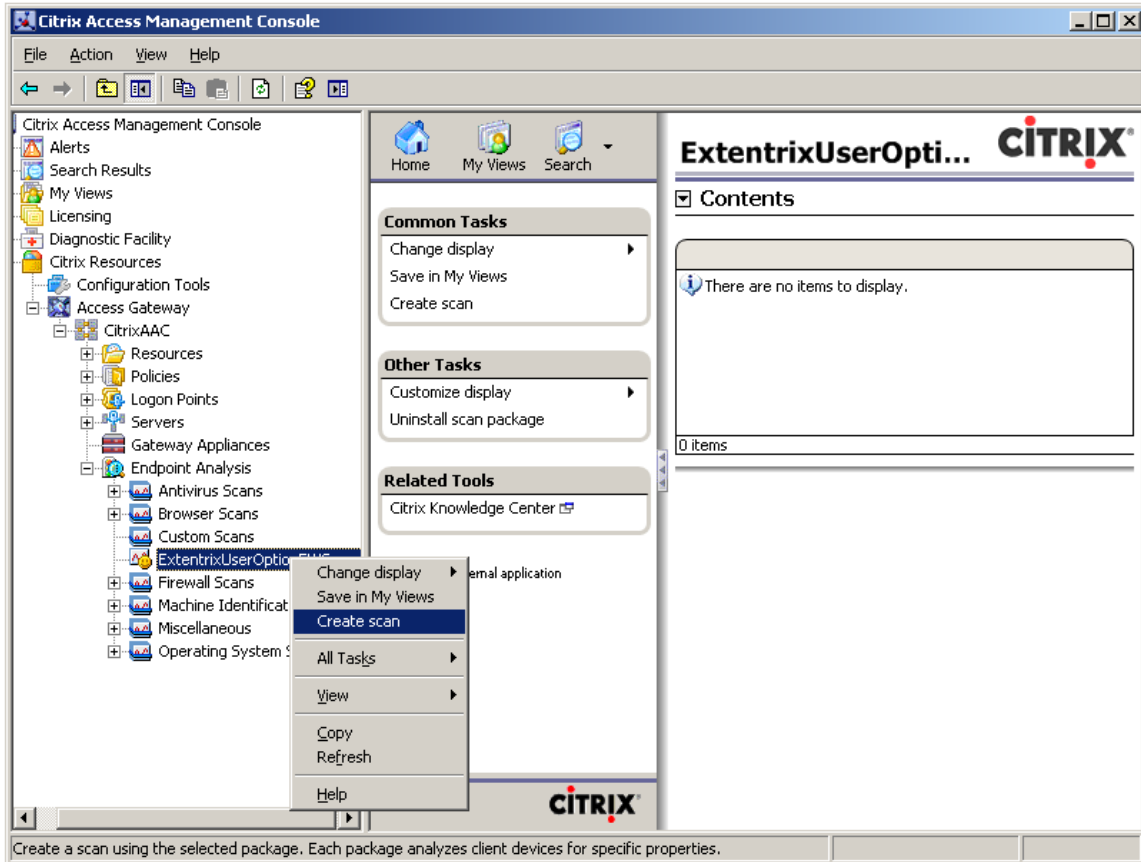
The package will be displayed in the console as shown in the following picture:



INSTALLING THE SCAN PACKAGE

Please follow the steps below to create scans and rules for the **Extentrix User Option FW Scan**.

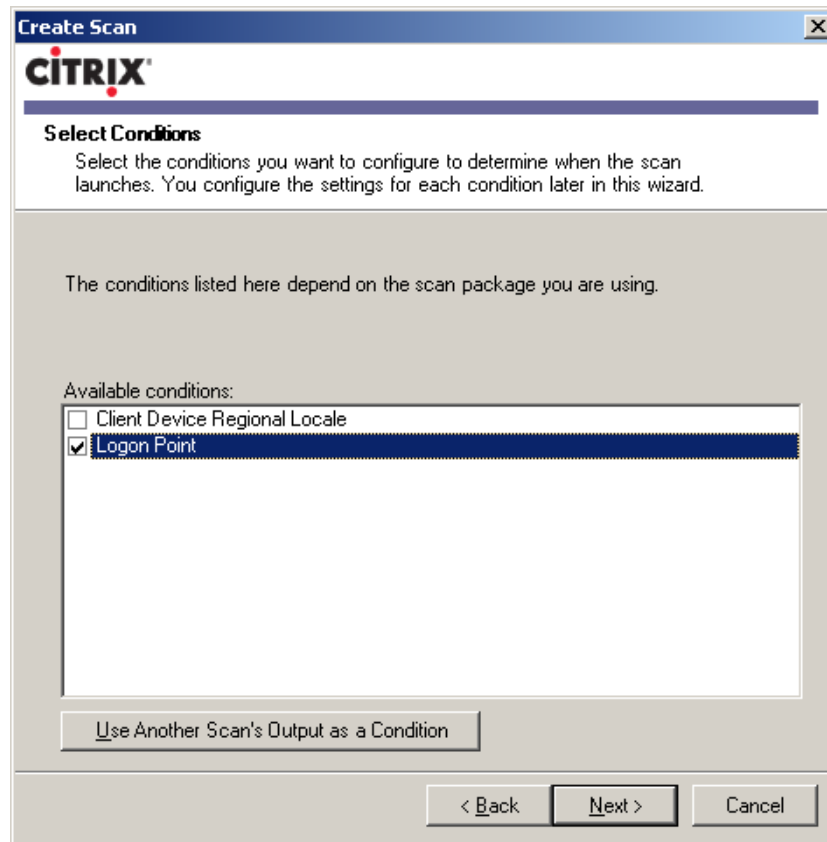
1. Select **ExtentrixUserOptionFWScan** to create scan for it, right click the icon and choose **Create Scan**.



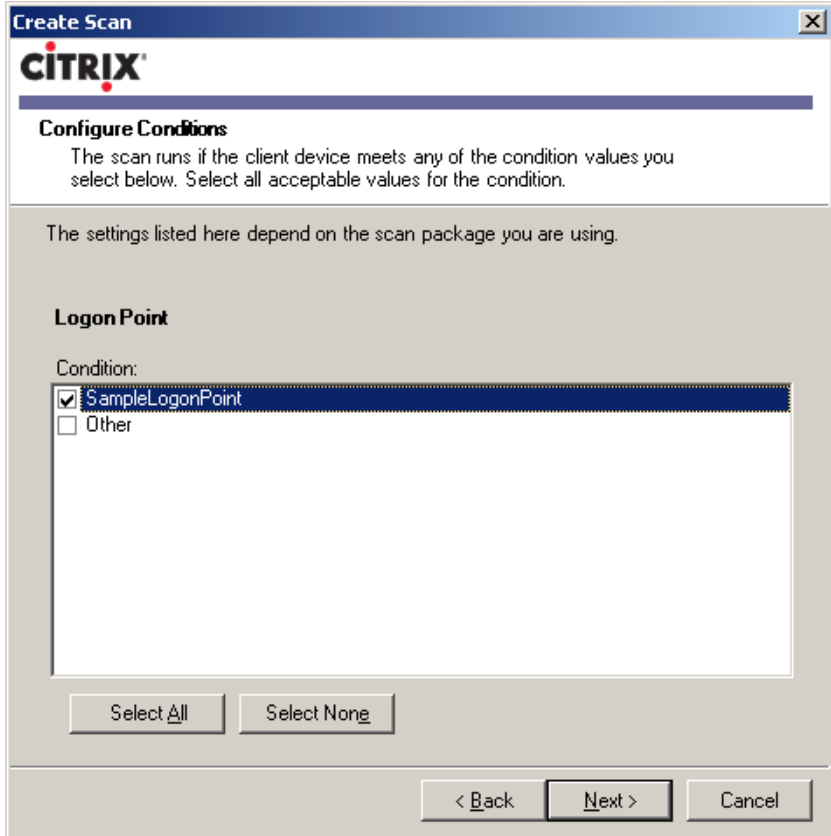
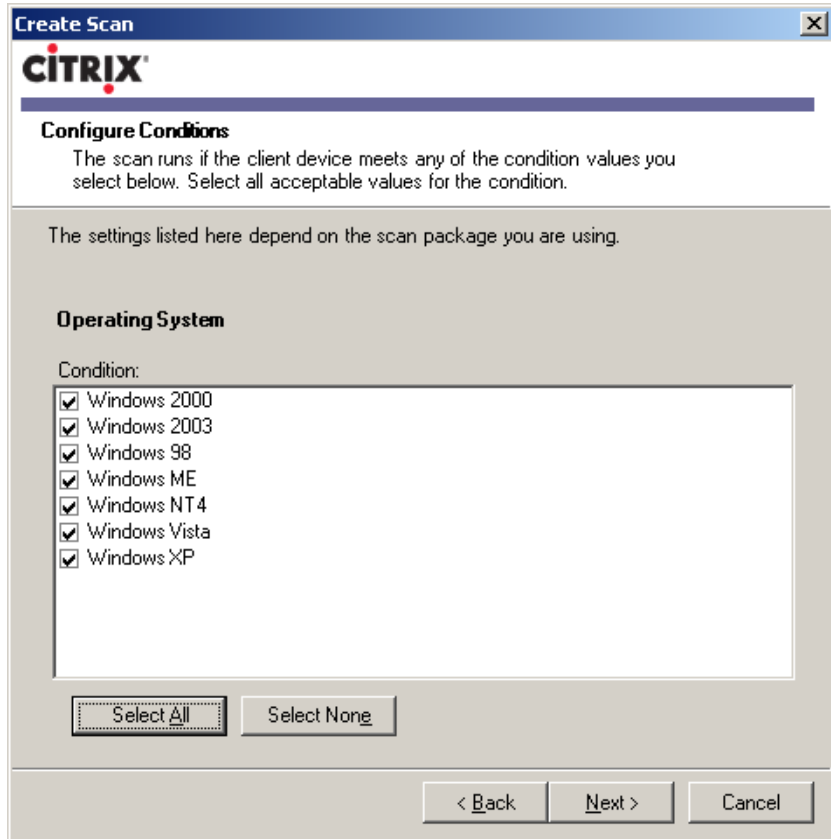
2. Type a name for the scan:



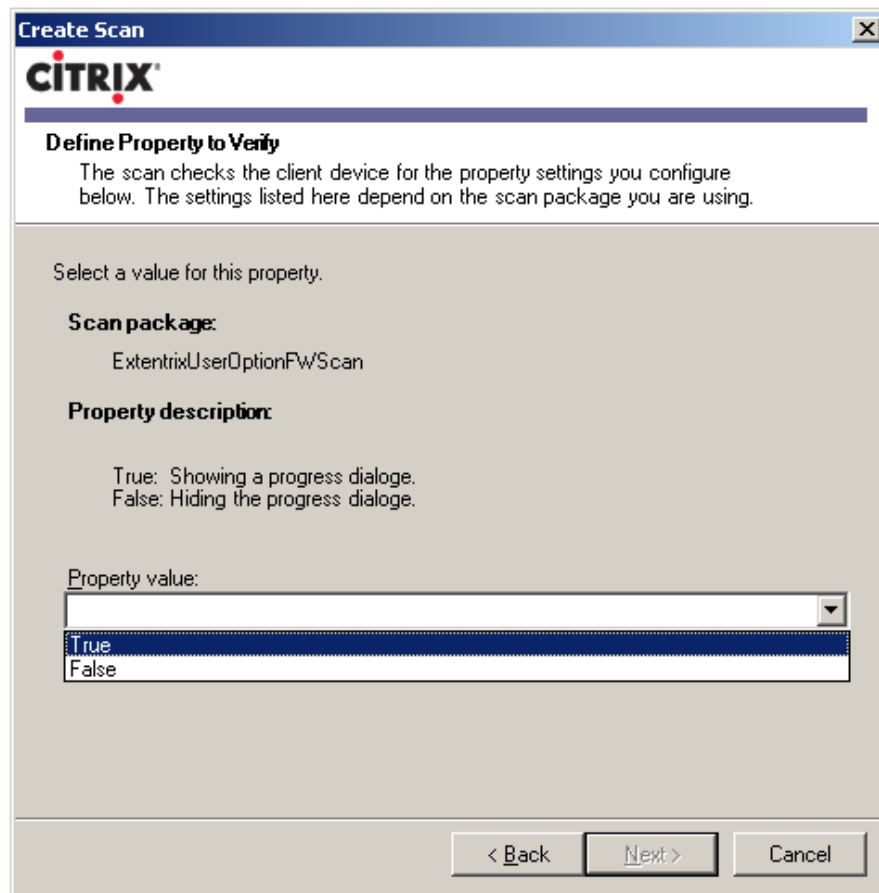
3. Set the scan conditions:



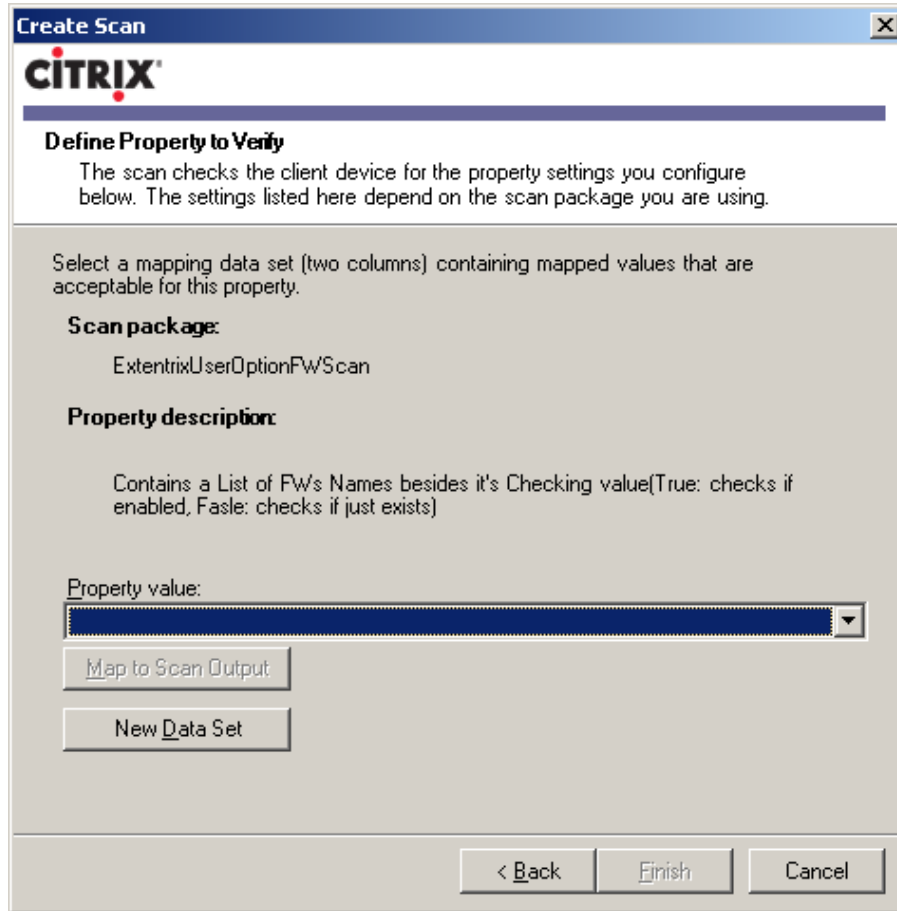
4. Type rule name and set rule conditions:



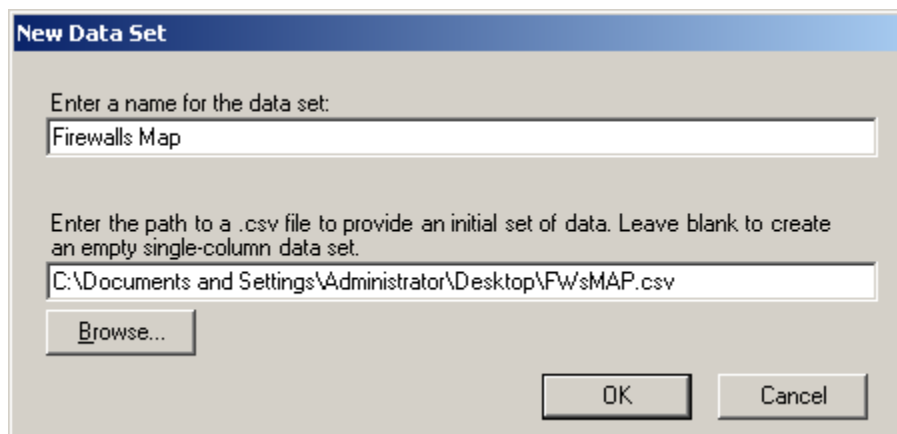
5. Type the name in **Property Value**.



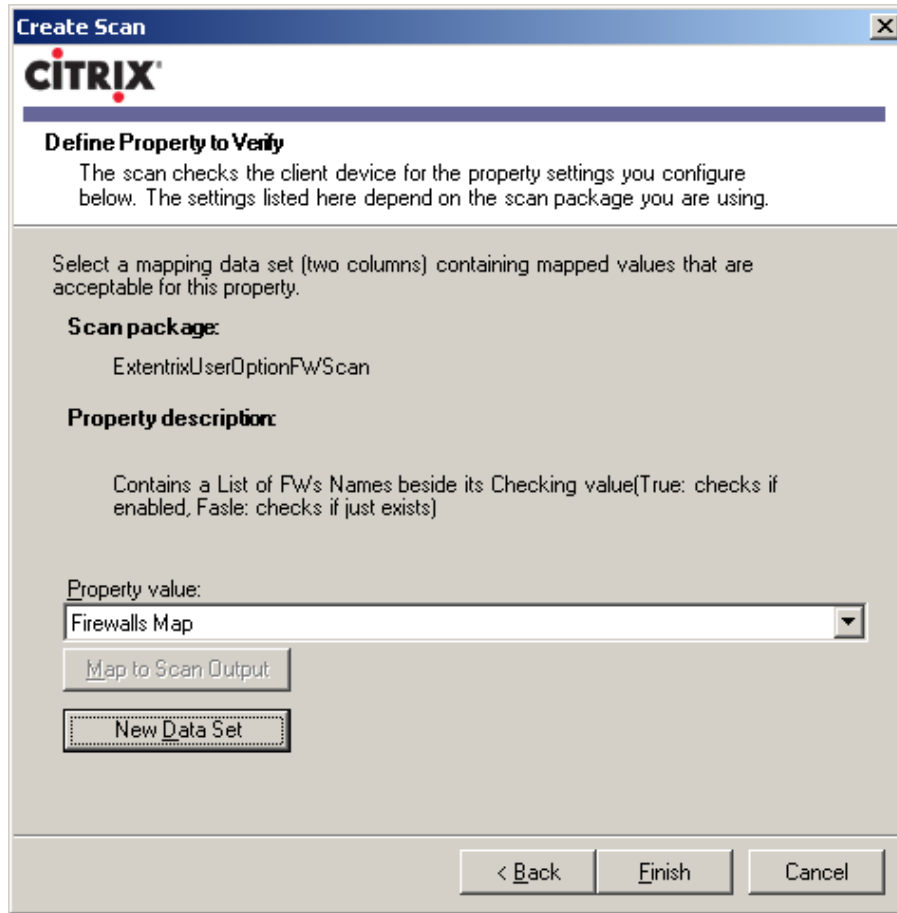
6. Define a data set (map) using a comma delimited .csv file. To do that, click on **New Data Set** to import the file. The file will have a list of Firewalls names and its desired time allowed.



7. A dialog box named **“New Data Set”** will appear. Type a name for the new data set and use **Browse** to enter the path of the .csv file.



- When you are done, click **Finish**.

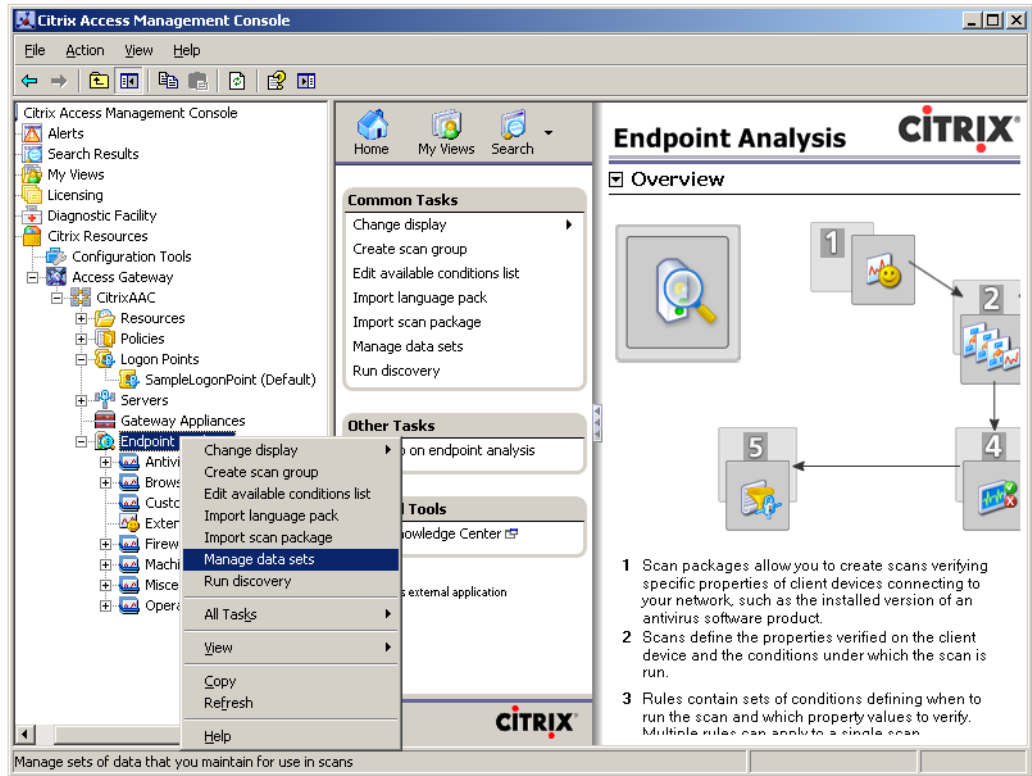


In the other side, when clients attempt to connect to the server that deploys this scan package, an active X control will be installed and it will perform the scanning operation. During this process, a progress bar will be shown to inform the clients about the scan progress as shown below:

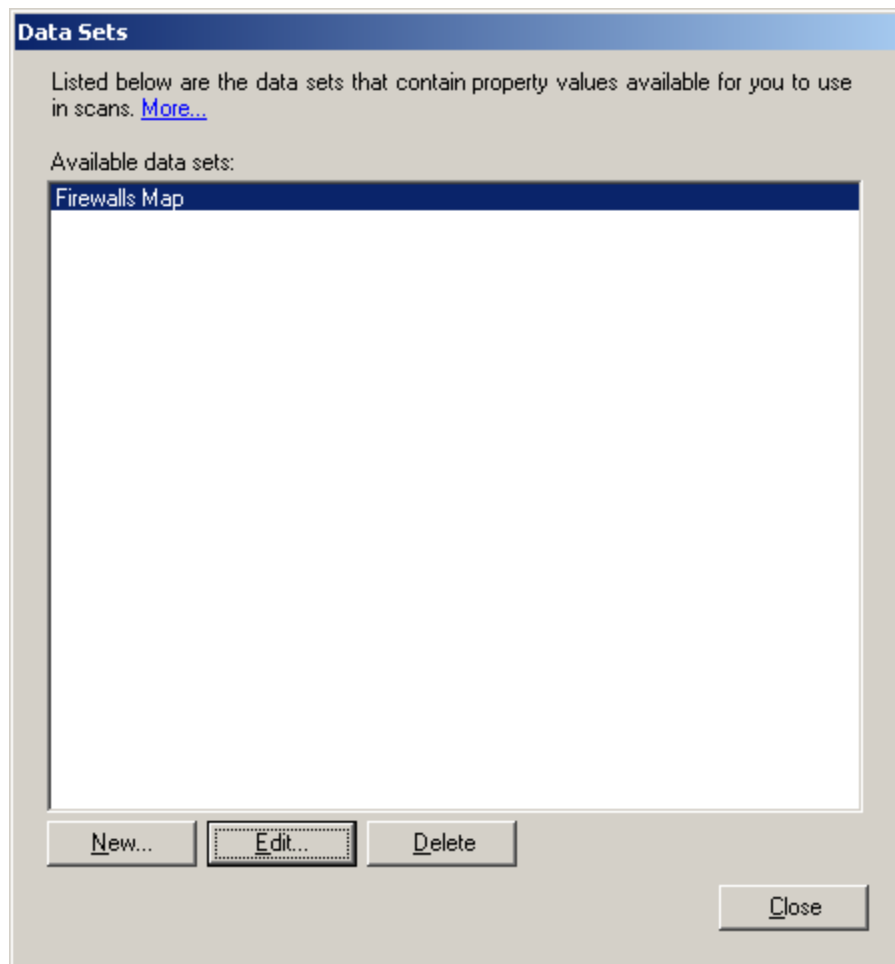


Note: You can edit the value later after you create the data set. To edit the data set:

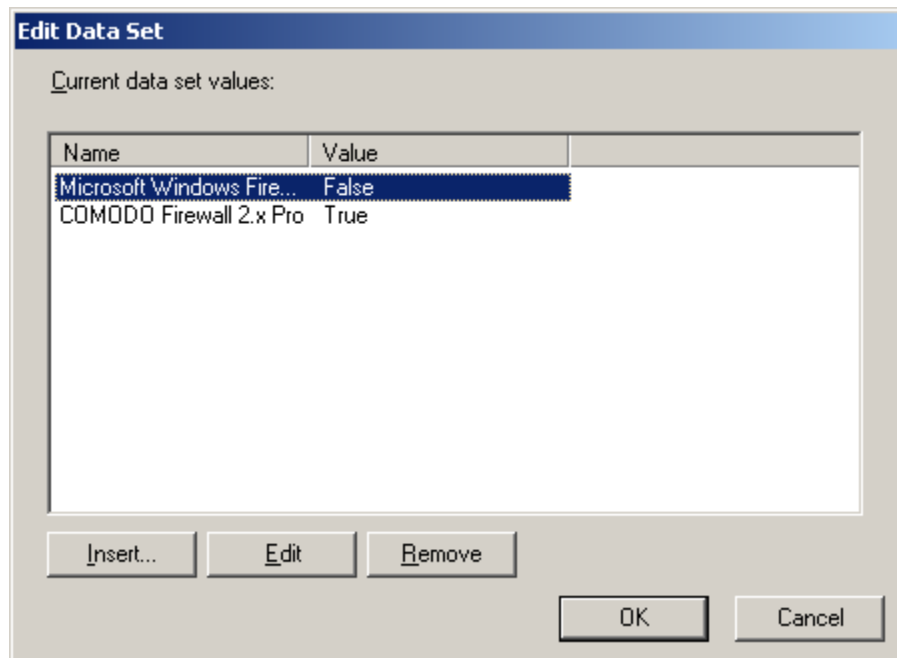
- Right click **Endpoint Analysis** in the console tree and select **Manage Data Set** from the action menu.



- A window named **“Data Sets”** will appear. Click the data set for which you want to make editing then click **Edit**.



- A window named **“Edit Data Set”** will appear.



- Make the editing you want (whether inserting new values, Editing or removing existing values). When you are done, click **OK**.

5. EXTENTRIX ANTI SPYWARE SCAN

SCAN DESCRIPTION

Scan Name: Extentrix AS Scan.

Description: It allows the administrator to check if the client machine has Antispyware installed and supported by Extentrix Anti spyware list and ensure that the installed antispyware is running and up to date.

Parameters:

- Show/Hide Dialog – a Boolean value which allows administrators to show (true) or hide (false) the progress dialog to the client while scanning his/her machine
- Time Allowed – an integer value which presents the numbers of days that will be allowed since last update time.

Scan Output:

- Allow Access - a Boolean output which indicates whether the client has an antispyware with allowed update period, enable and run /or not.
 - TRUE – indicates that the client has one of Extentrix supported Anti spyware installed, enable and running.
 - FALSE – indicates that the client doesn't have one of Extentrix supported Anti spyware installed, enable and running.
- License Status- a String output which indicates whether the scan is licensed or not.
 - TRIAL LICENSE – indicates that the scan has a trial license.
 - INVALID LICENSE – indicates that the scan hasn't a license.
 - VALID LICENSE – indicates that the scan is licensed.

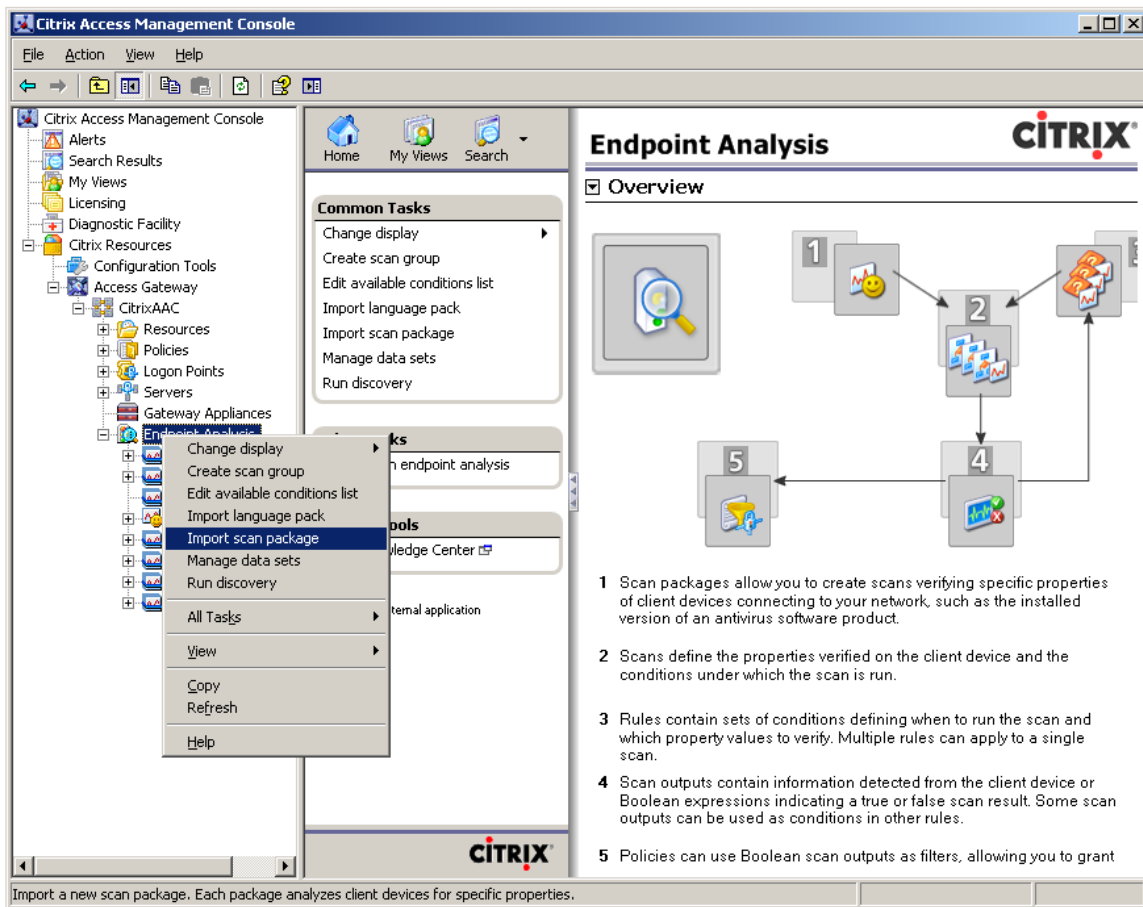
Note: If the License Status has an Invalid License value, the Allow Access will be false.

INSTALLATION AND CONFIGURATION

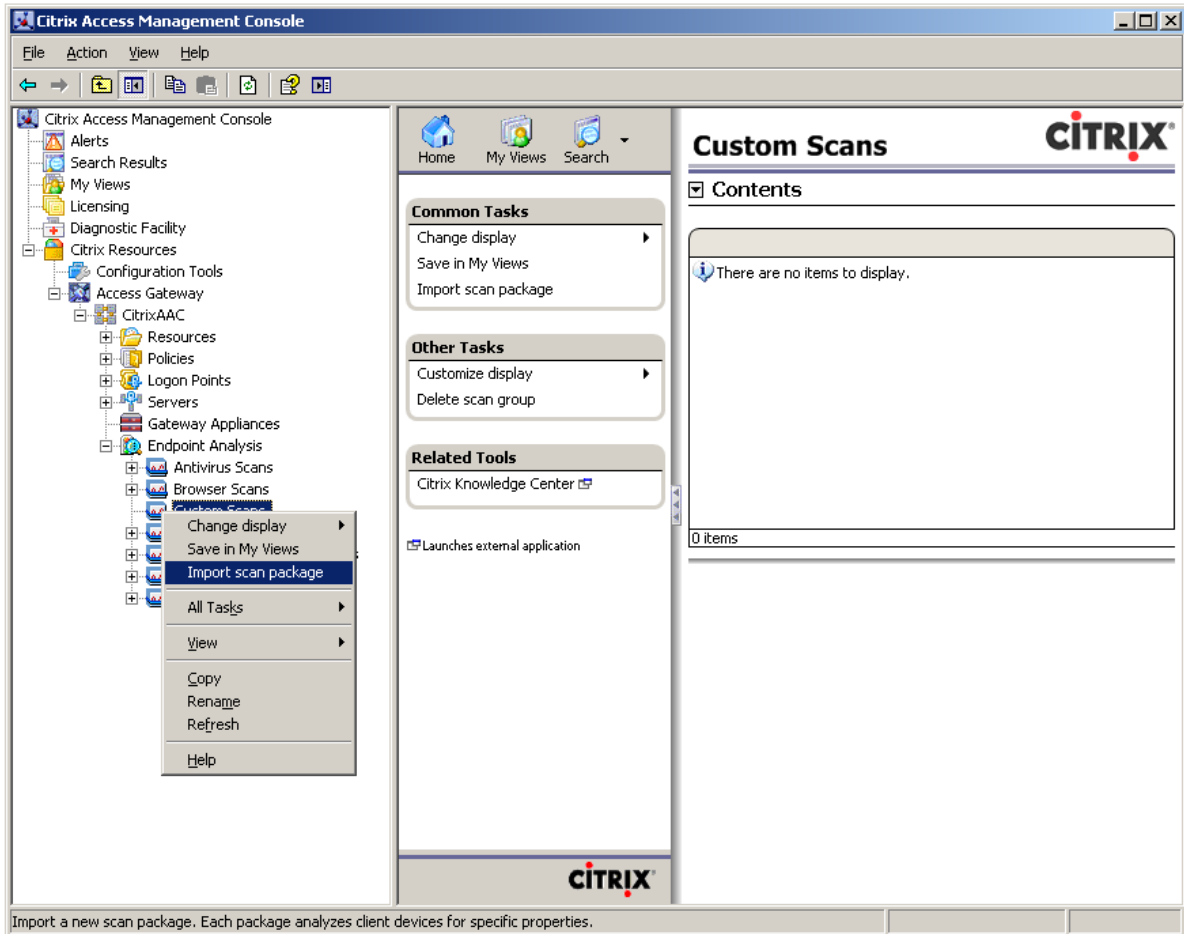
IMPORTING SCAN PACKAGES

To install a custom end point analysis scan package follow the following steps:

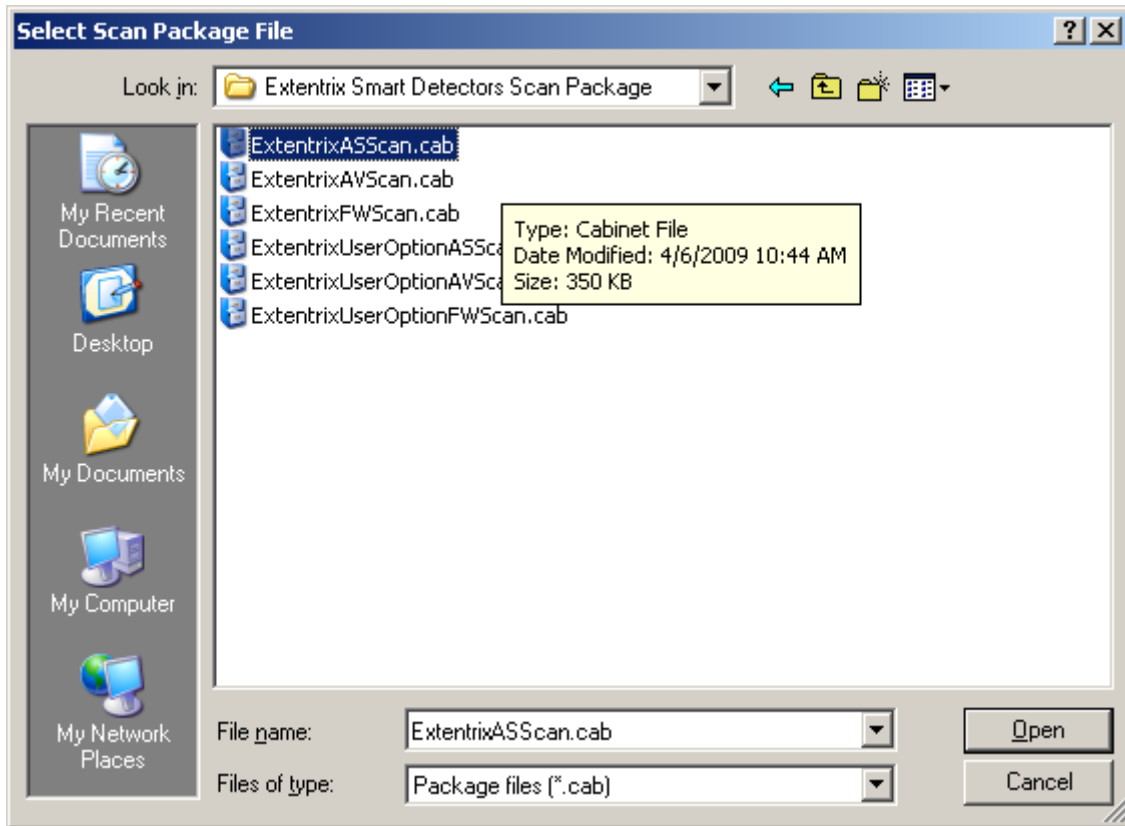
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



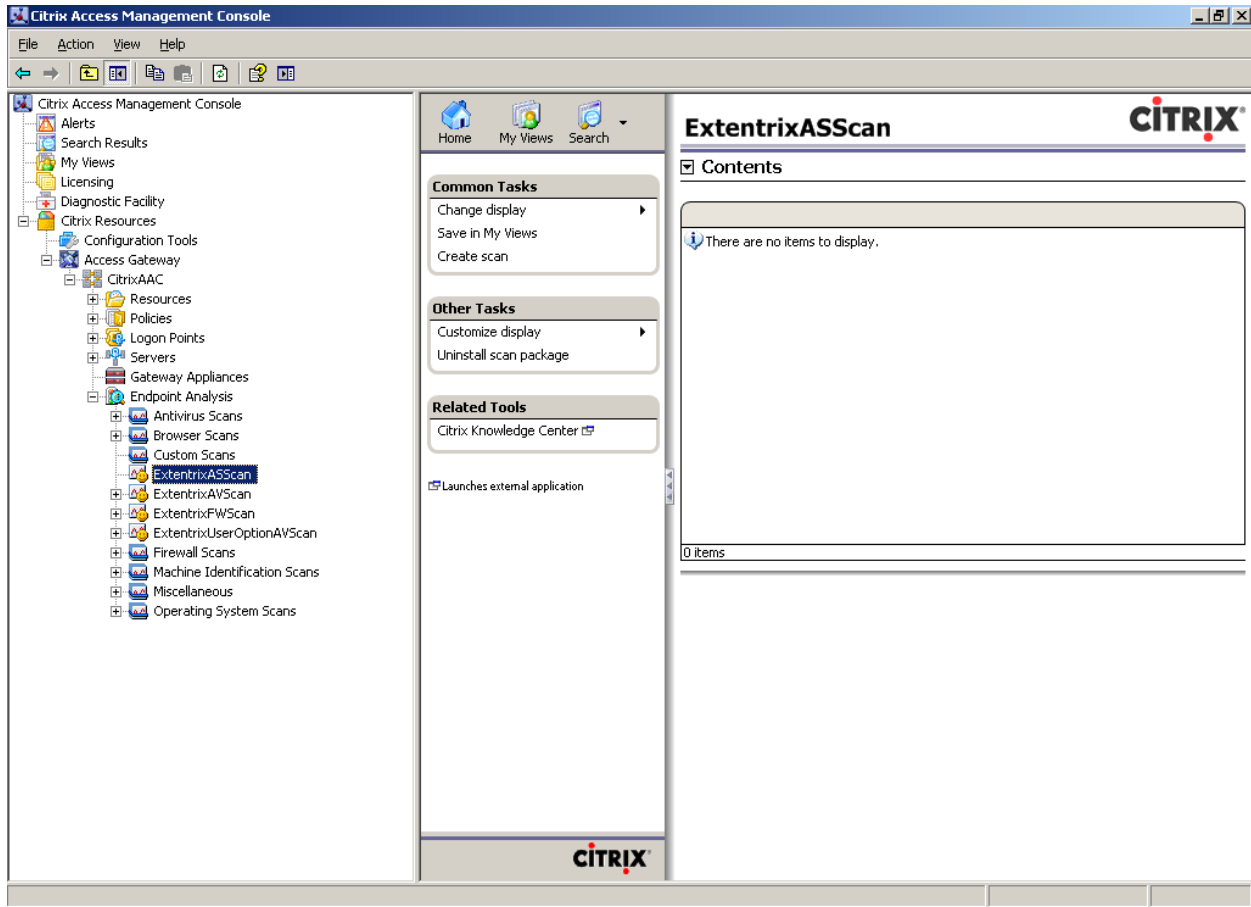
Also you can choose to insert the scan package to a specific scan package group as shown in the following picture:



3. A dialog box named **“Select Scan Package File”** will appear. Double click on the (.cab) file which contains the Scan.



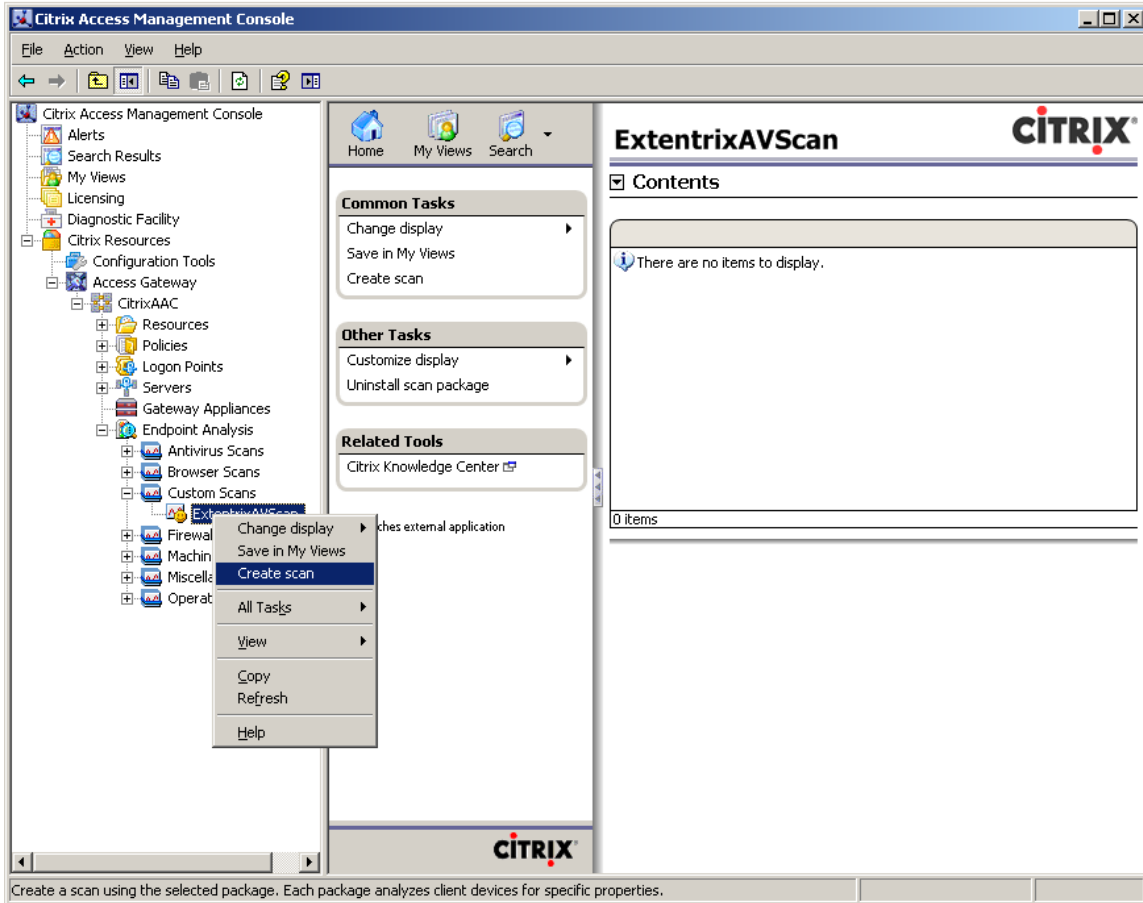
The package will be displayed in the console as shown in the following picture:



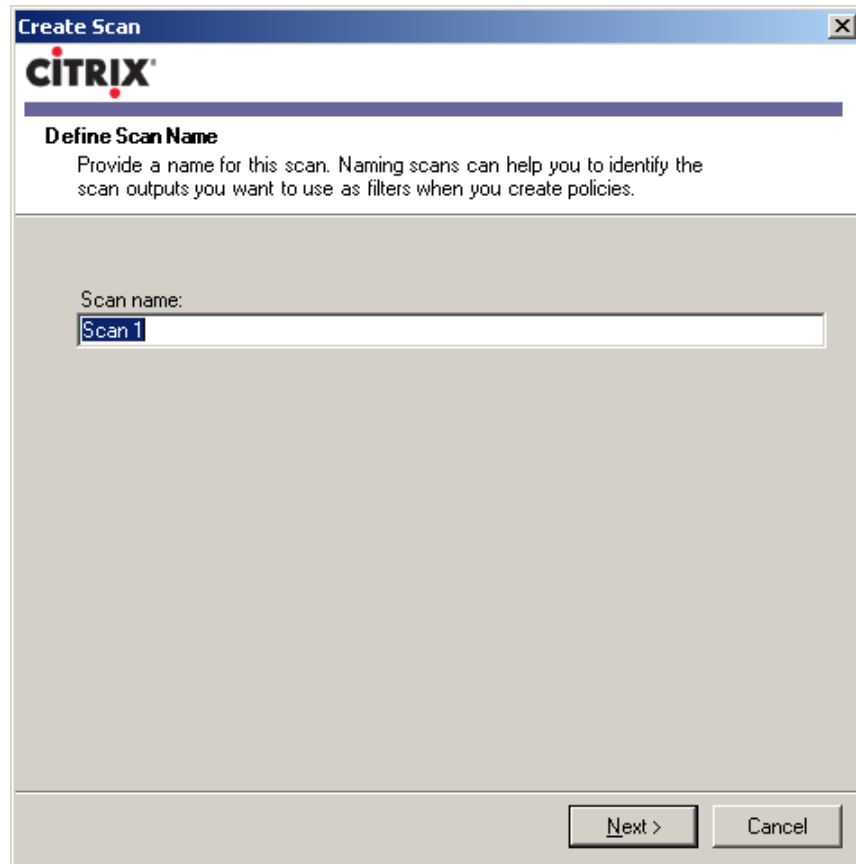
INSTALLING THE SCAN PACKAGE

Please follow the steps below to create scans and rules for the **Extentrix AS Scan**.

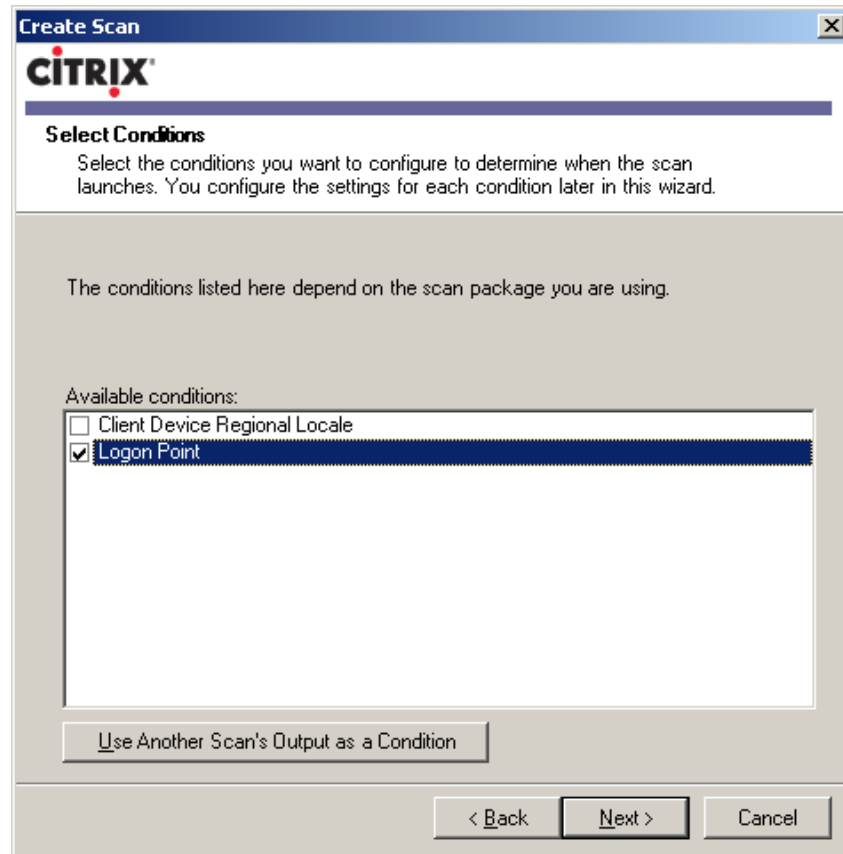
1. Select **ExtentrixASScan** to create scan for it, right click the icon and choose **Create Scan**.



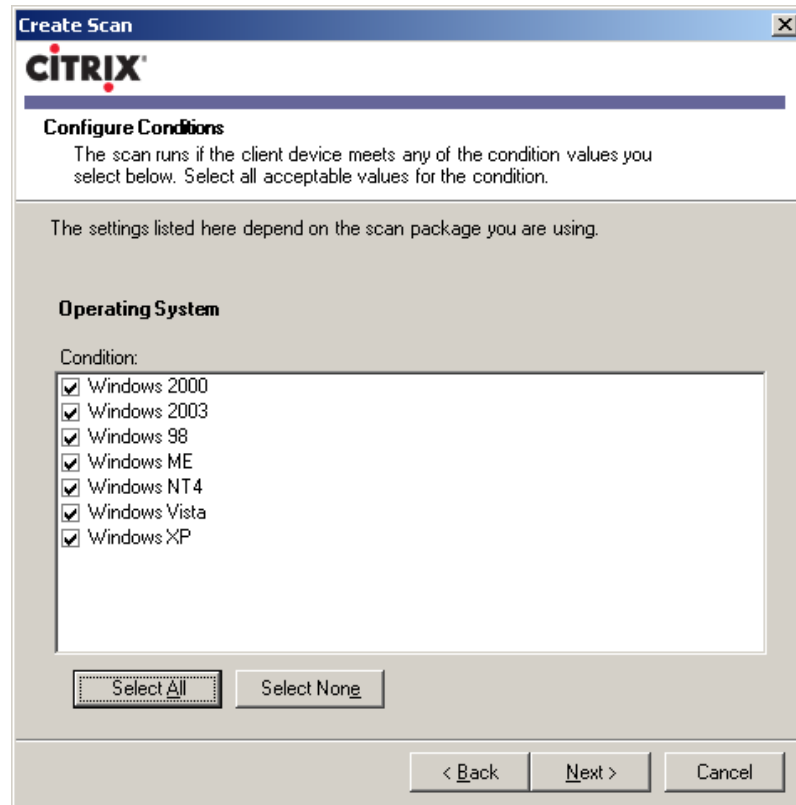
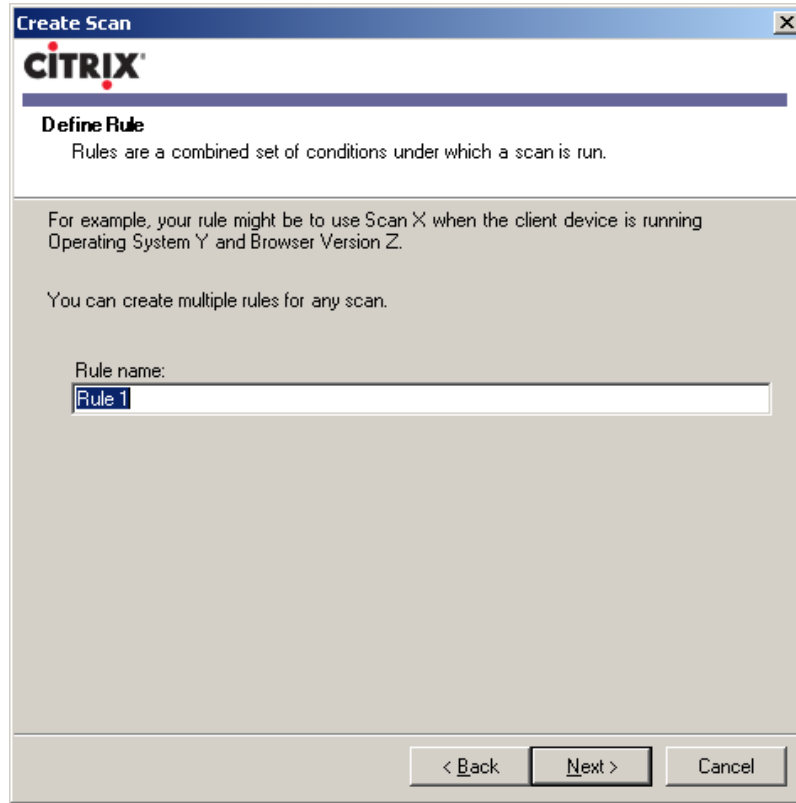
2. Type a name for the scan:

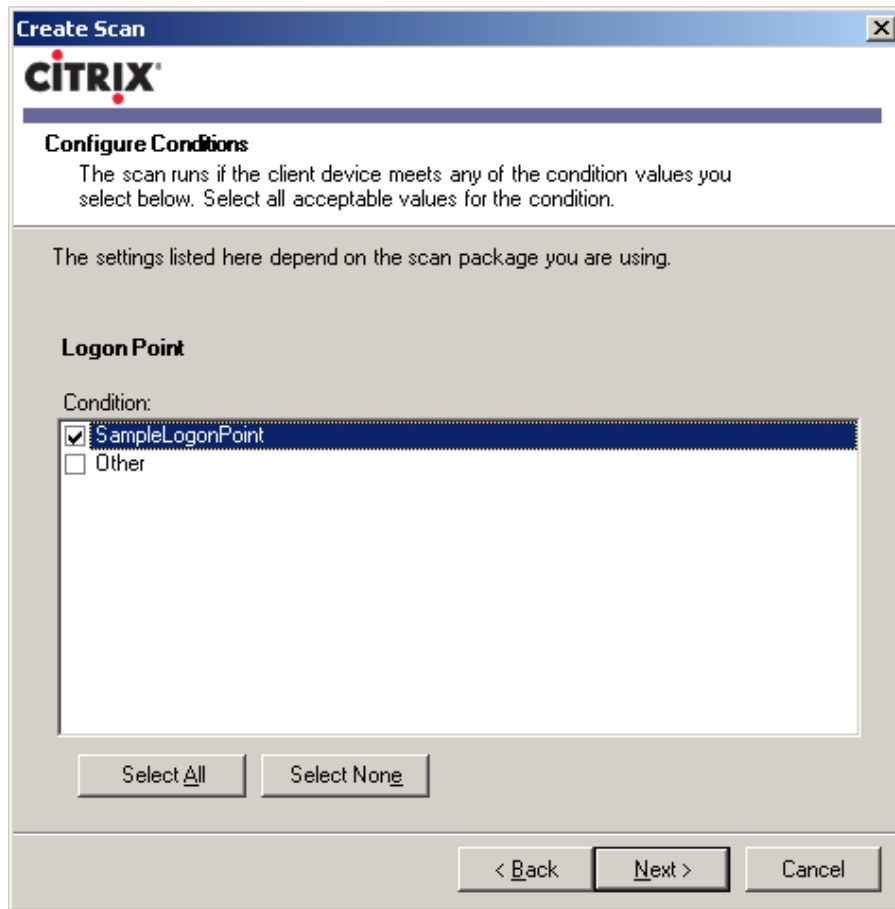


3. Set the scan conditions:

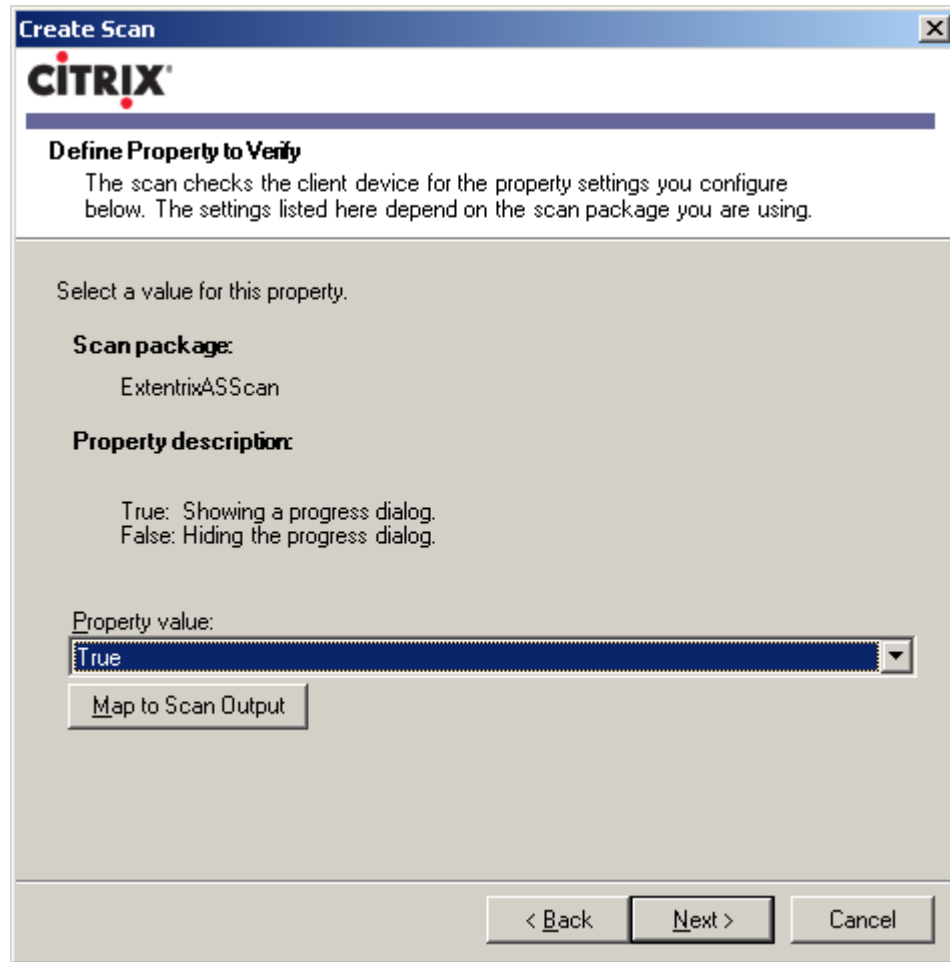


4. Type rule name and set rule conditions:





5. Select to view progress dialog to client during scan or not.



6. Type the name in **Property Value**.

Create Scan

CITRIX

Define Property to Verify
The scan checks the client device for the property settings you configure below. The settings listed here depend on the scan package you are using.

Enter a whole number for this property.

Scan package:
ExtentrixASScan

Property description:
Define the maximum time which is allowed to elapse from update date to access request date.

Property value:
15

Map to Scan Output

< Back Finish Cancel

7. When you are done, click **Finish**.

6. EXTENTRIX USER OPTION AS SCAN

SCAN DESCRIPTION

Scan Name: Extentrix User Option AS Scan.

Description: This scan will check each Antispyware defined in Extentrix Antispyware supported list, if it exists in the client machine, up to date and running. It makes sure of:

- Existence of the AS (antispyware).
- Real time protection.
- Last update anti spyware definition files.

Parameters:

- Show/Hide Dialog – a Boolean value which allows administrators to show (true) or hide (false) the progress dialog to the client while scanning his/her machine.
- AS Map – a double-columned data set, each one of its records has an Antispyware name and time allowed pair. Antispyware name is a string value as named on <http://www.extentrix.com/EPA/AVsFWs.htm>, and the time allowed is a string value that defines number of days of last update time allowed to the AS.

Scan Output:

- Allow Access - a Boolean output which indicates whether the client has an antispyware with allowed update period or not.

TRUE – indicates that the client has one of supported administrator AS list (list created by administrator using Extentrix supported list) installed, enable and running.

FALSE – indicates that the client doesn't have one of supported administrator AS list (list created by administrator using Extentrix supported list) installed, enable and running.
- License Status- a String output which indicates whether the scan is licensed or not.

TRIAL LICENSE – indicates that the scan has a trial license.

INVALID LICENSE – indicates that the scan hasn't a license.

VALID LICENSE – indicates that the scan is licensed.

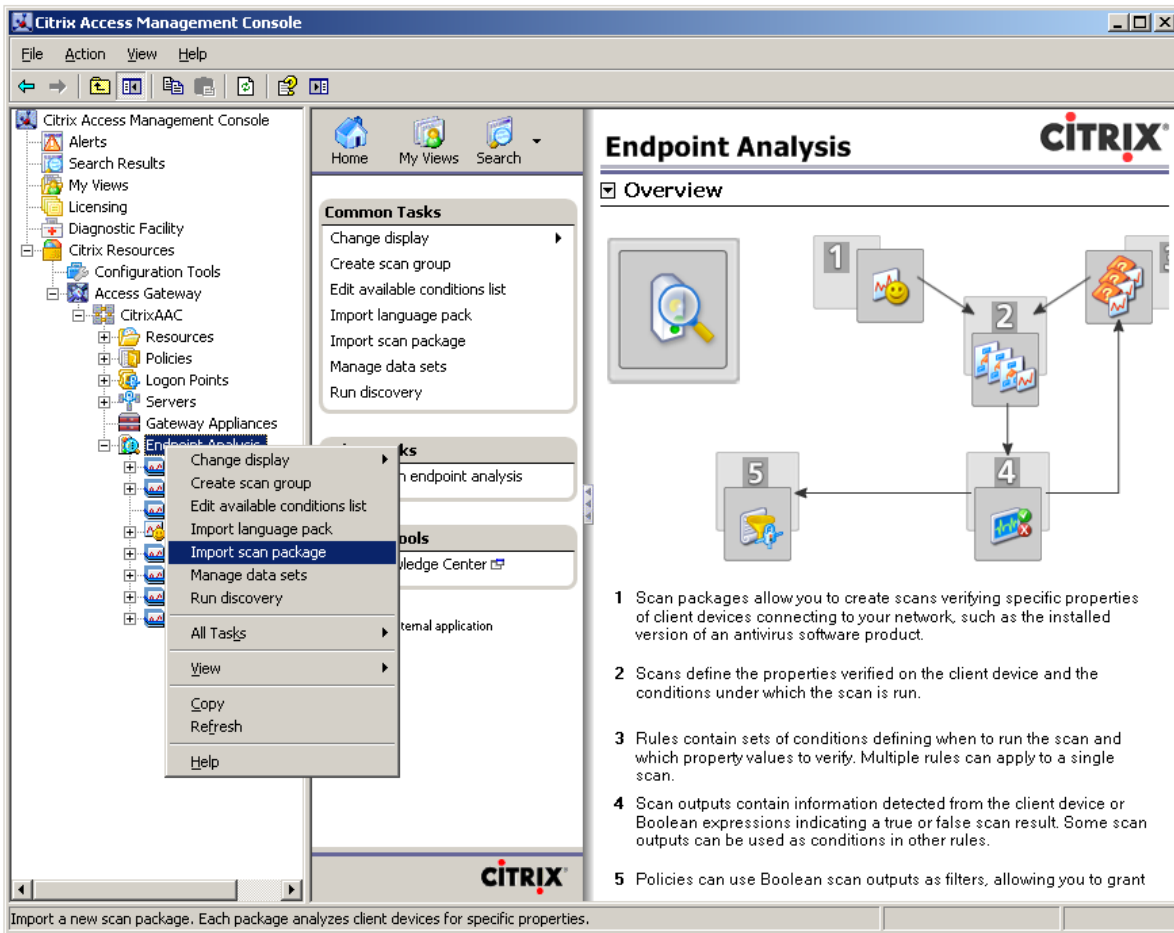
Note: If the License Status has an Invalid License value, the Allow Access will be false.

INSTALLATION AND CONFIGURATION

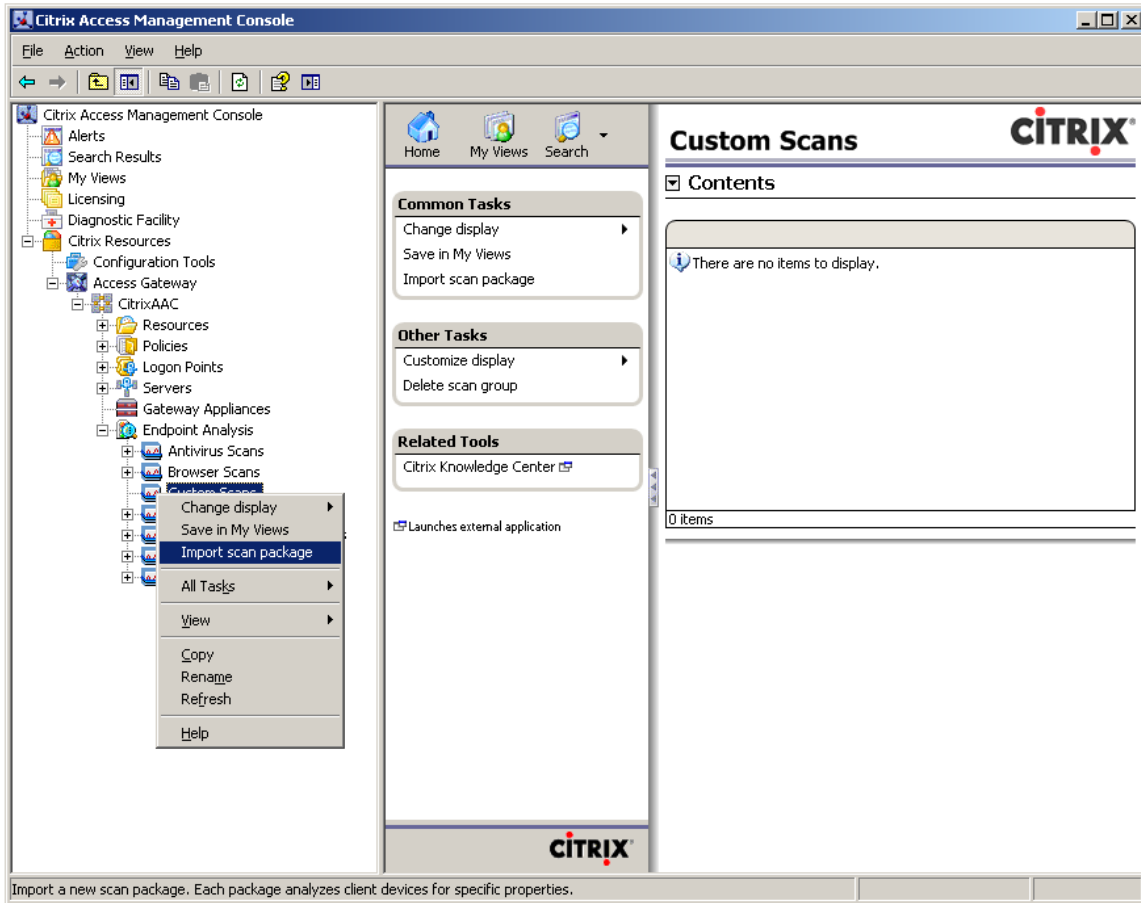
IMPORTING SCAN PACKAGES

To install a custom end point analysis scan package follow the following steps:

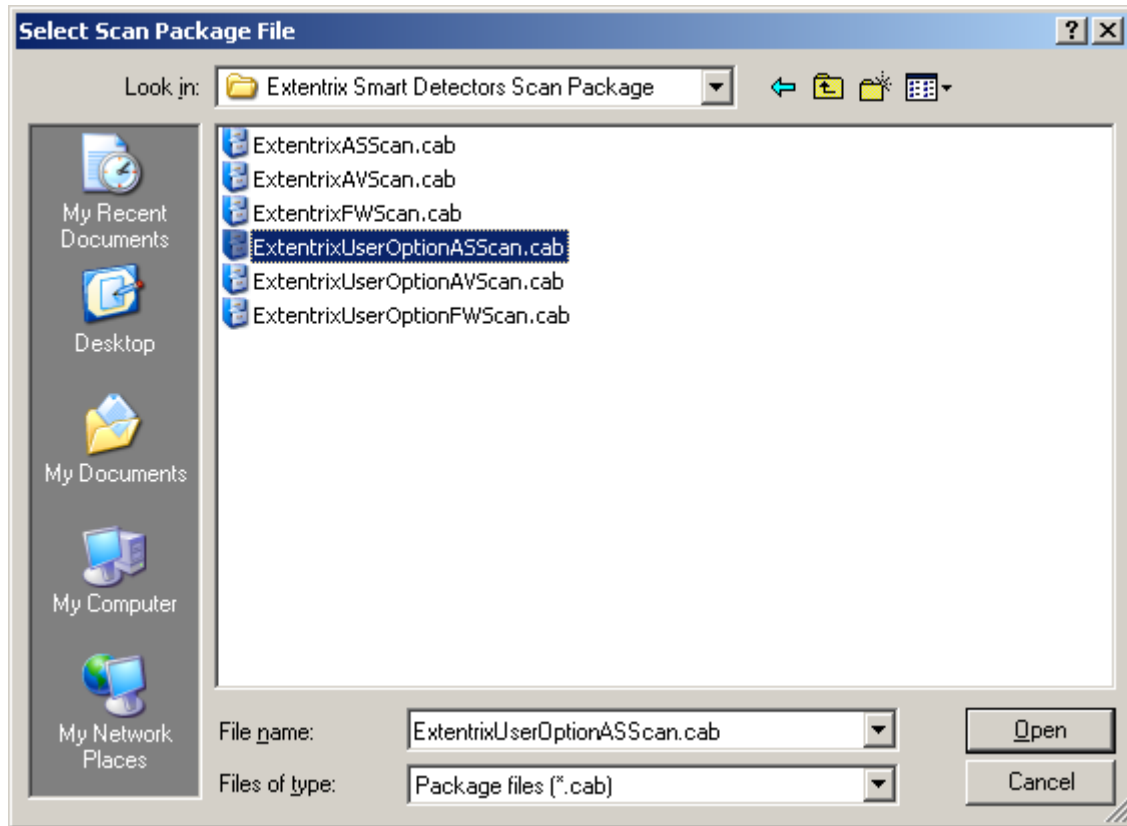
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



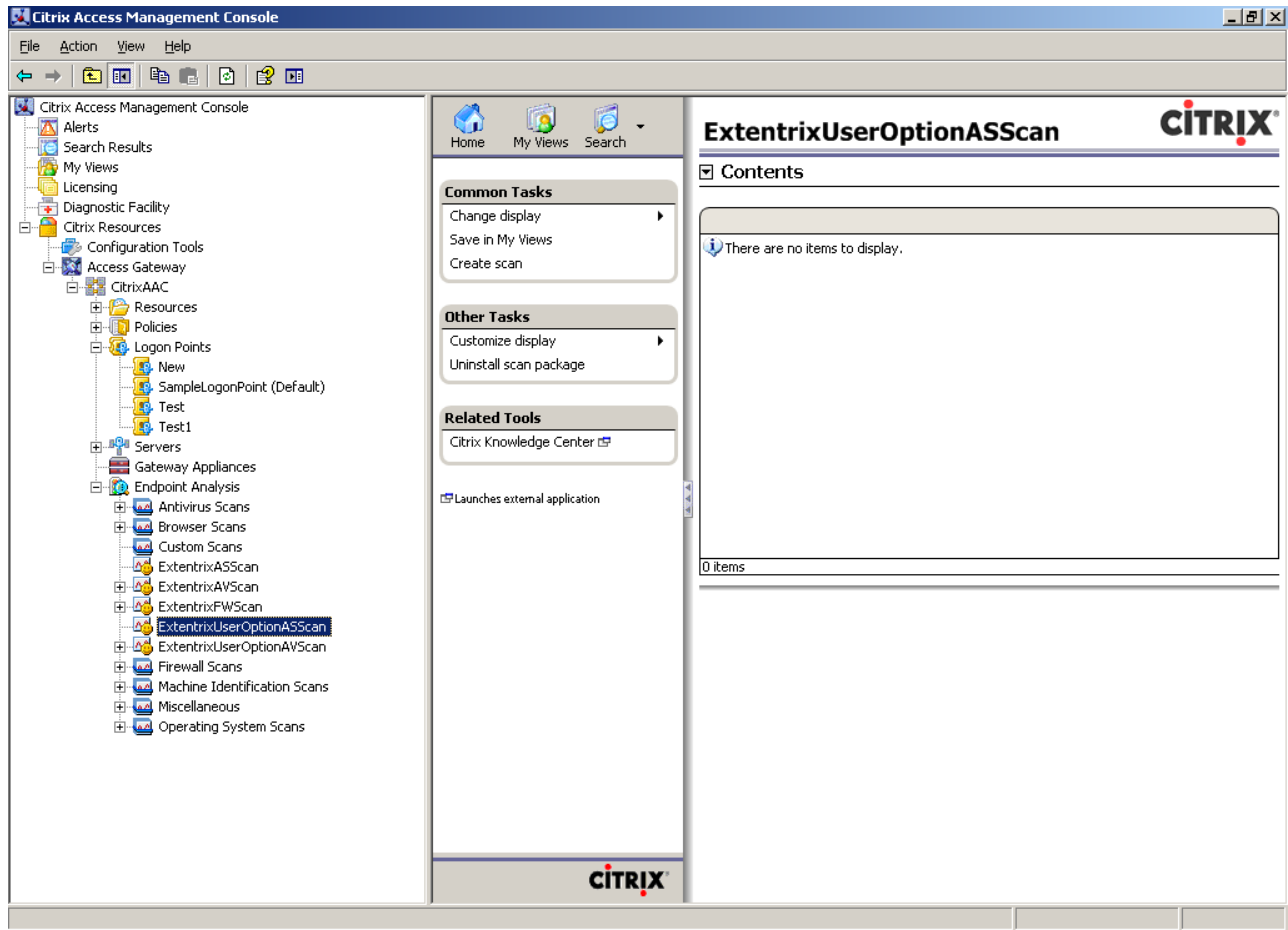
Also you can choose to insert the scan package to a specific scan package group as shown in the following picture:



3. A dialog box named “Select Scan Package File” will appear. Double click on the (.cab) file which contains the Scan.



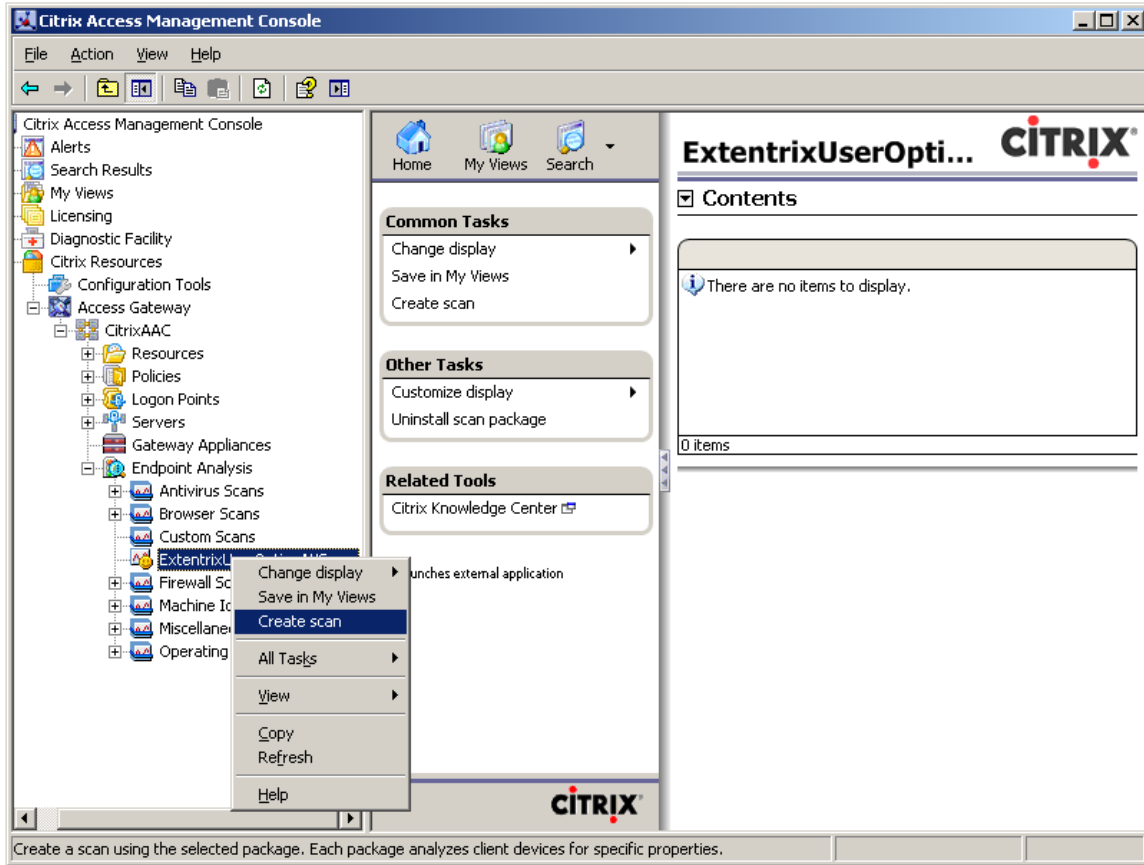
The package will be displayed in the console as shown in the following picture:



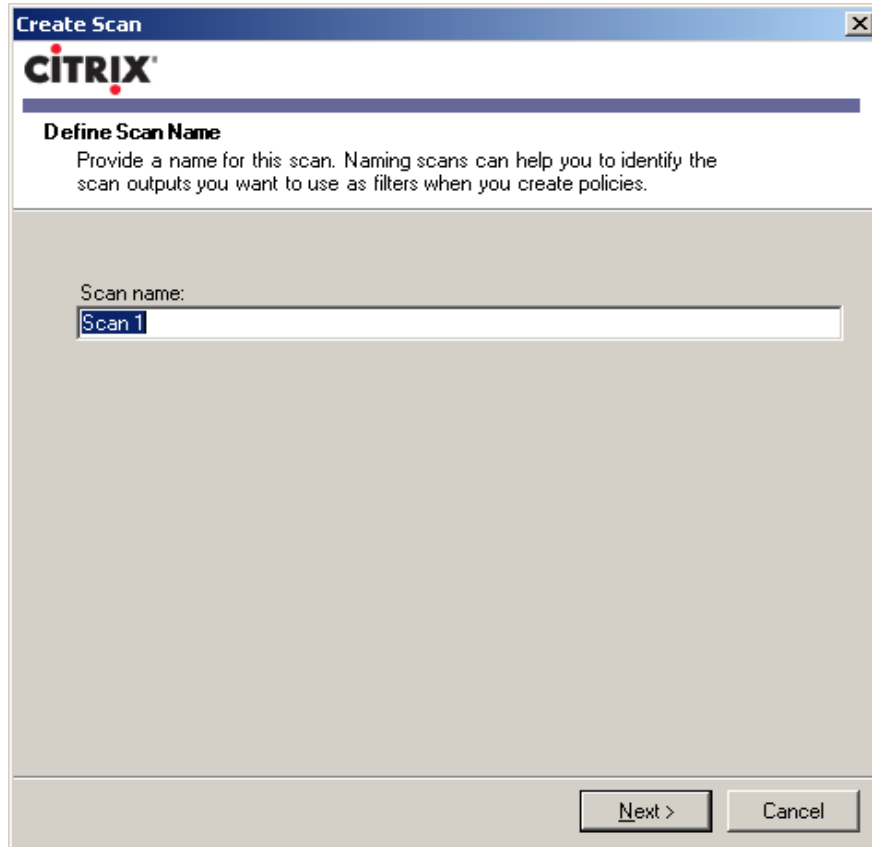
INSTALLING THE SCAN PACKAGE

Please follow the steps below to create scans and rules for the **Extentrix User Option AS Scan**.

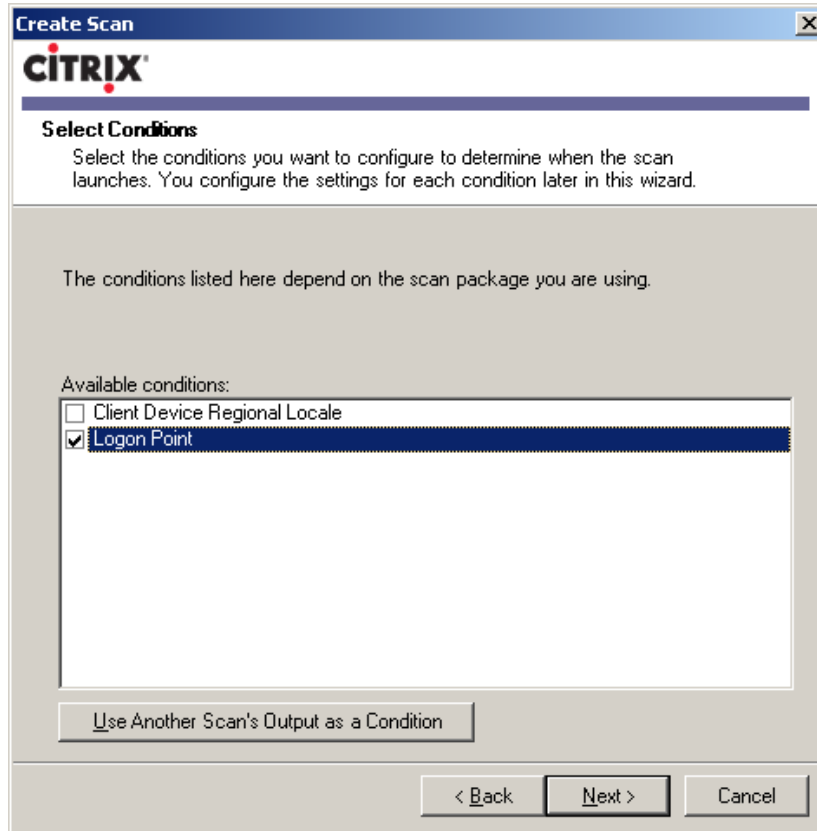
1. Select **ExtentrixUserOptionASScan** to create scan for it, right click the icon and choose **Create Scan**.



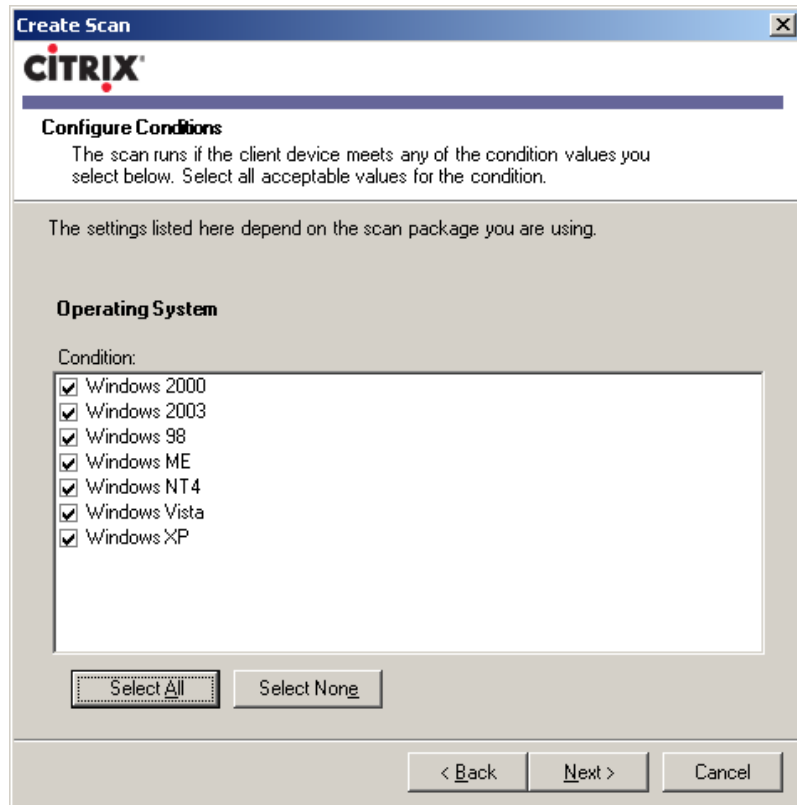
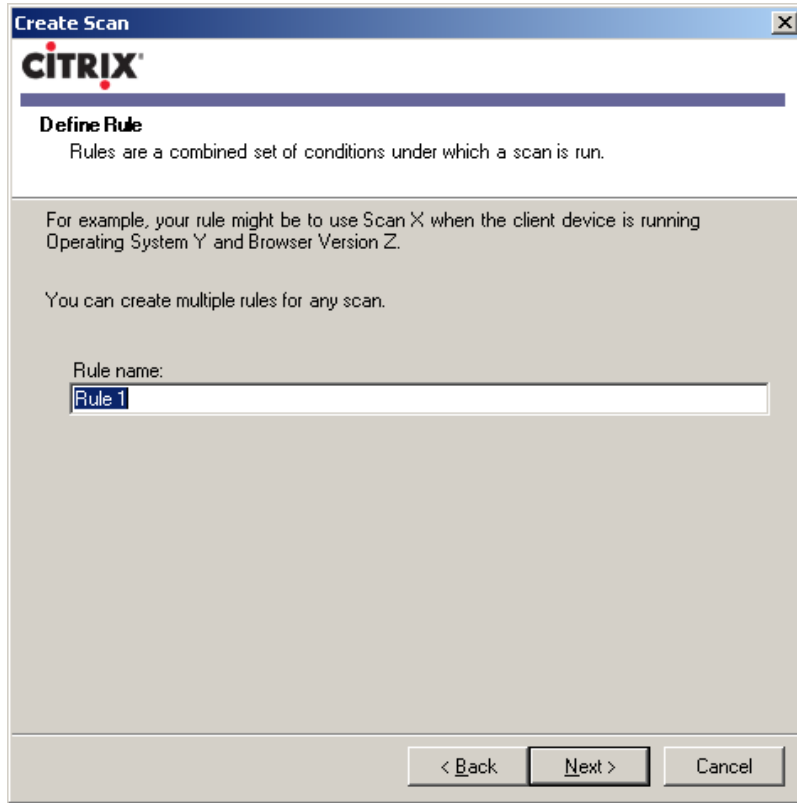
2. Type a name for the scan:

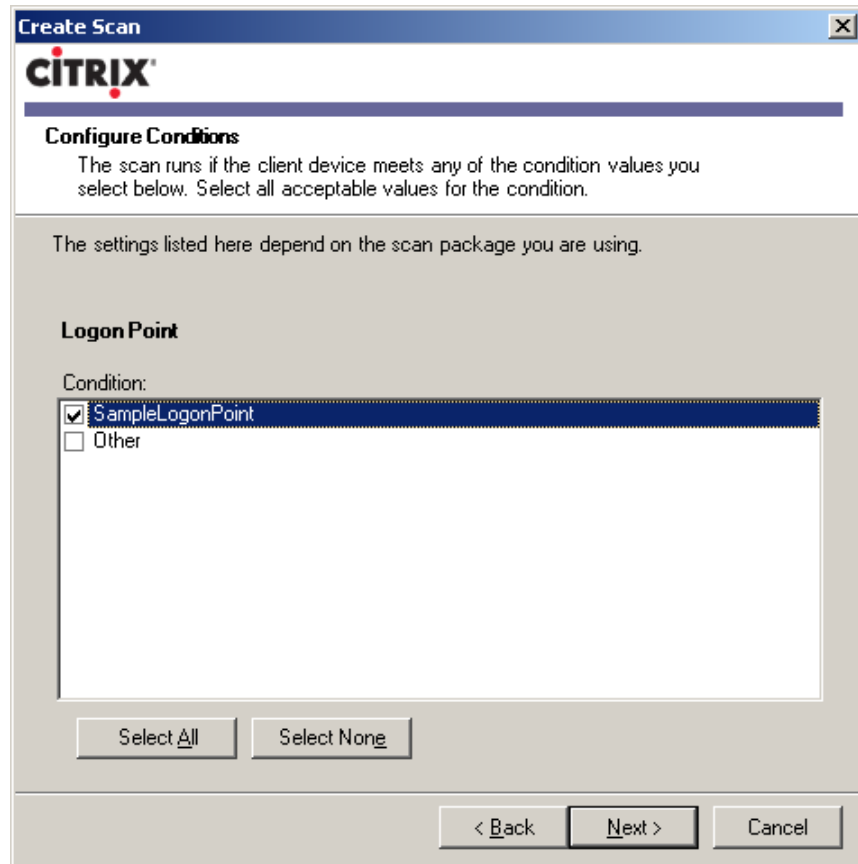


3. Set the scan conditions:

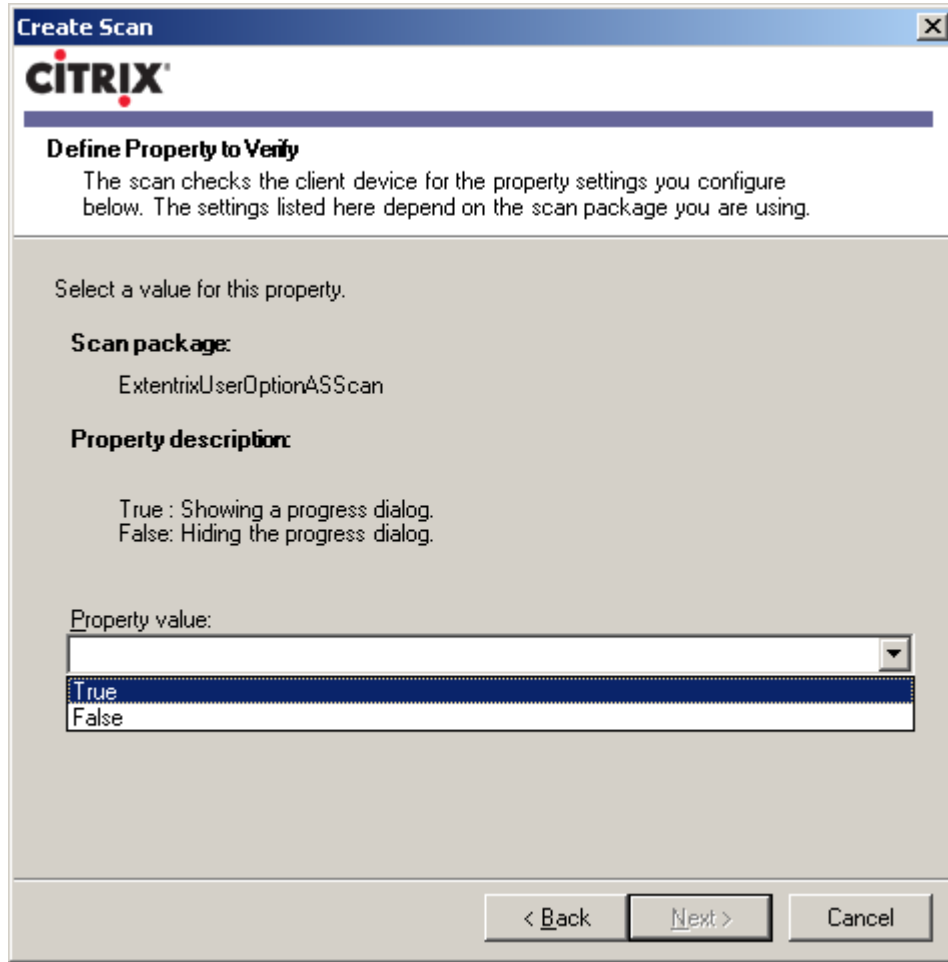


4. Type rule name and set rule conditions:

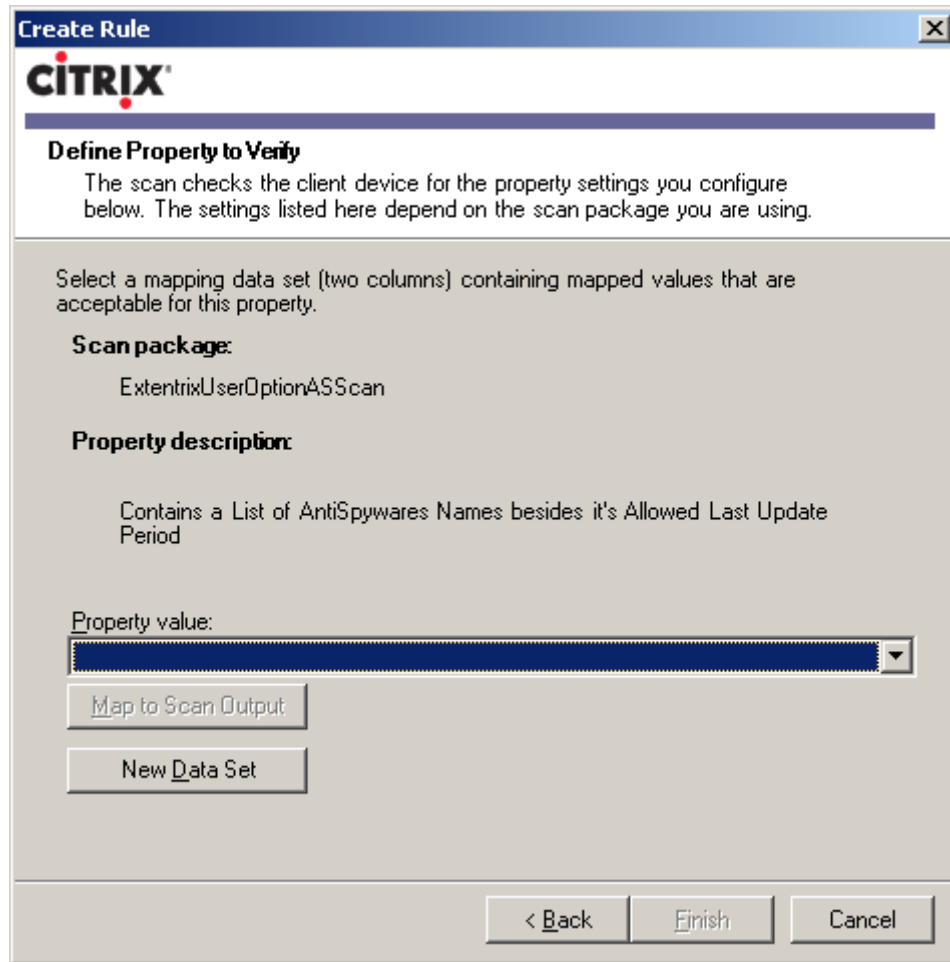




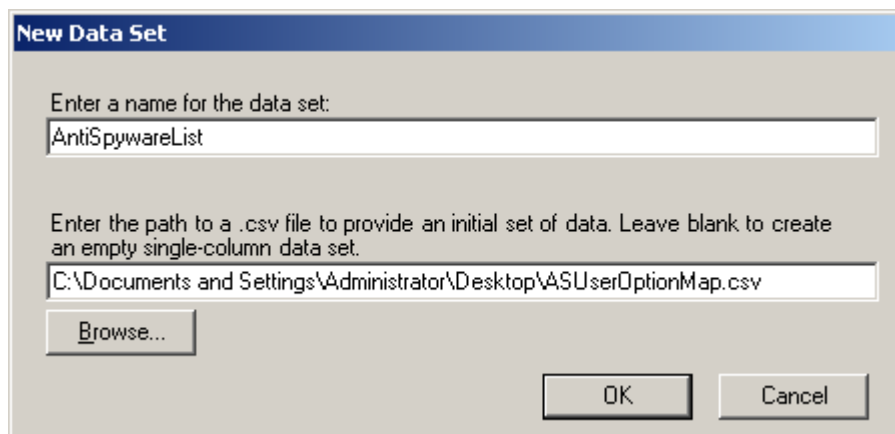
5. Type the name in **Property Value**.



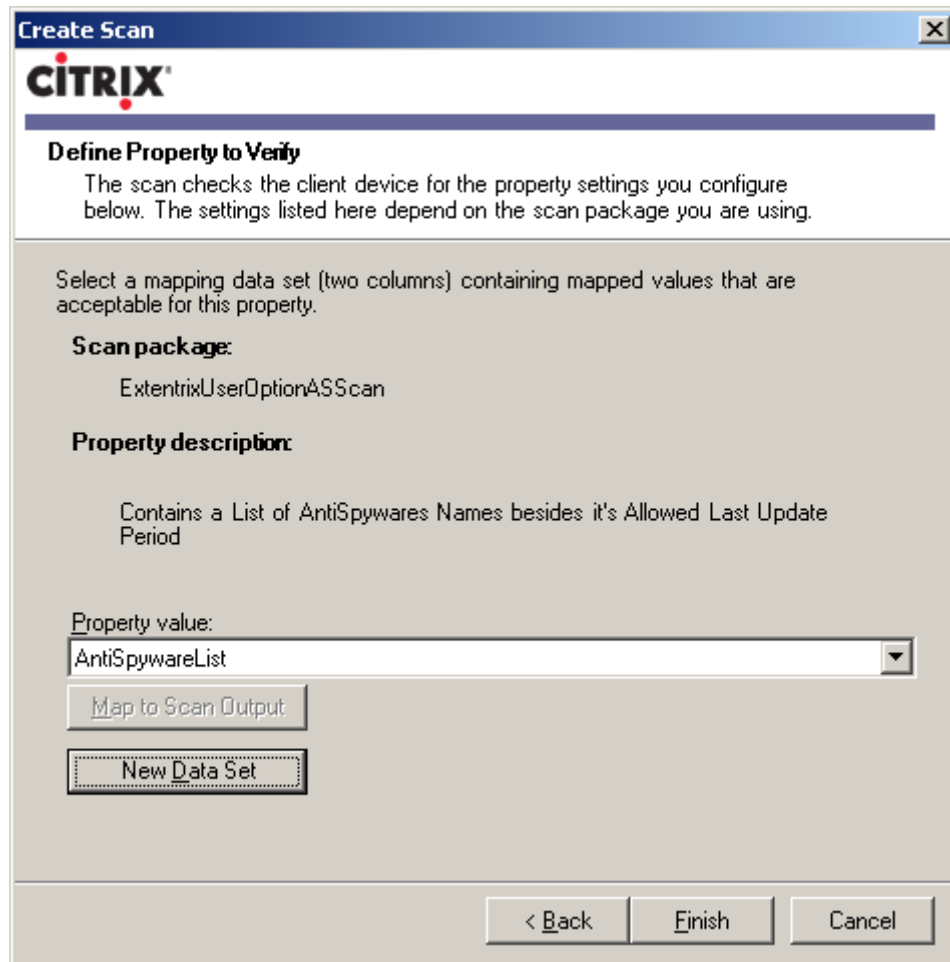
6. Define a data set (map) using a comma delimited .csv file. To do that, click on **New Data Set** to import the file. The file will have a list of Antispyware names and its desired time allowed.



7. A dialog box named “**New Data Set**” will appear. Type a name for the new data set and use **Browse** to enter the path of the .csv file.



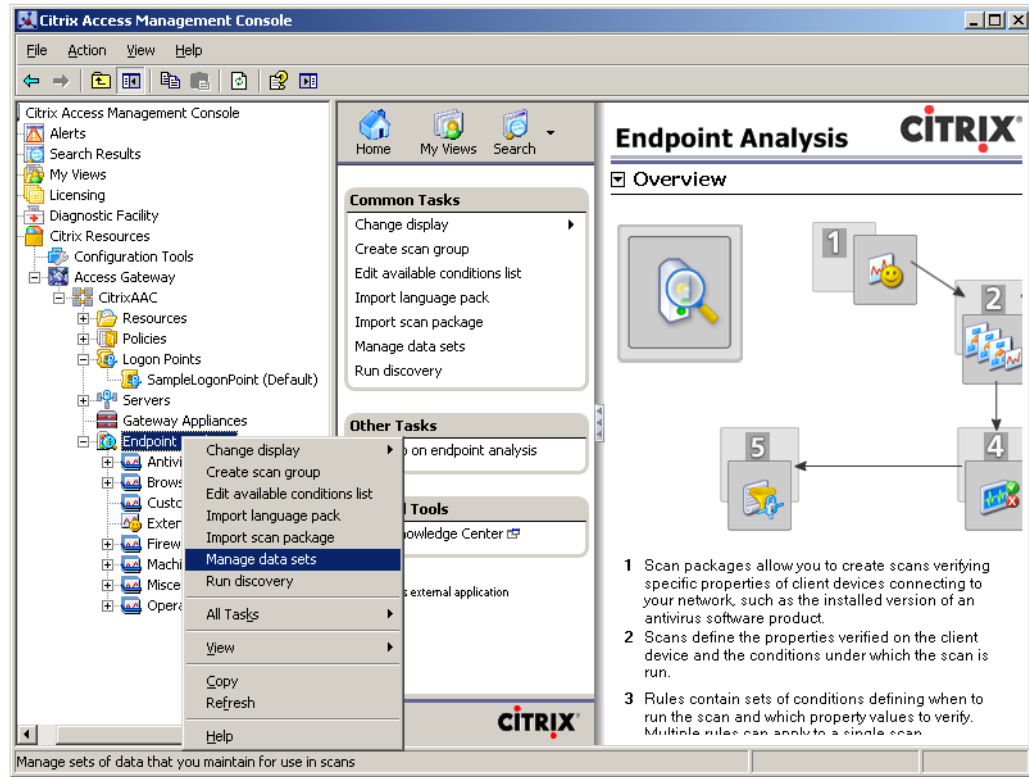
8. When you are done, click **Finish**.



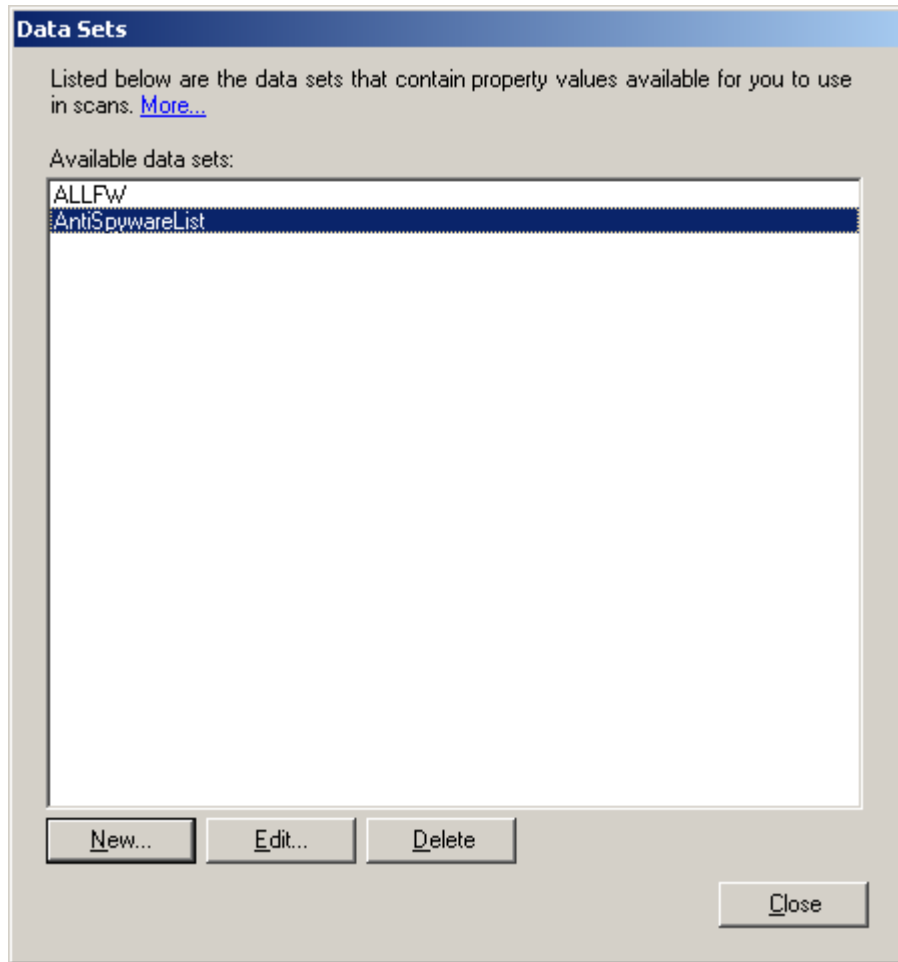
In the other side, when clients attempt to connect to the server that deploys this scan package, an active X control will be installed and it will perform the scanning operation. During this process, a progress bar will be shown to inform the clients about the scan progress.

Note: You can edit the value later after you create the data set. To edit the data set:

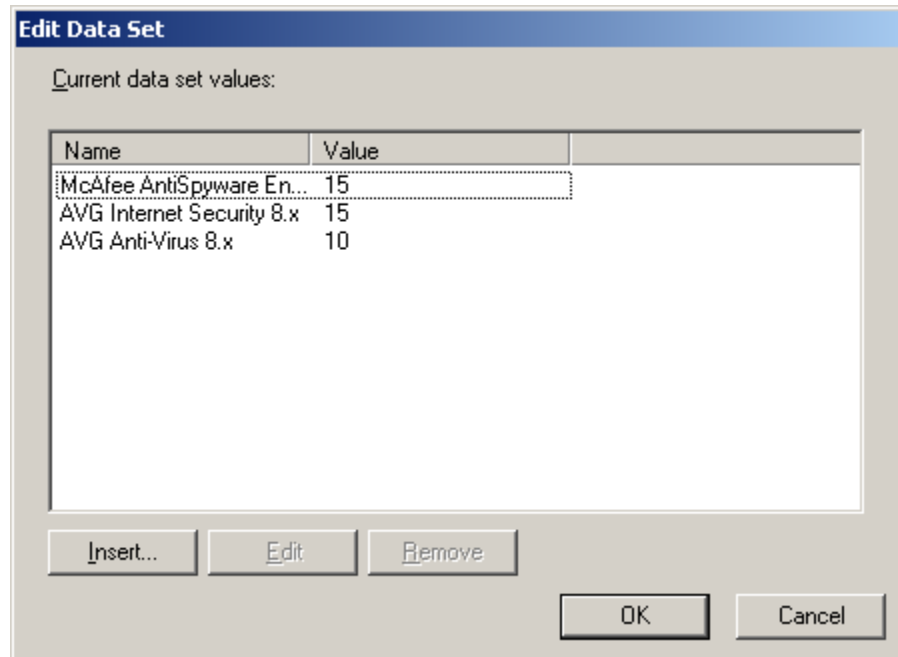
- a. Right click **Endpoint Analysis** in the console tree and select **Manage Data Set** from the action menu.



- b. A window named **“Data Sets”** will appear. Click the data set for which you want to make editing then click **Edit**.



- c. A window named **"Edit Data Set"** will appear.



- d. Make the editing you want (whether inserting new values, Editing or removing existing values). When you are done, click **OK**.

SUPPORT

Support for Extentrix Smart Detectors Scan Package is available at [Extentrix Forum](#)

For any support issues, please email your questions or problems to: support@extentrix.com

GLOSSARY

Endpoint analysis A process that scans a client device and detects information such as the presence and version level of operating system, antivirus, firewall, or browser software. Endpoint analysis can verify that the client device meets your requirements before allowing it to connect. This information can be included as a filter within a policy to determine the appropriate level of access to corporate resources.

Endpoint Analysis Client An ActiveX control or a browser plug-in used to discover information about a device's configuration (such as the operating system, antivirus pattern, and so on).

INDEX

E

Endpoint analysis, 91

Endpoint Analysis Client, 91

Extentrix AV Scan, 5, 62

Extentrix FW Scan, 18

Extentrix User Option AV Scan, 30, 74

Extentrix User Option FW Scan, 47

I

Importing scan packages, 6, 19, 32, 48, 63, 75

Installing the scan package, 10, 23, 36, 52, 67, 79

Introduction, 4

P

Parameters, 5, 18, 30, 47, 62, 74

S

Scan Output, 5, 18, 30, 47, 62, 74

support, 90

ABOUT EXTENTRIX

Founded in 2006, Extentrix Systems is a leading software development company specializing in virtualization and developing custom software solutions for Microsoft and Citrix customers. Established by former software engineers at Citrix, Extentrix have developed access solutions that simplify and speed users' access to Terminal Services and Citrix platforms.

Extentrix Systems is privately held with company headquarters in RAK, UAE. For more information, please visit the company's Web site at www.extentrix.com or call +971-4-208-8496.

For additional support in writing new scan packages or customizing the current one, please contact Extentrix at info@extentrix.com or by visiting the company's home page at <http://www.extentrix.com/>.