

extentrix



Extentrix
Essentials Scan Packages

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..... 2

TABLE OF CONTENTS 3

INTRODUCTION 5

SCANS INCLUDED INSIDE EXTENTRIX ESSENTIALS SCAN PACKAGE 6

1. EXTENTRIX PROCESS NAME CHECK SCAN 6

Scan description 6

Installation and configuration..... 7

Importing scan packages 7

 Installing the scan package 11

2. EXTENTRIX REGISTRY KEY SCAN..... 23

Scan description 23

Installation and configuration..... 25

Importing scan packages 25

Installing the scan package 29

3. EXTENTRIX SCREEN SAVER SCAN 41

Scan description 41

Importing scan packages 42

 Installing the scan package 46

4. EXTENTRIX SERVICES CHECKER SCAN 54

Scan description 54

Installation and configuration..... 55

Importing scan packages 55

 Installing the scan package 59

5. EXTENTRIX FILES’ DATE SCAN 70

Scan description 70

Installation and configuration..... 71

Importing scan packages 71

Installing the scan package 75

6. EXTENTRIX FILES' SIZES SCAN..... 87

Scan description 87

Installation and configuration..... 88

Importing scan packages 88

Installing the scan package 92

7. EXTENTRIX FILE SCAN..... 103

Scan description 103

Installation and configuration..... 104

Importing scan packages 104

Installing the scan package 108

8. EXTENTRIX EXTENDED REGISTRY KEY SCAN 119

Scan description 119

Installation and configuration..... 121

Importing scan packages 121

Installing the scan package 125

9. EXTENTRIX WORKING HOURS SCAN 140

Scan description 140

Installation and configuration..... 141

Importing scan packages 141

Installing the scan package 145

SUPPORT..... 154

GLOSSARY 155

INDEX..... 156

ABOUT EXTENTRIX 157

INTRODUCTION

The key design goal for Extentrix Essential Scan Package is to help IT administrators setup their corporate security policies for the end point users to meet the requirements before they are establishing the connection with the XenApp server. By providing this, the administrator ensures ongoing control over users machines in today's changing environment.

Extentrix Essentials Scan Package enables IT administrators to perform a variety of essential checks that are necessary to exist on user's machine before granting him a connection to their resources. Examples of these various checks are: the value of a certain registry value, the running status of a certain process, whether a certain windows service is running or not, the presence of screensaver and is it password protected? , verifying that subnet information and the connection type of a user machine are within scope plus other necessary checks.

Using Extentrix Essentials Scan Package enables IT administrators to have a centralized Control over end point users' machines. The increased number of scans in enables IT administrators to centrally customize a secure global policies plan that suits their company needs.

The Extentrix Essentials Scan Package is a comprehensive scan solution that consists of:

1. Distributed File:

- EPAClient.exe / EPAPLugin.exe if build Hotfix 4`
- Append.txt

2. Scans:

- Extentrix Process Name Check Scan
- Extentrix Registry Key Scan
- Extentrix Screen Saver Scan
- Extentrix Services Checker Scan
- Extentrix Files' Dates Scan
- Extentrix Files' Sizes Scan
- Extentrix File Scan
- Extentrix Extended Registry Key Scan
- Extentrix Working Hours Scan

SCANS INCLUDED INSIDE EXTENTRIX ESSENTIALS SCAN PACKAGE

Extentrix Essentials Scan Package contains many Scans inside. They are:

1. EXTENTRIX PROCESS NAME CHECK SCAN

SCAN DESCRIPTION

Scan Name: Extentrix Process Name Check.

Description: It scans the client's machine and ensures that a specified list of processes is running on that machine. For example, an IT administrator may specify that the process *outlook.exe* which stands for Microsoft Outlook application must be installed on the client's machine before granting him/her connection with XenApp. The connection will be established if the scan result indicates that the process *outlook.exe* process exist and running.

Parameters: Process names list – a list of all process names that should be verified to be running on the client's machine.

Scan Output:

- o Allow Access - a Boolean output which indicates whether the process list is running on the client's machine or not.

TRUE – indicates that all given processes are running on the client's machine.

FALSE – indicates that at least one of the processes is not running on the client's machine.

- o 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.

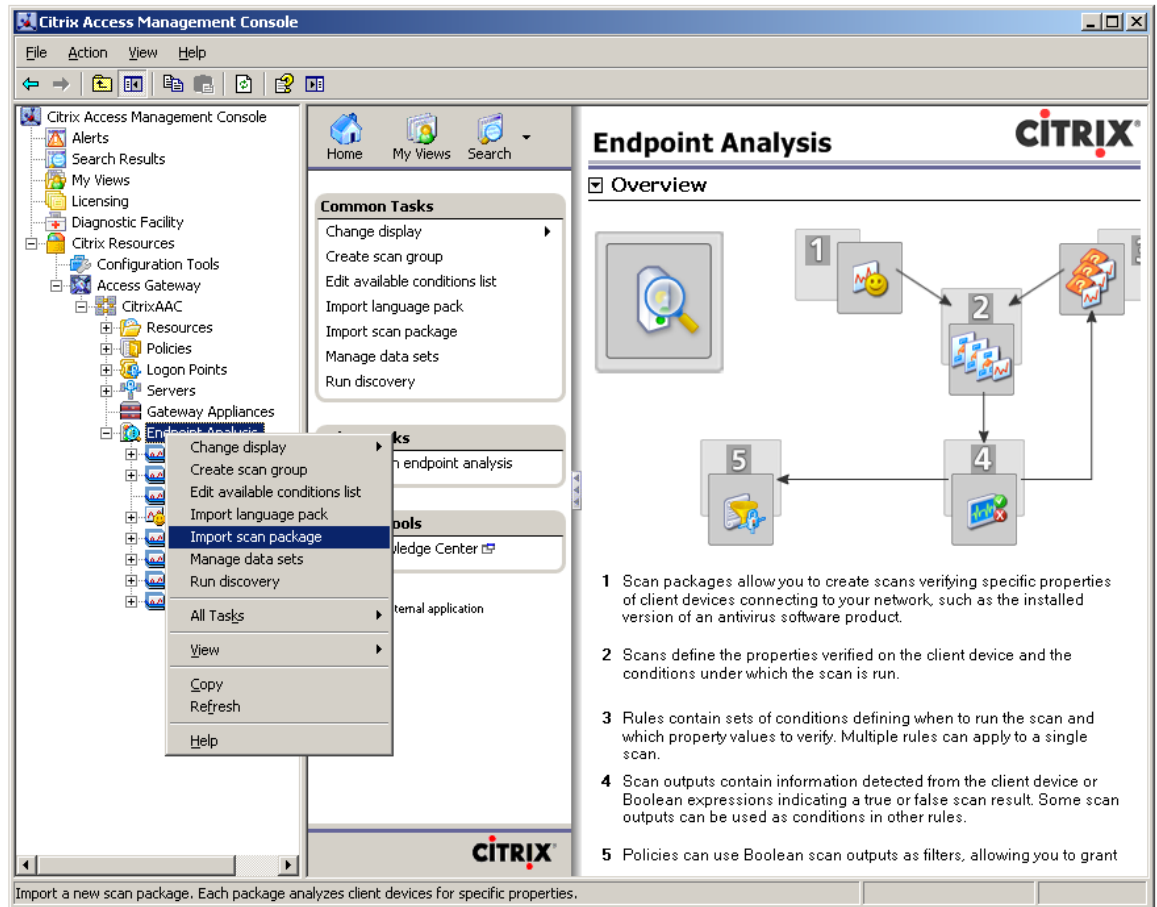
Note: If the License Status has an Invalid License value, the Allow Access will be false.

INSTALLATION AND CONFIGURATION

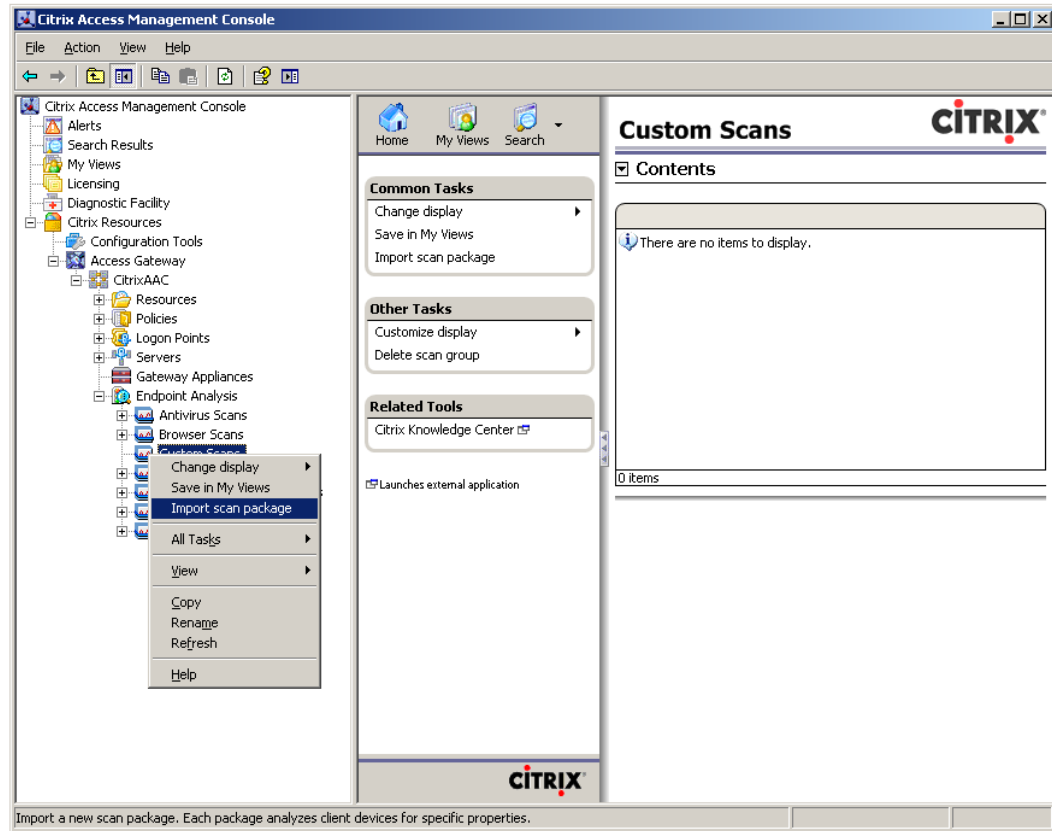
IMPORTING SCAN PACKAGES

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

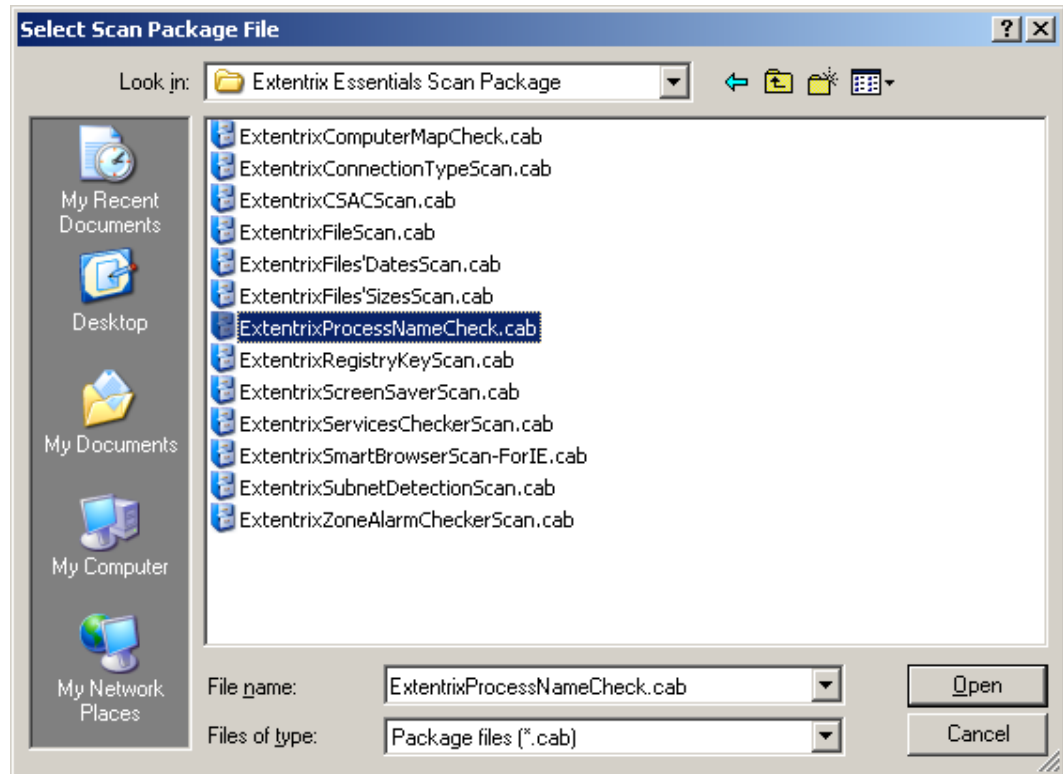
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



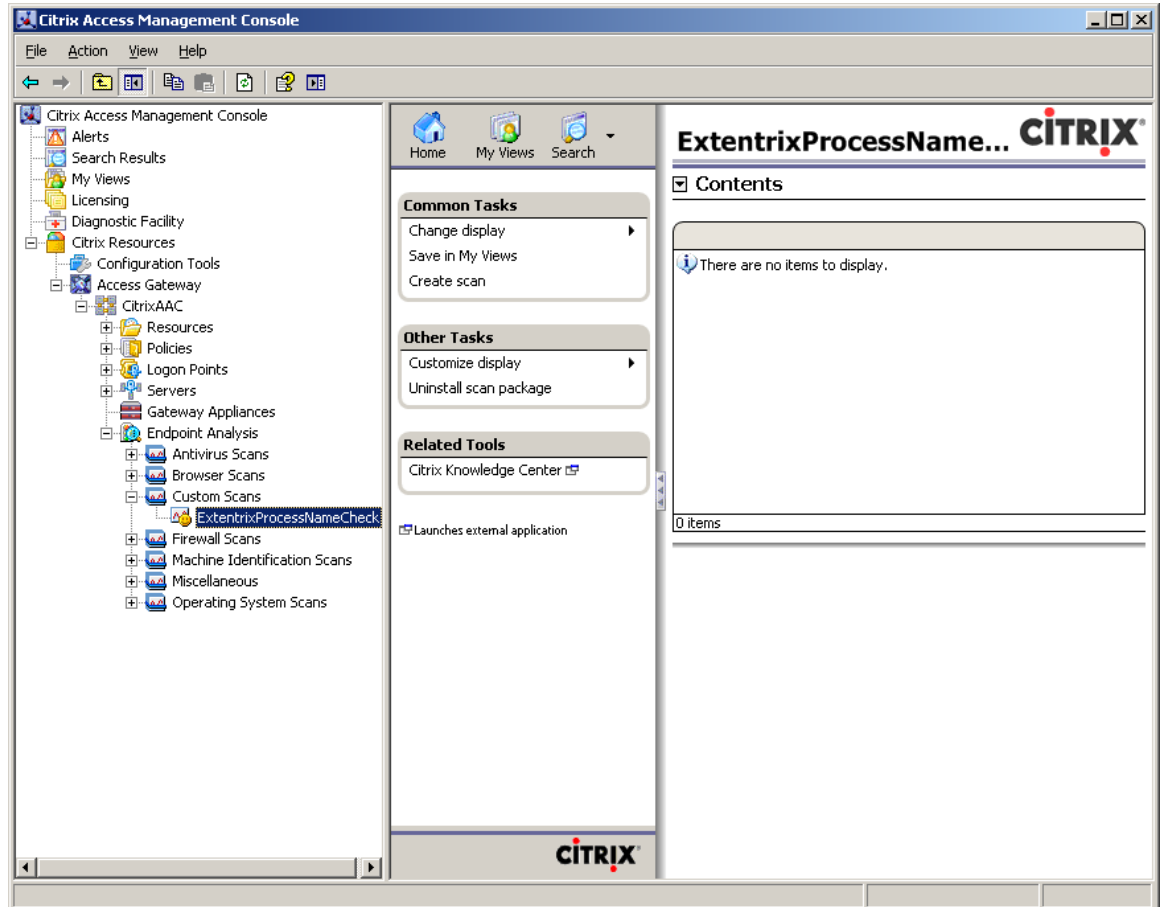
Also you can choose to insert the scan package to any scan category listed in the tree as shown in the following picture:



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



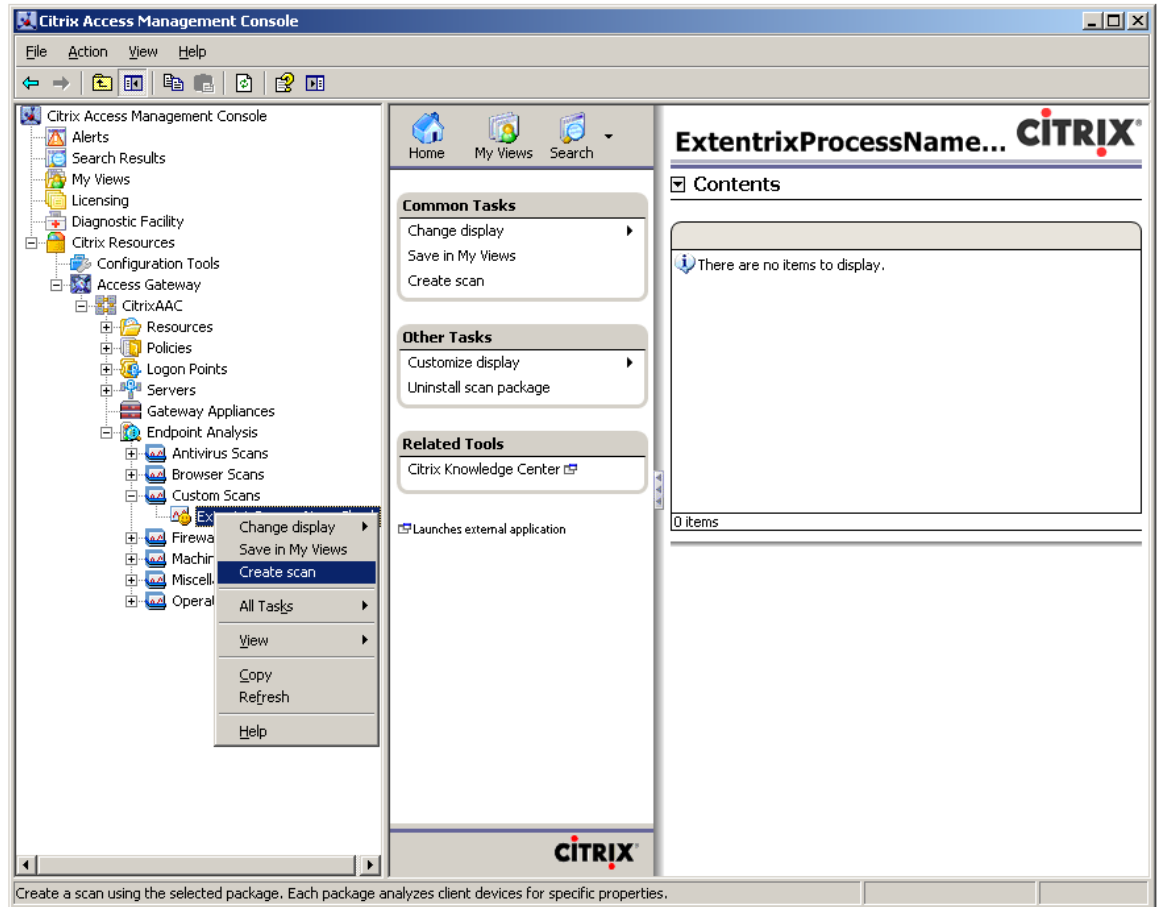
The package will be displayed in the console as shown in the following picture:



INSTALLING THE SCAN PACKAGE

Please follow the steps below to create scans and rules for the **Extentrix Process Name Check**.

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



2. Type a name for the scan:

Create Scan

CITRIX

Define Scan Name

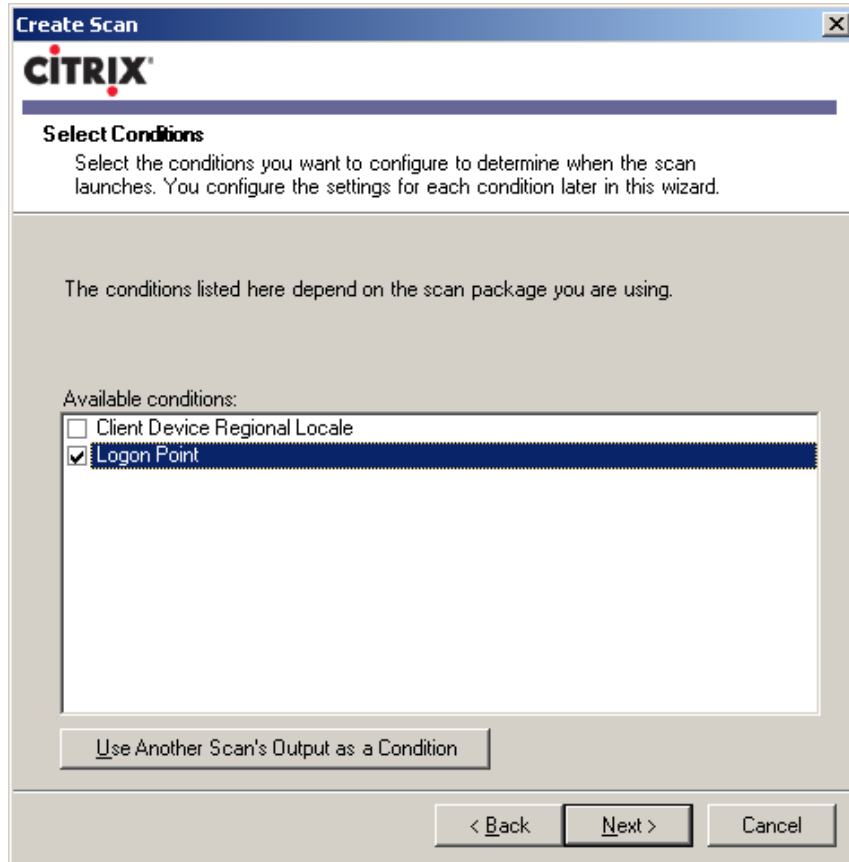
Provide a name for this scan. Naming scans can help you to identify the scan outputs you want to use as filters when you create policies.

Scan name:

Scan 1

Next > Cancel

3. Set the scan conditions:



4. Type rule name and set rule conditions:

Create Scan

CITRIX

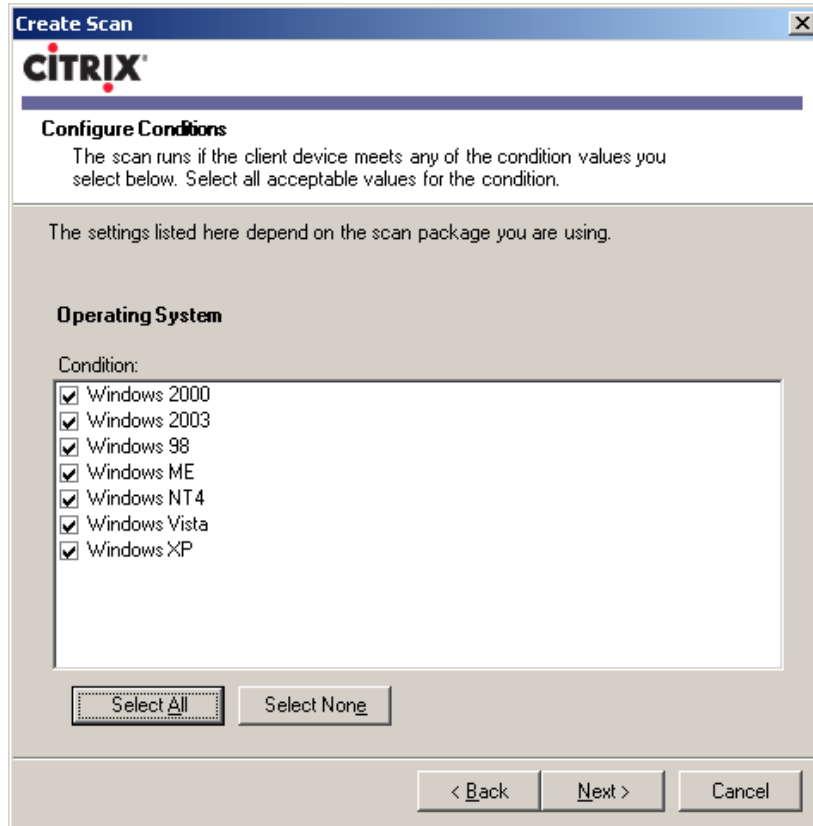
Define Rule
Rules are a combined set of conditions under which a scan is run.

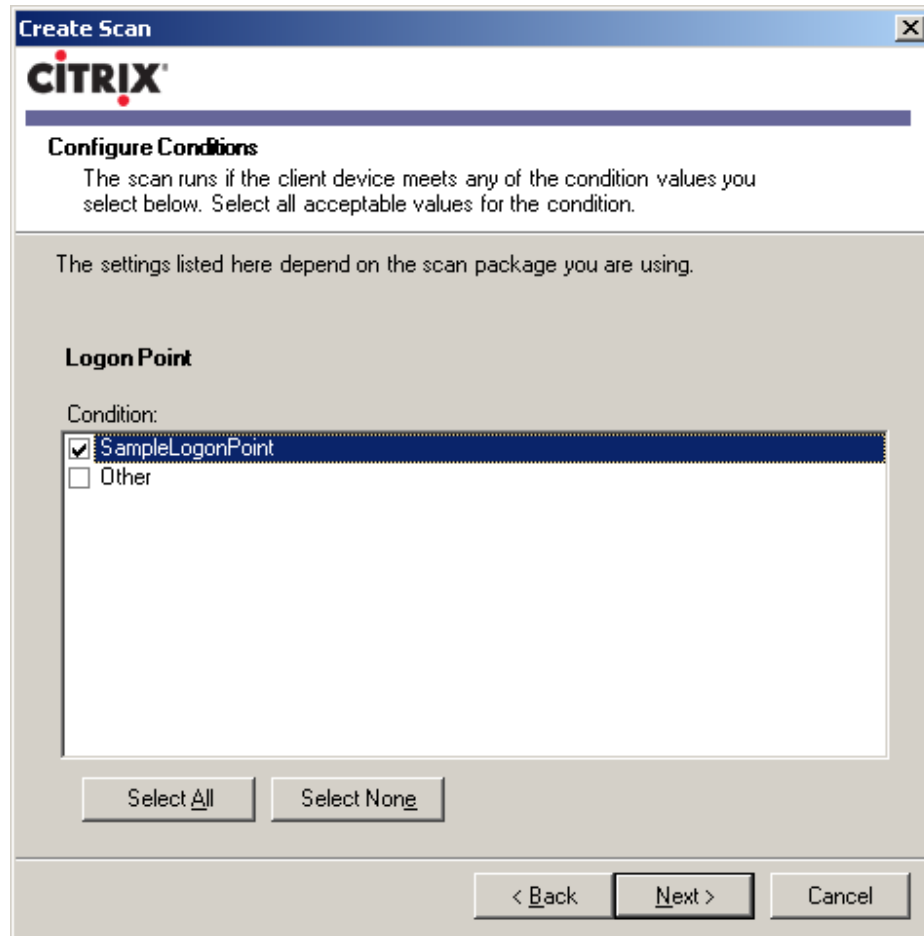
For example, your rule might be to use Scan X when the client device is running Operating System Y and Browser Version Z.

You can create multiple rules for any scan.

Rule name:

< Back Next > Cancel





5. Define a data set 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 process names to check if they are running or not. An example of process name is *outlook.exe* which stands for Microsoft Outlook application.

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.

Select a data set (single column) containing values that are acceptable for this property.

Scan package:
ExtentrixProcessNameCheck

Property description:
list of processes needed to be exist

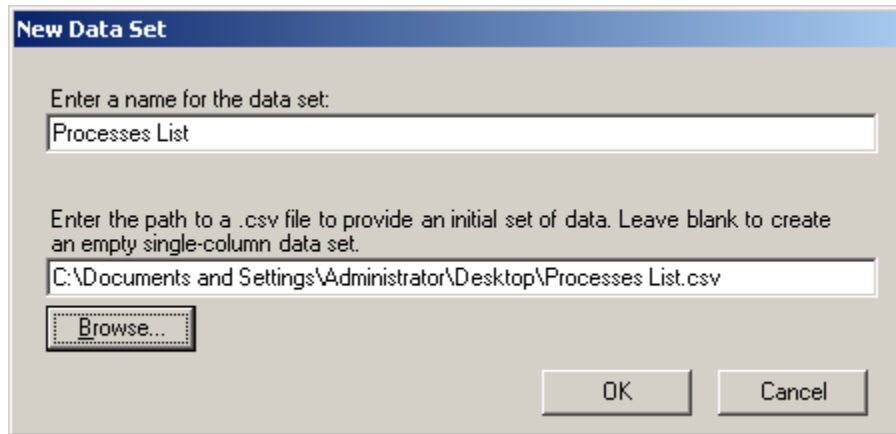
Property value:
[Dropdown menu]

Map to Scan Output

New Data Set

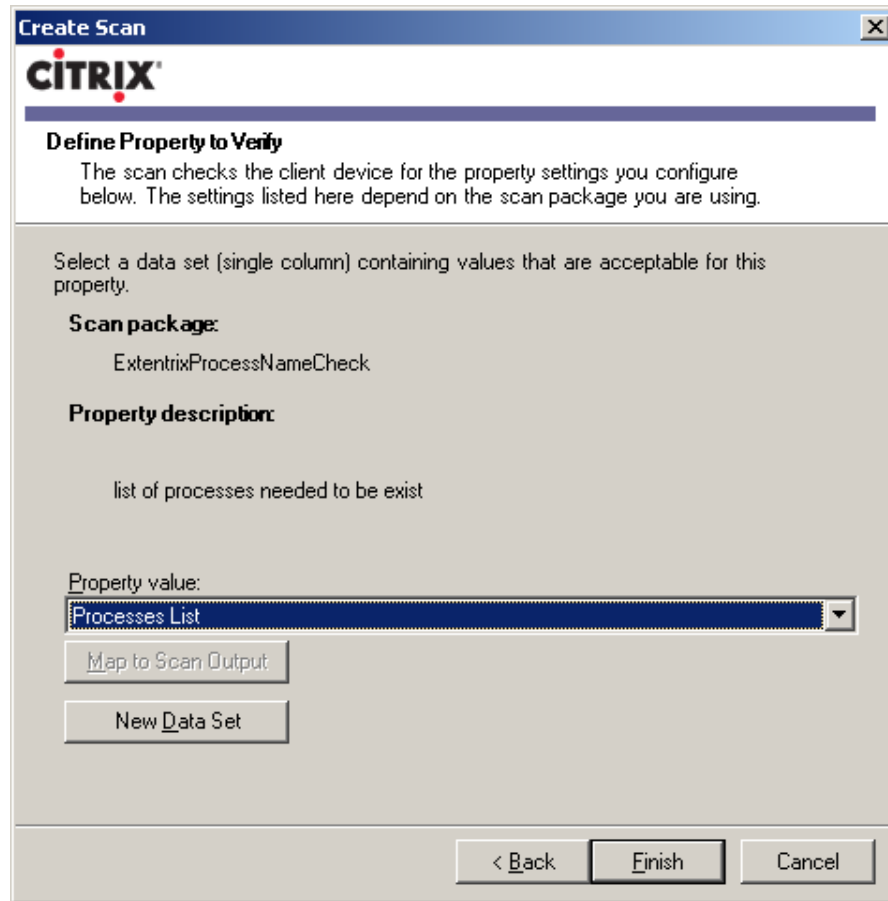
< Back Finish Cancel

6. 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.



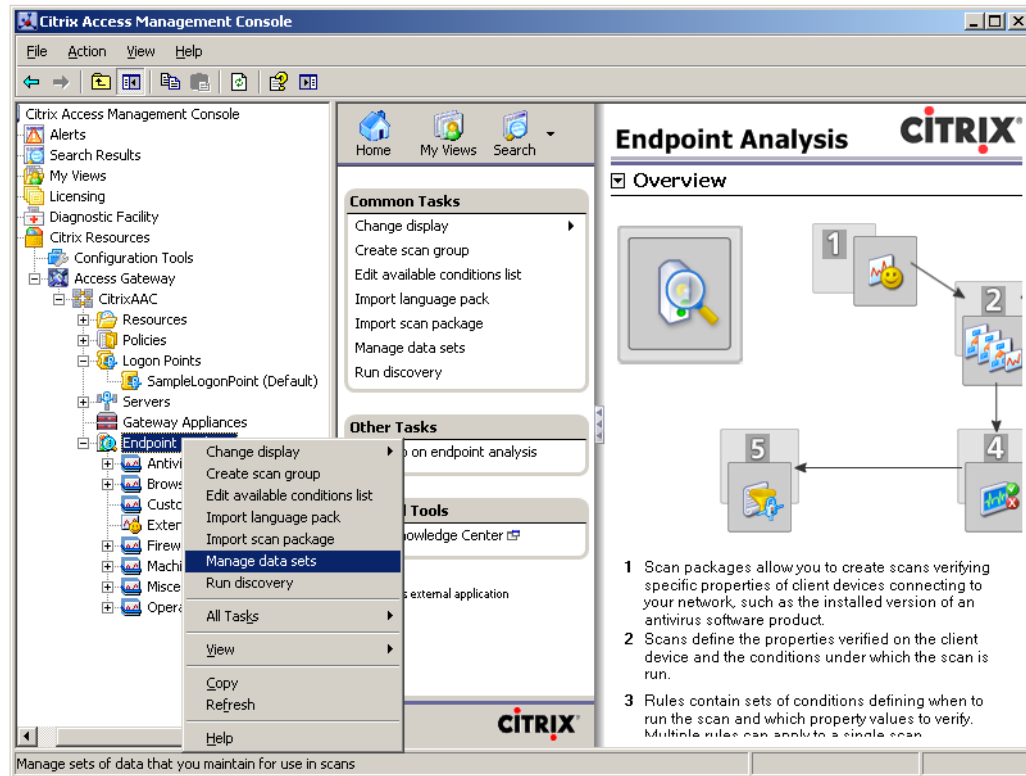
The image shows a dialog box titled "New Data Set". It has a blue header bar with the title. Below the header, there are two text input fields. The first field is labeled "Enter a name for the data set:" and contains the text "Processes List". The second field is labeled "Enter the path to a .csv file to provide an initial set of data. Leave blank to create an empty single-column data set." and contains the path "C:\Documents and Settings\Administrator\Desktop\Processes List.csv". Below the second field is a "Browse..." button. At the bottom right of the dialog box are "OK" and "Cancel" buttons.

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

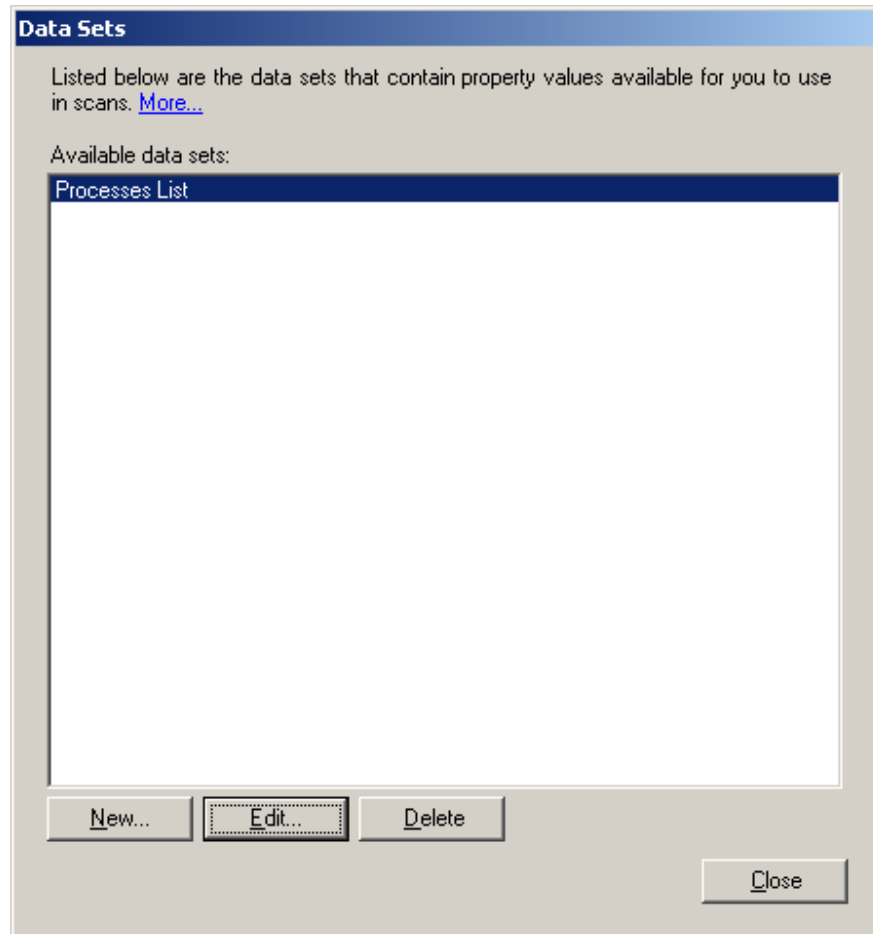


Note: You can leave the path of the file empty to create an empty single-column data set. You can edit the value later after you create the data set. To edit the data set:

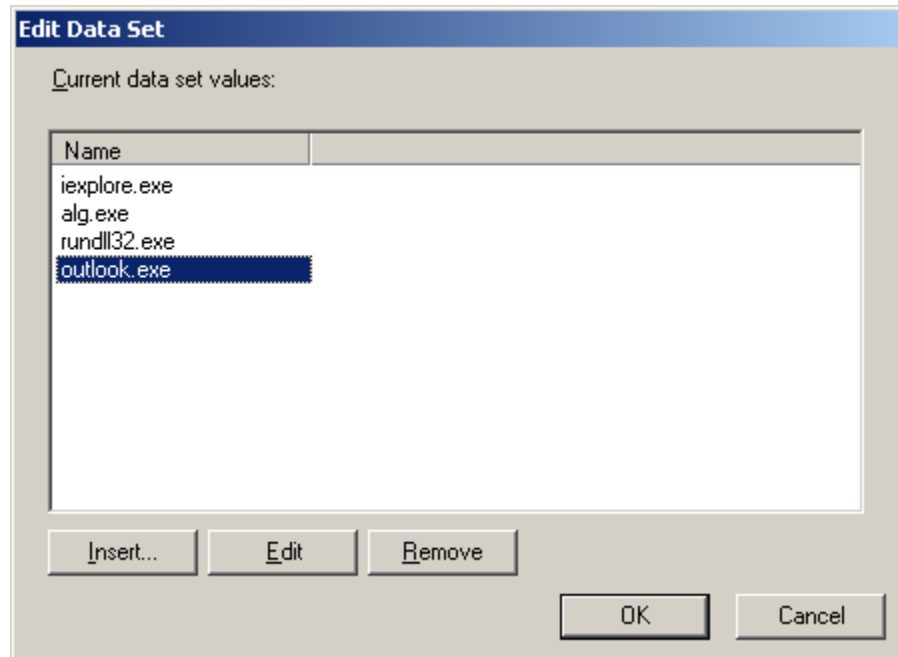
- Right click **Endpoint Analysis** in the console tree and select **Manage Data Set** from the action menu.



- 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**.

2. EXTENTRIX REGISTRY KEY SCAN

SCAN DESCRIPTION

Scan Name: Extentrix Registry Key.

Description: It allows IT administrators to scan the client's machine and verify whether a specified registry key/value is registered on that machine or not.

Parameters:

- Base Registry Key: specifies the base registry key.
- Sub Key: specifies the sub key ex: Software\Extentrix.
- Value Name: specifies the name of the value (NULL if you are looking for a key).
- Value Type: specifies the type of the value (NULL if you are looking for a key).
- Value Data: specifies the data of the value (NULL if you are looking for a key). Data could be REG_SZ → String, REG_BINARY → Binary, REG_DWORD → Double Word.

Note: If the data is binary or dword, it should be written as hexadecimal without space ex:05f47e.

Note: If the data is string, then the WILD CHARACTER (?,*) is supported as well as the exact string.

Scan Output:

- Allow Access - a Boolean output which indicates whether the key or the value is registered on the client's machine or not.
 - TRUE – indicates that a given key/value is registered on the client's machine.
 - FALSE – indicates that a given key/value is not registered on the client's machine or contains wrong information.
- 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.

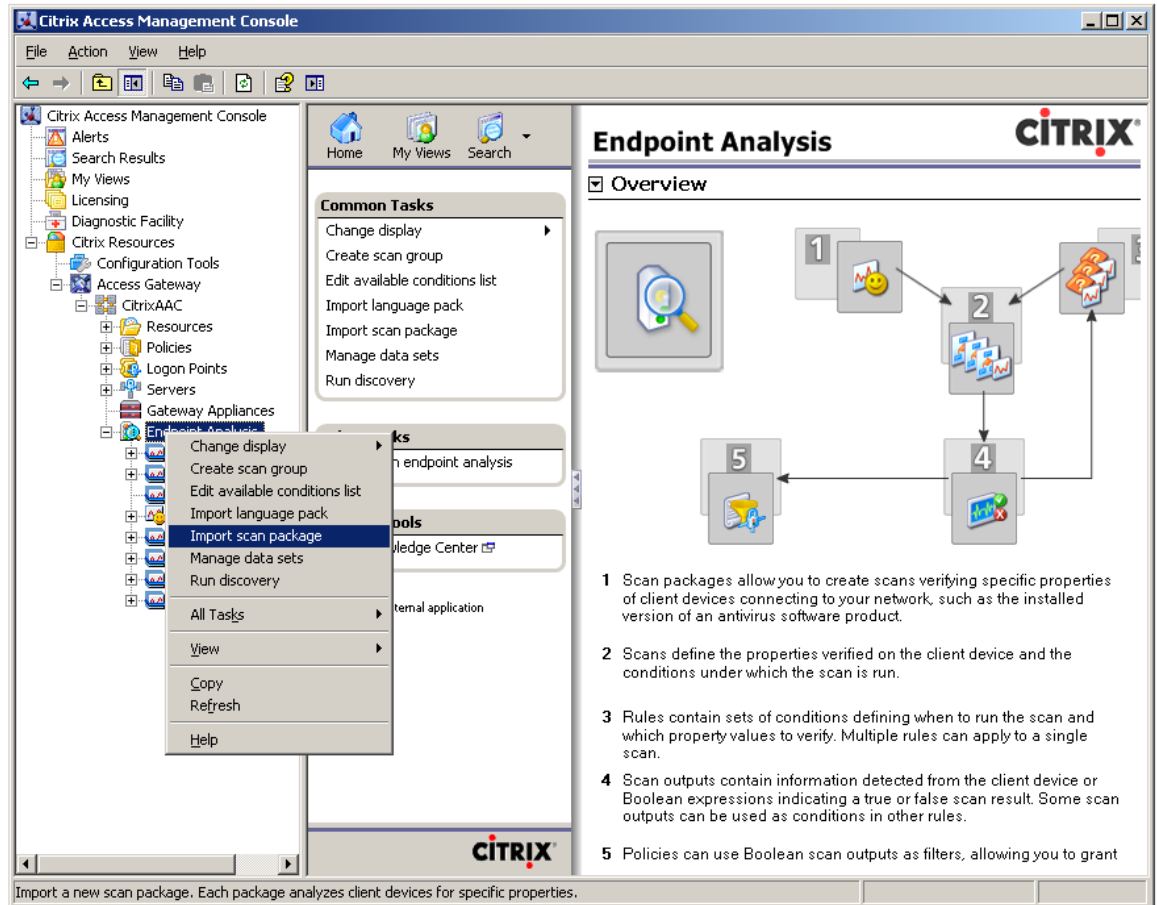
Note: If the License Status has an Invalid License value, the Allow Access will be false.

INSTALLATION AND CONFIGURATION

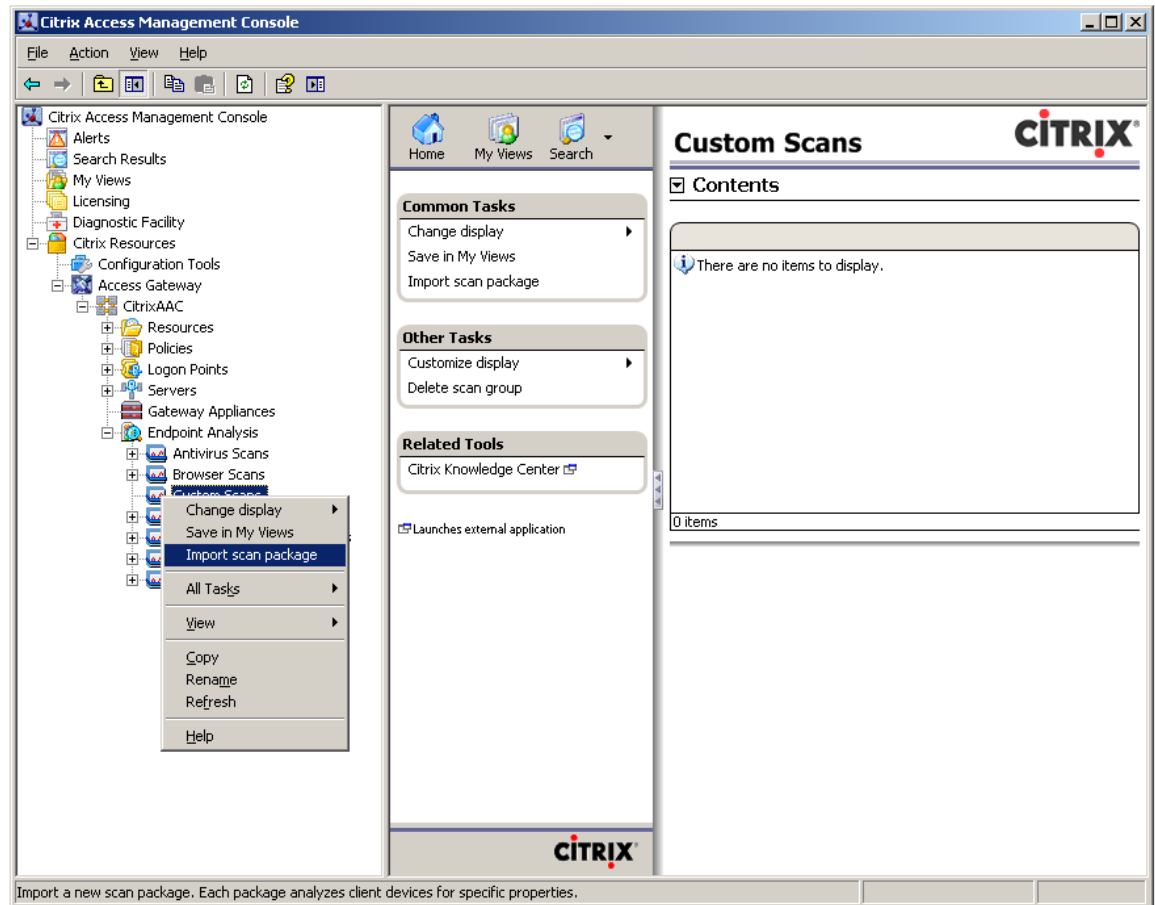
IMPORTING SCAN PACKAGES

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

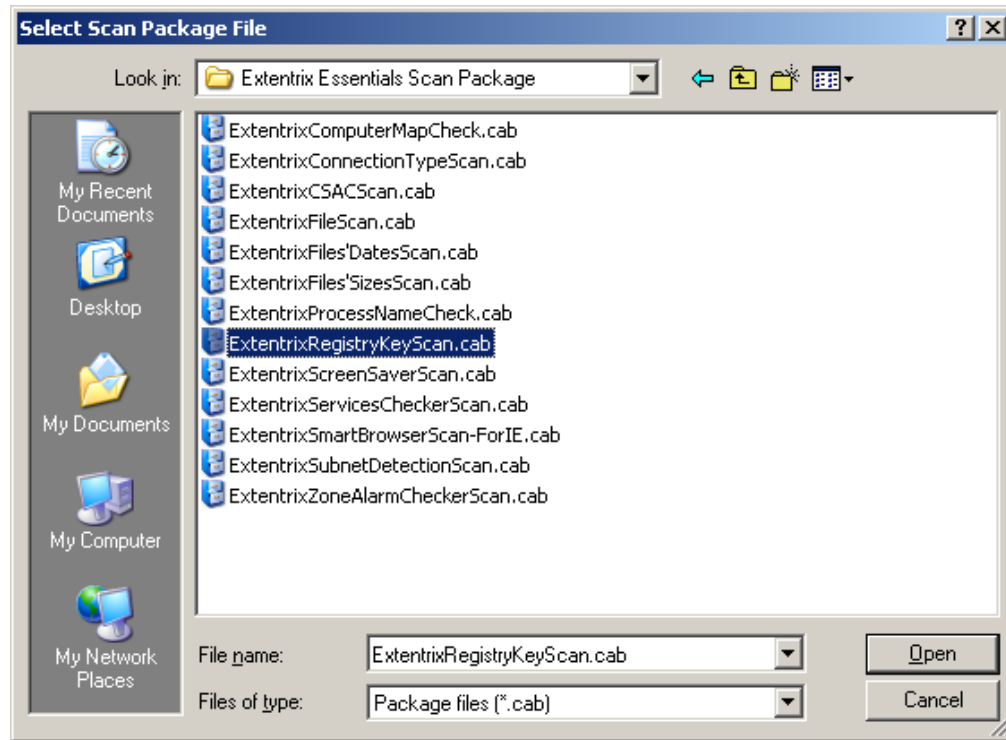
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



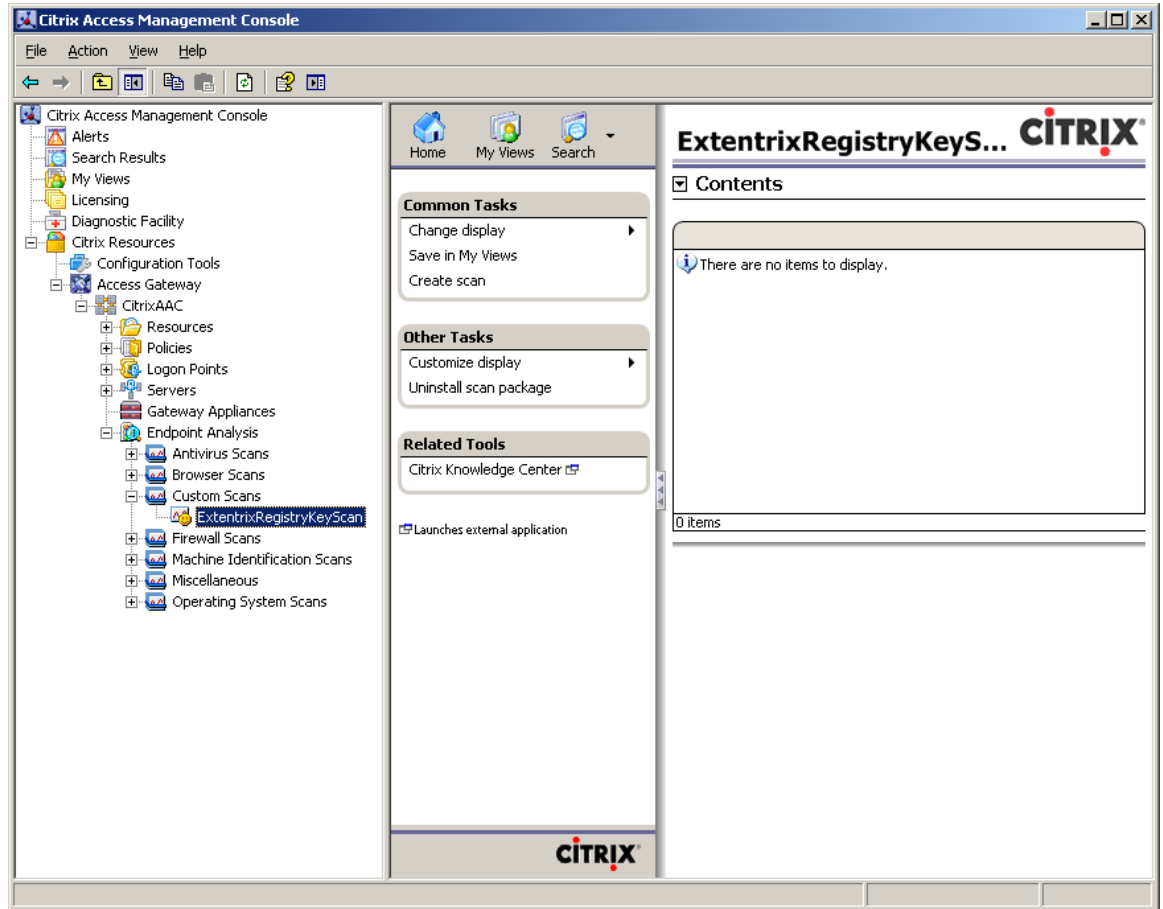
Also you can choose to insert the scan package to any scan category listed in the tree as shown in the following picture:



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



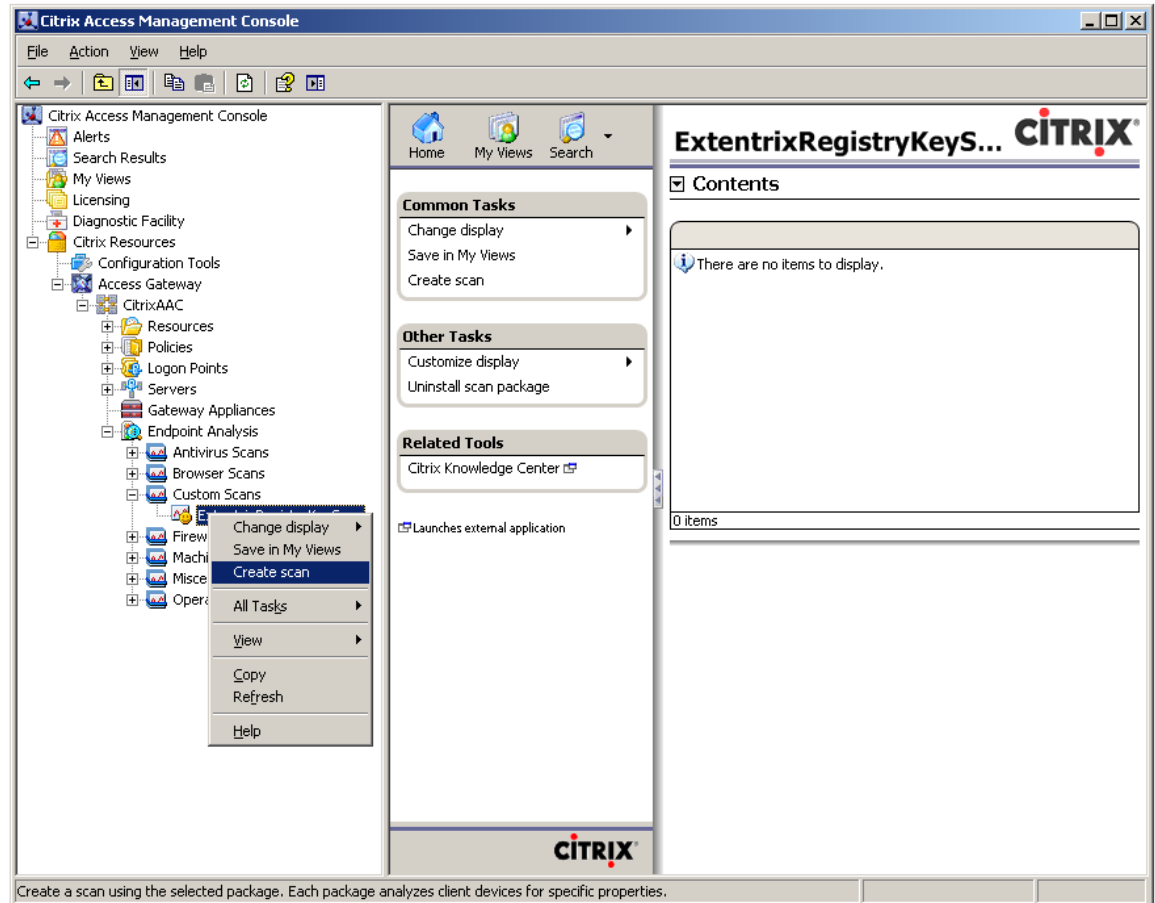
The package will be displayed in the console as shown in the following picture:



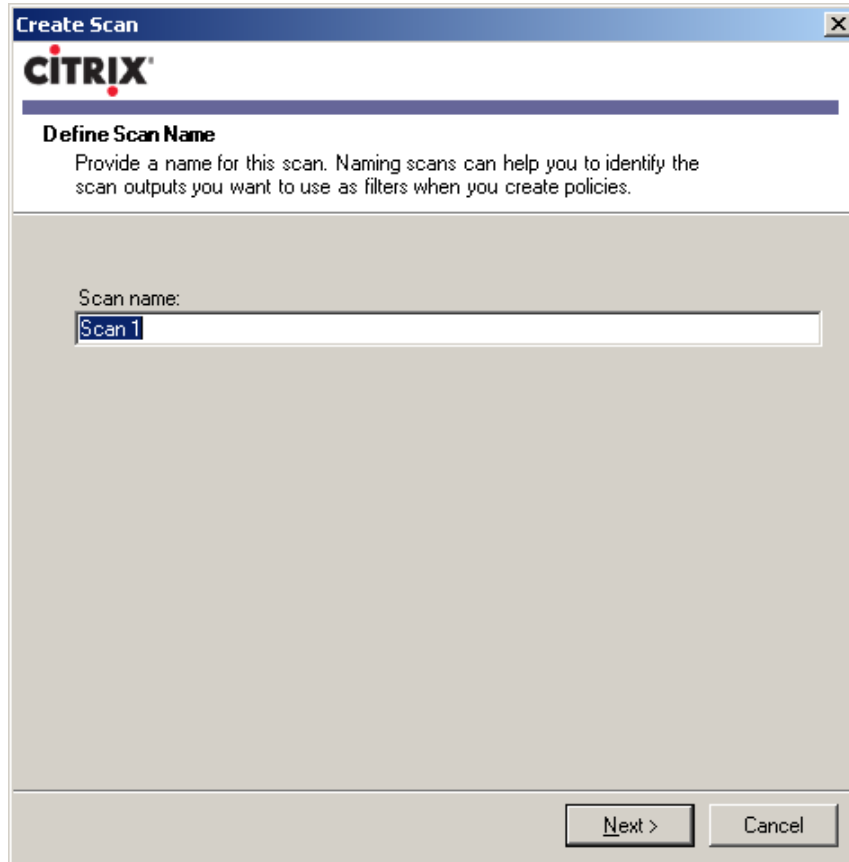
INSTALLING THE SCAN PACKAGE

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

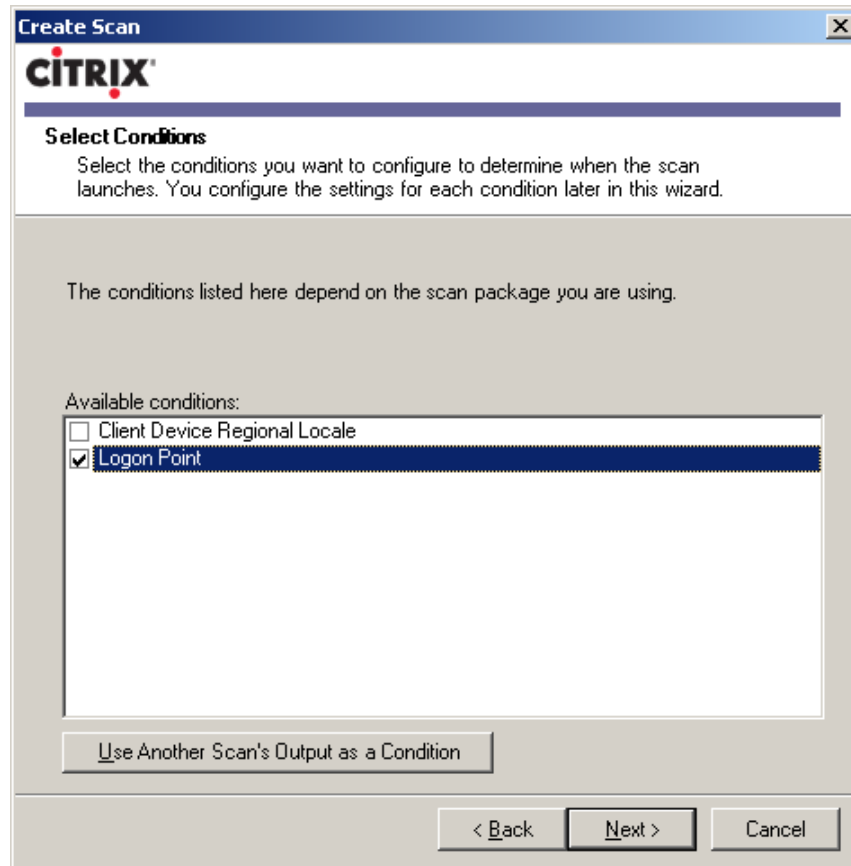
1. Select **ExtentrixRegistryKeyScan** to create scan for it, right click the icon and choose **Create Scan**.



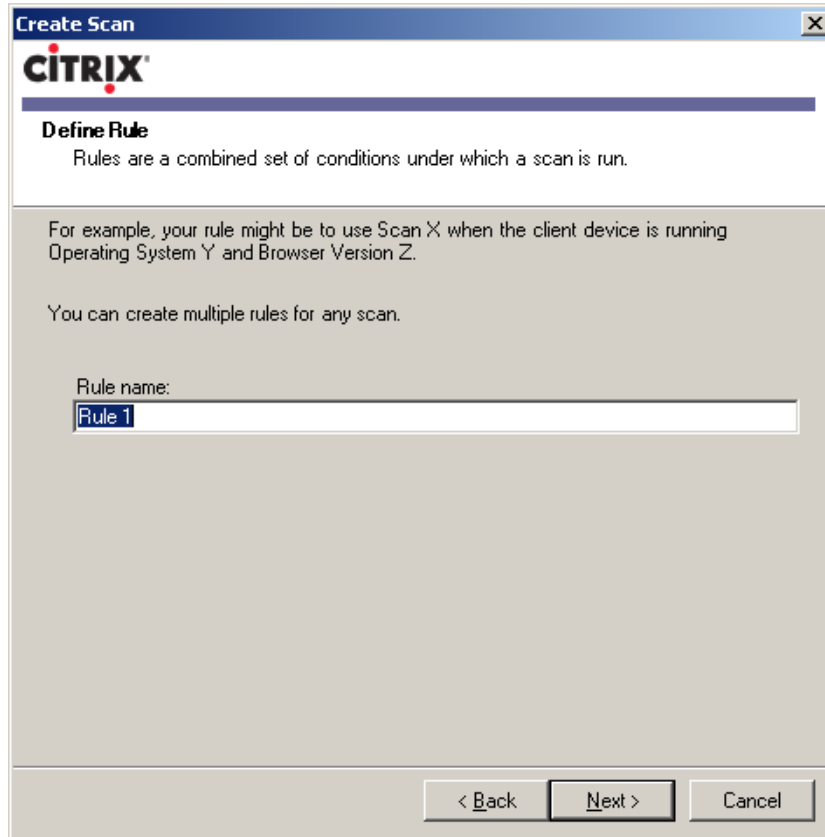
2. Type a name for the scan:

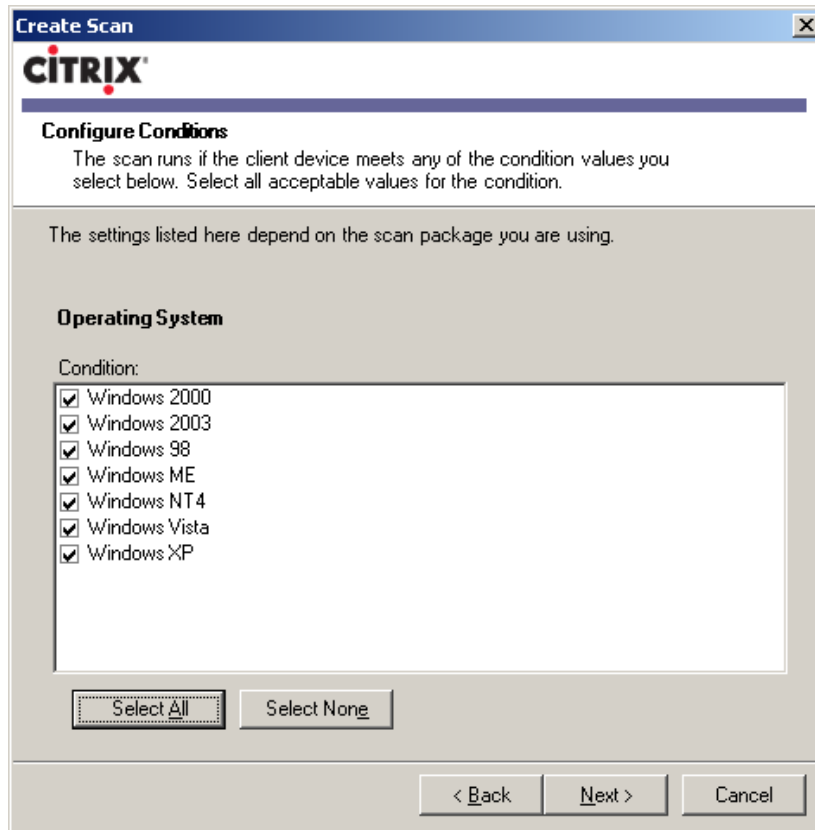


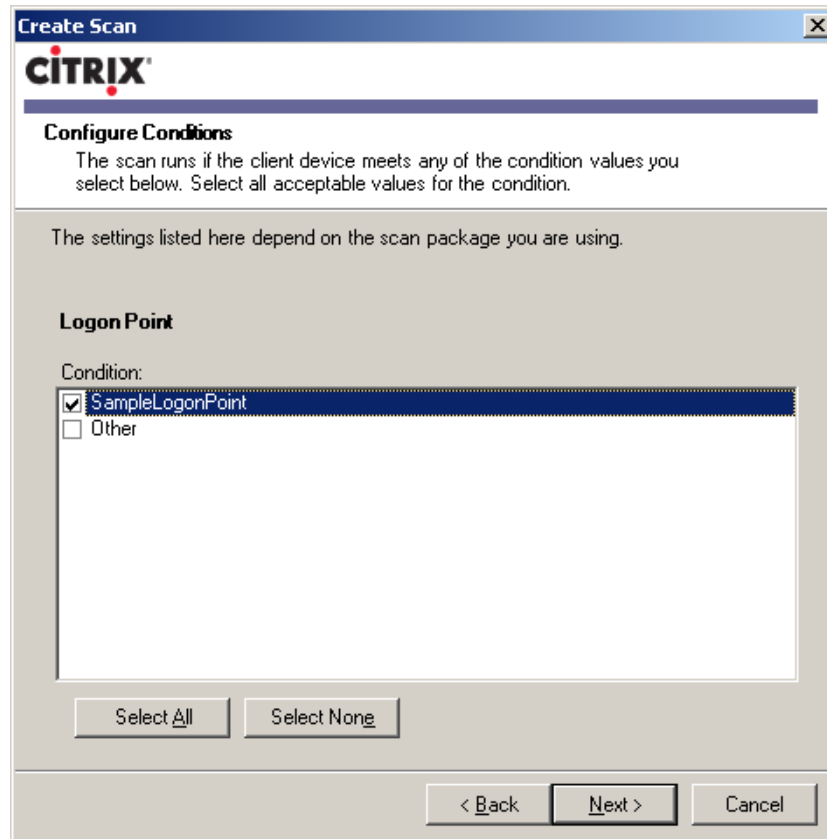
3. Set the scan conditions:



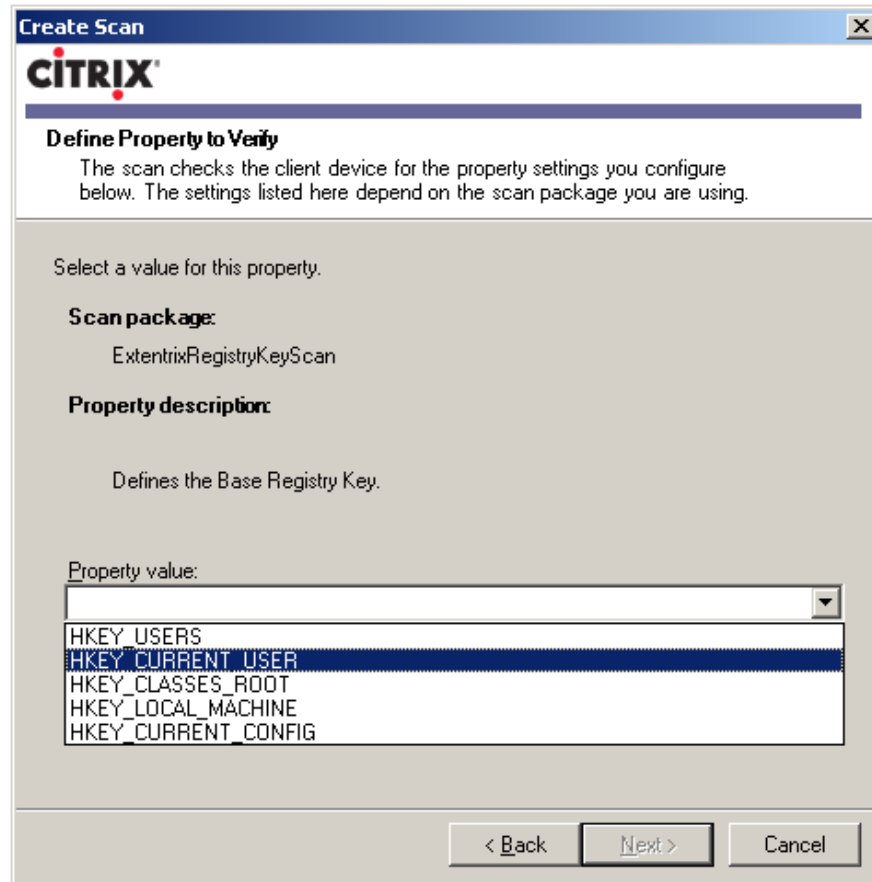
4. Type rule name and set rule conditions:



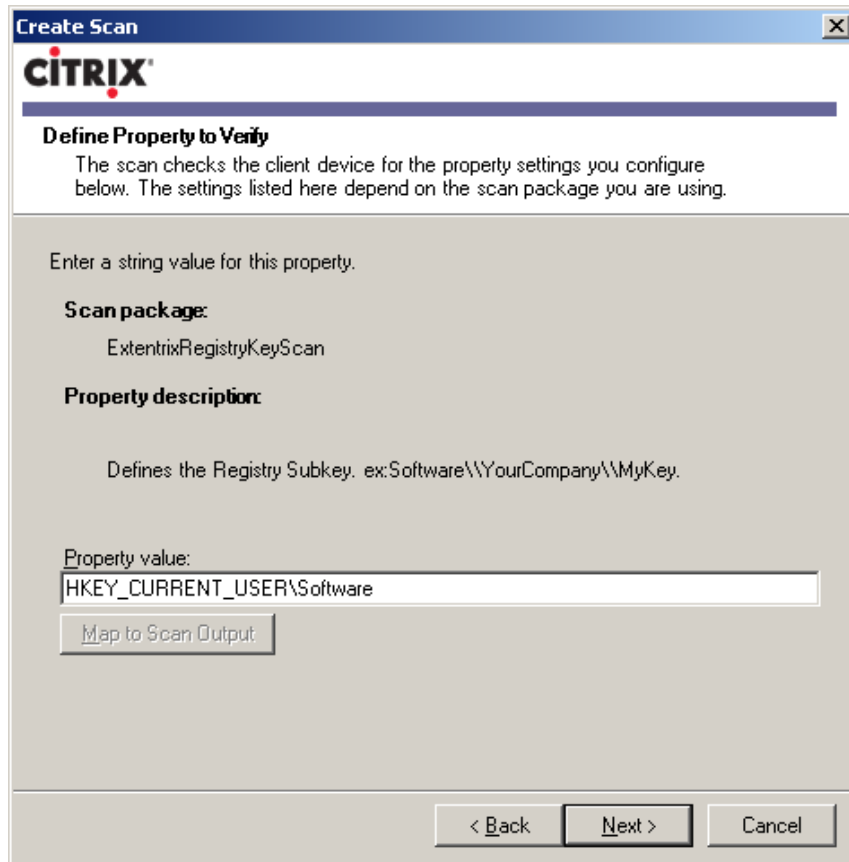




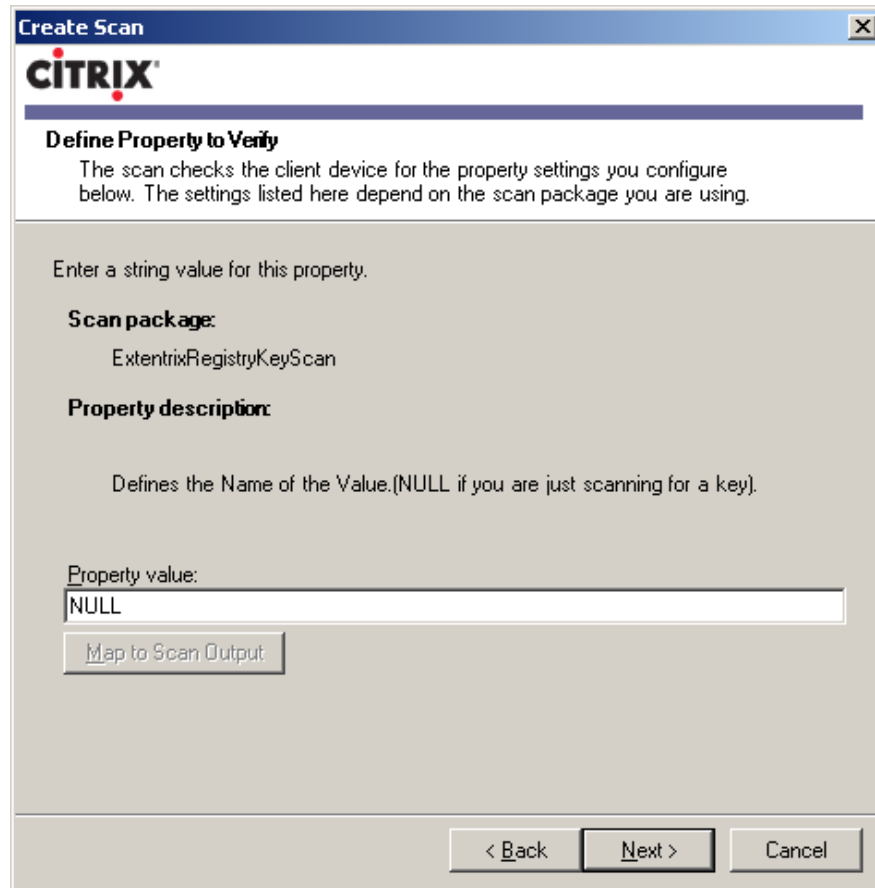
5. Choose a base registry key from the list:



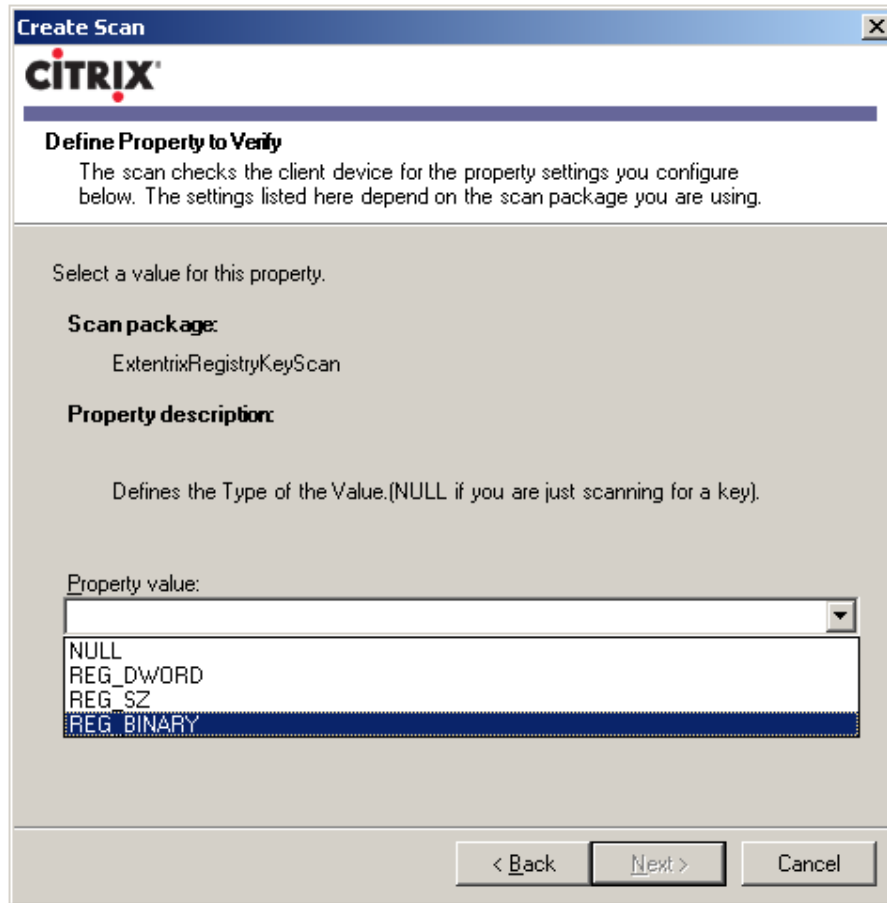
6. Type the sub key to be checked.



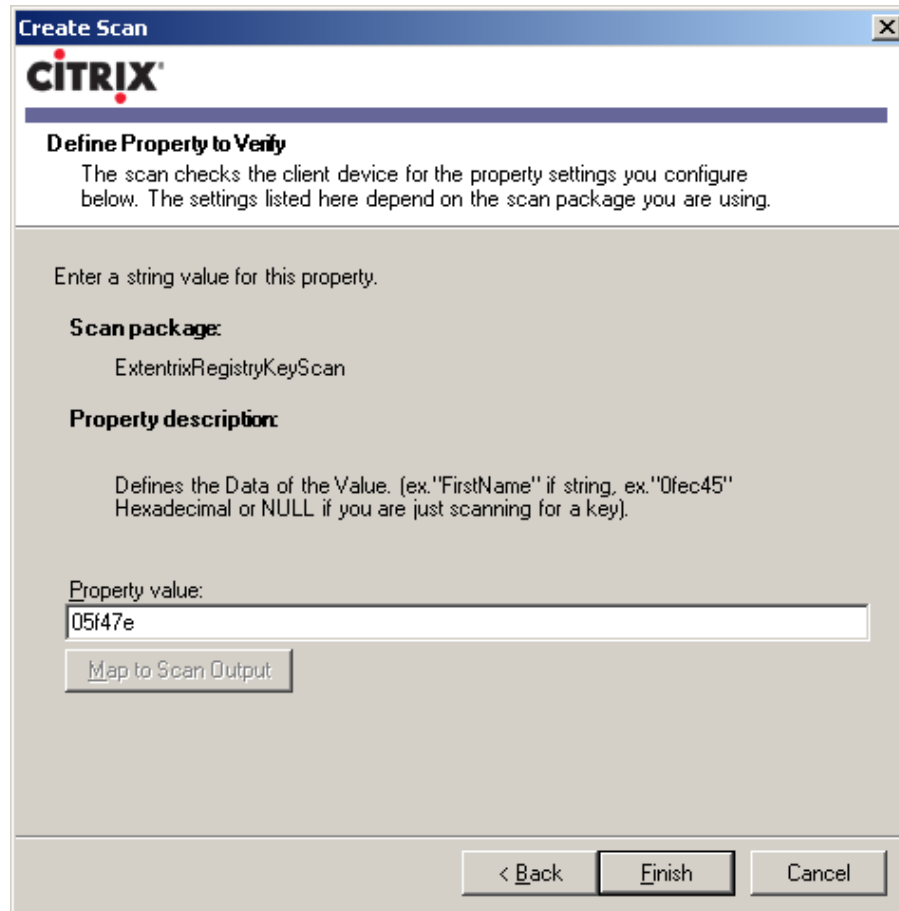
7. Type the Value Name if you will check the value or NULL if you will not.



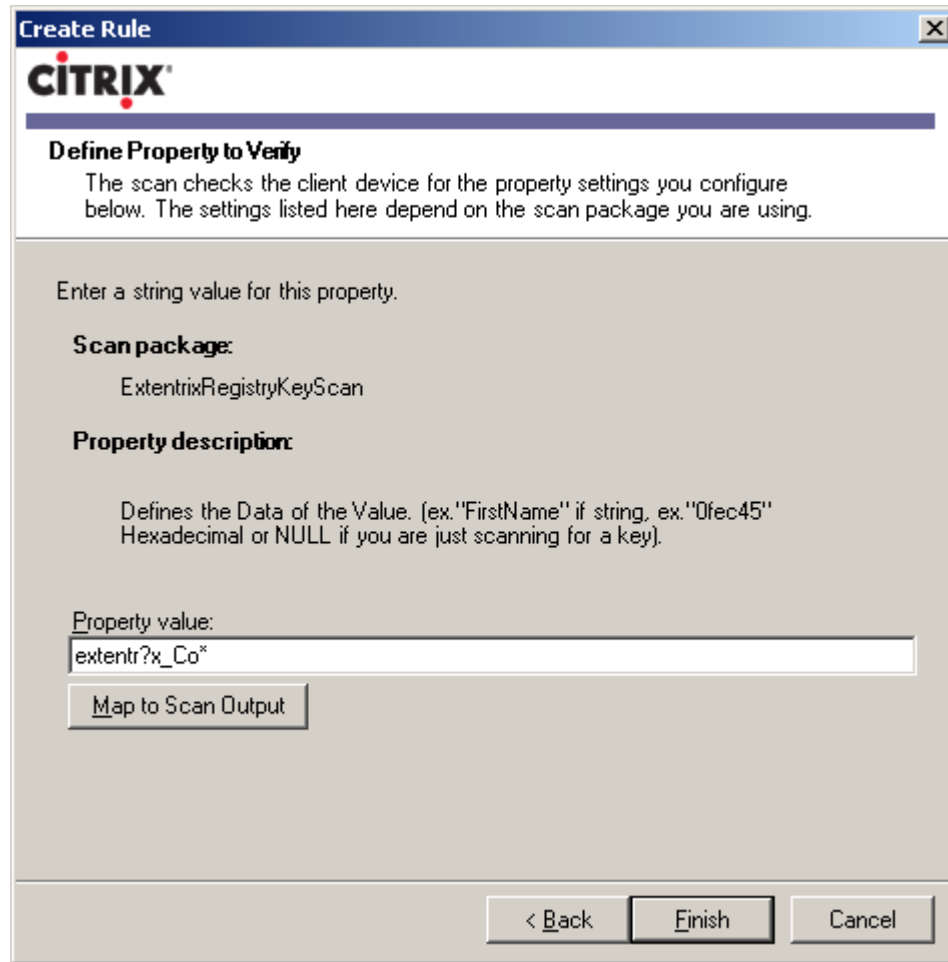
8. Choose the Type of the data from the list:



9. Type the data of the value: if the data is binary or dword it should be written as hexadecimal without space ex: 05f47e.



And if the data type is string then you can use wild char.



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

3. EXTENTRIX SCREEN SAVER SCAN

SCAN DESCRIPTION

Scan Name: Extentrix Screen Saver.

Description: IT administrators may require that the clients accessing their resources have screen saver on their machines for security purposes. This scan allows the admins to scan the client's machine and check for the presence of the Screen Saver and whether it is password protected or not.

Parameter:

- Check both Conditions: True value to detect the presence of the screen saver and if it is password protected, and False value to detect the presence of the screen saver only.

Scan Output:

- Allow Access - a Boolean output which indicates whether the Screen Saver exists and whether it is password protected or not.

TRUE – indicates that all conditions are satisfied on the client's machine.

FALSE – indicates that at least one condition is not satisfied on the client's machine.

- 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.

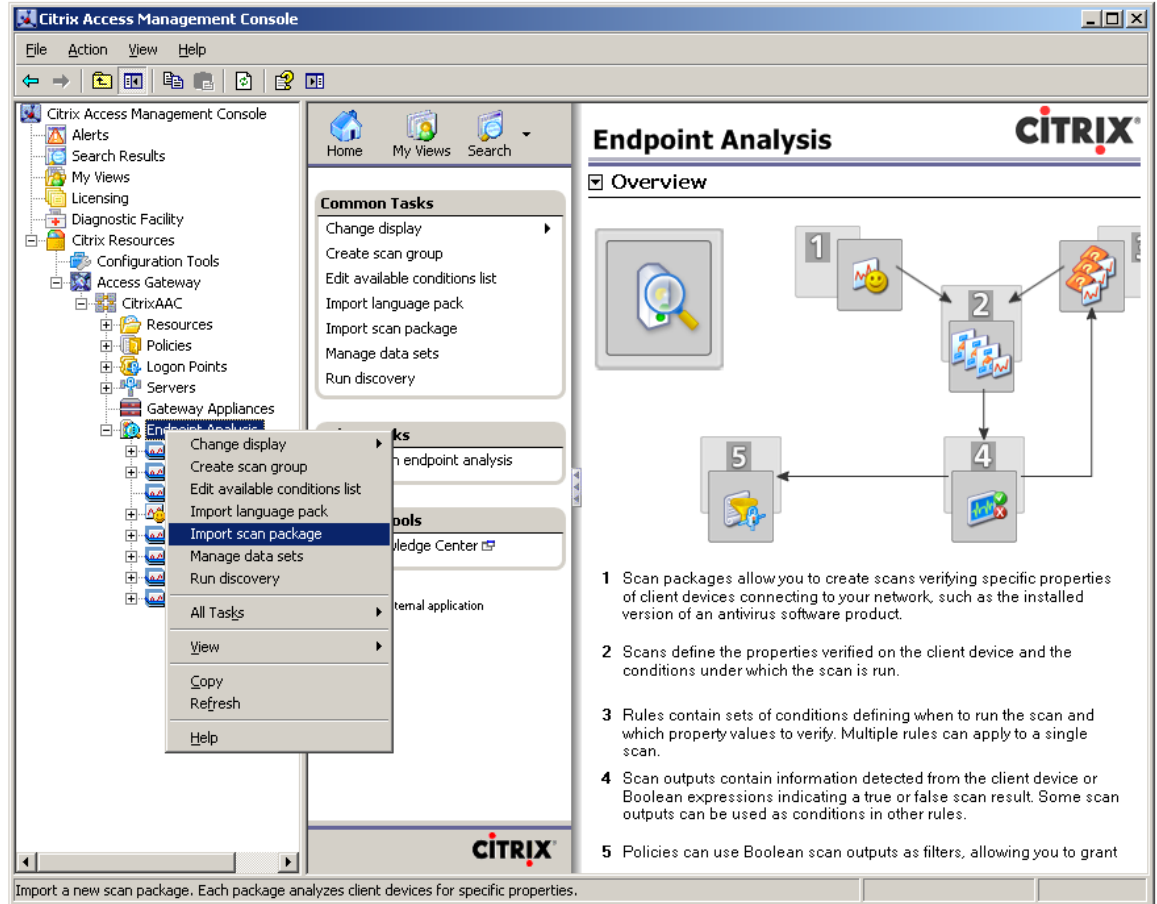
VALID LICENSE – indicates that the scan is licensed.

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

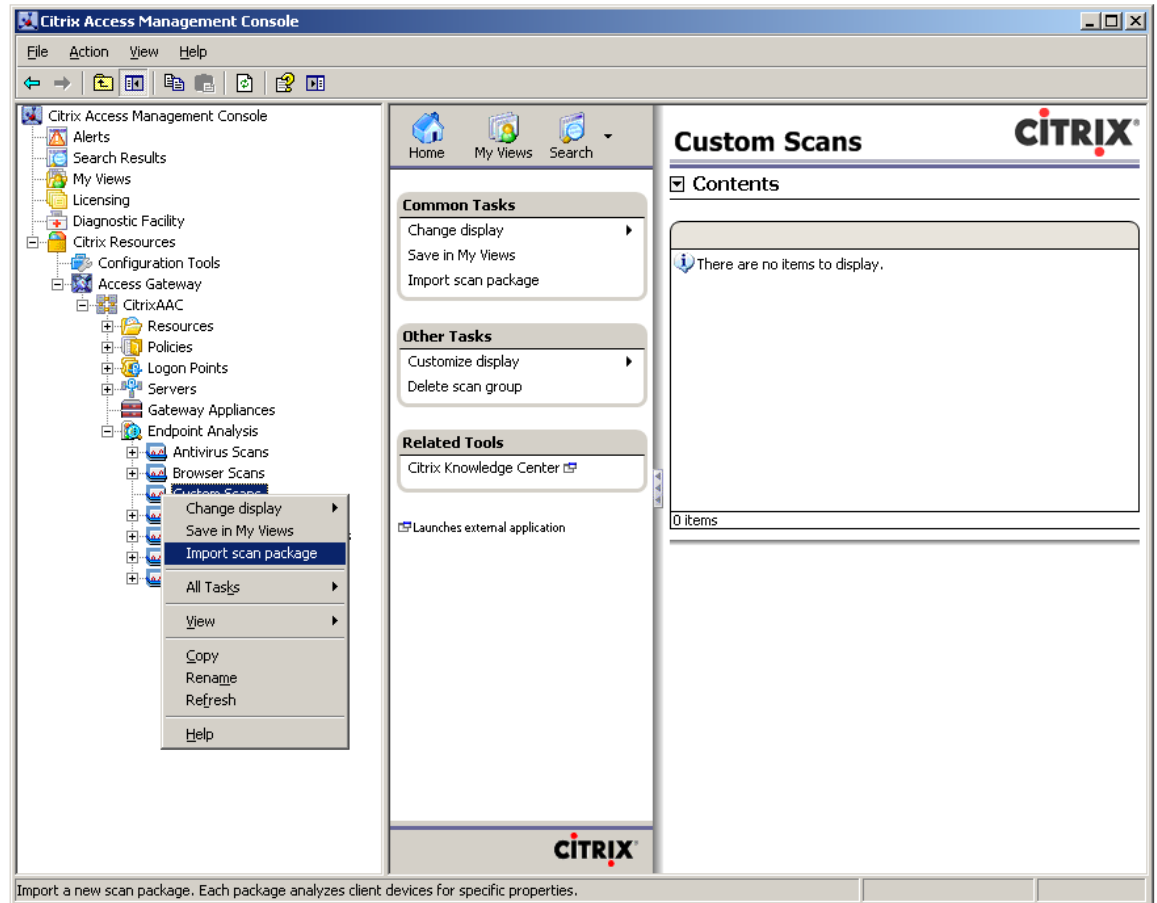
IMPORTING SCAN PACKAGES

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

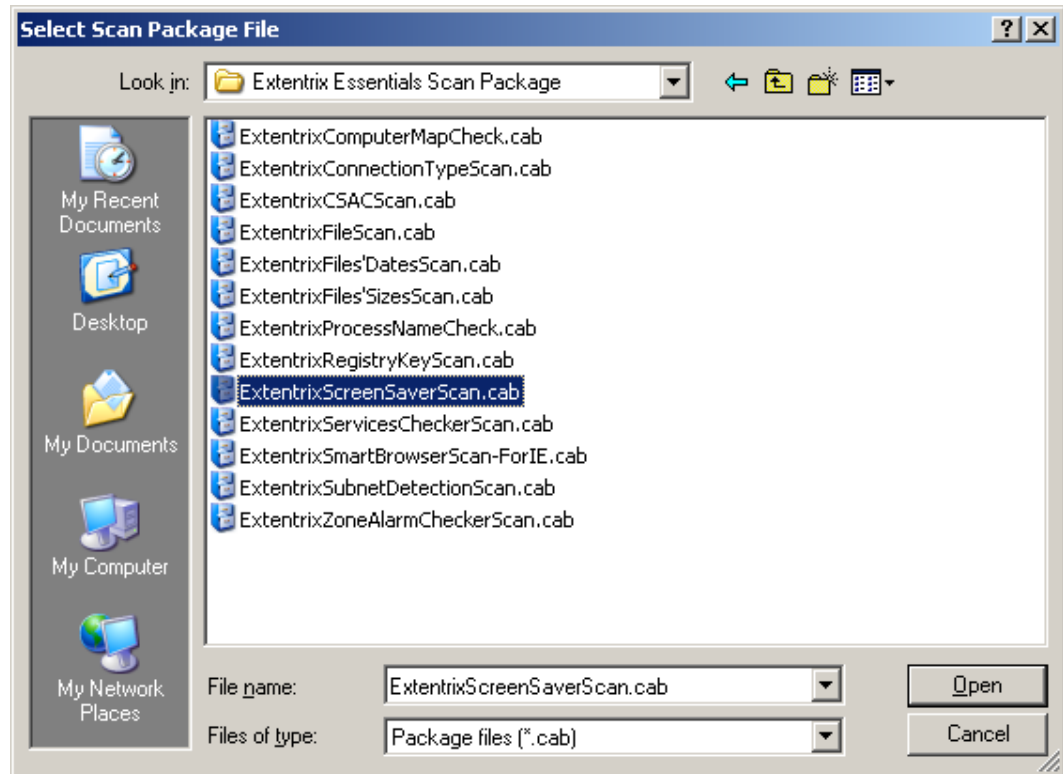
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



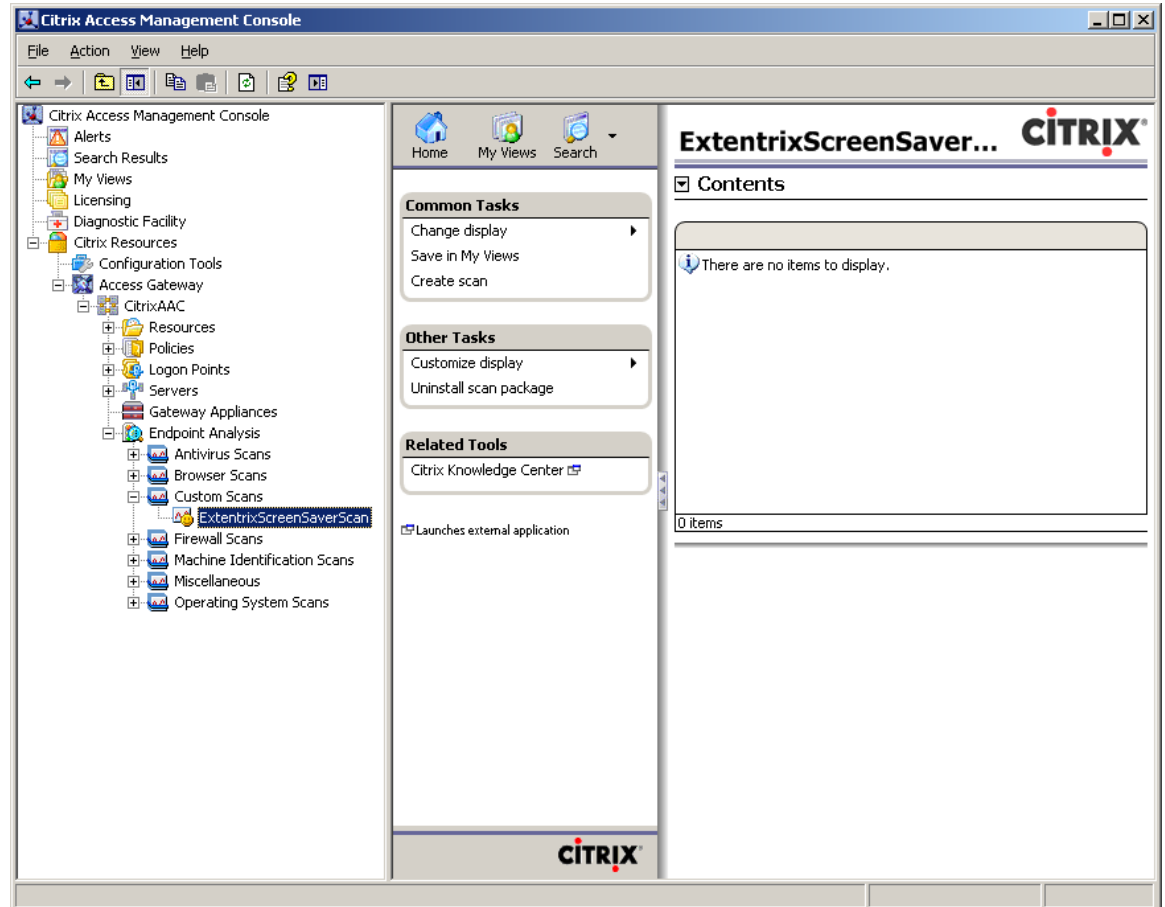
Also you can choose to insert the scan package to any scan category listed in the tree as shown in the following picture:



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



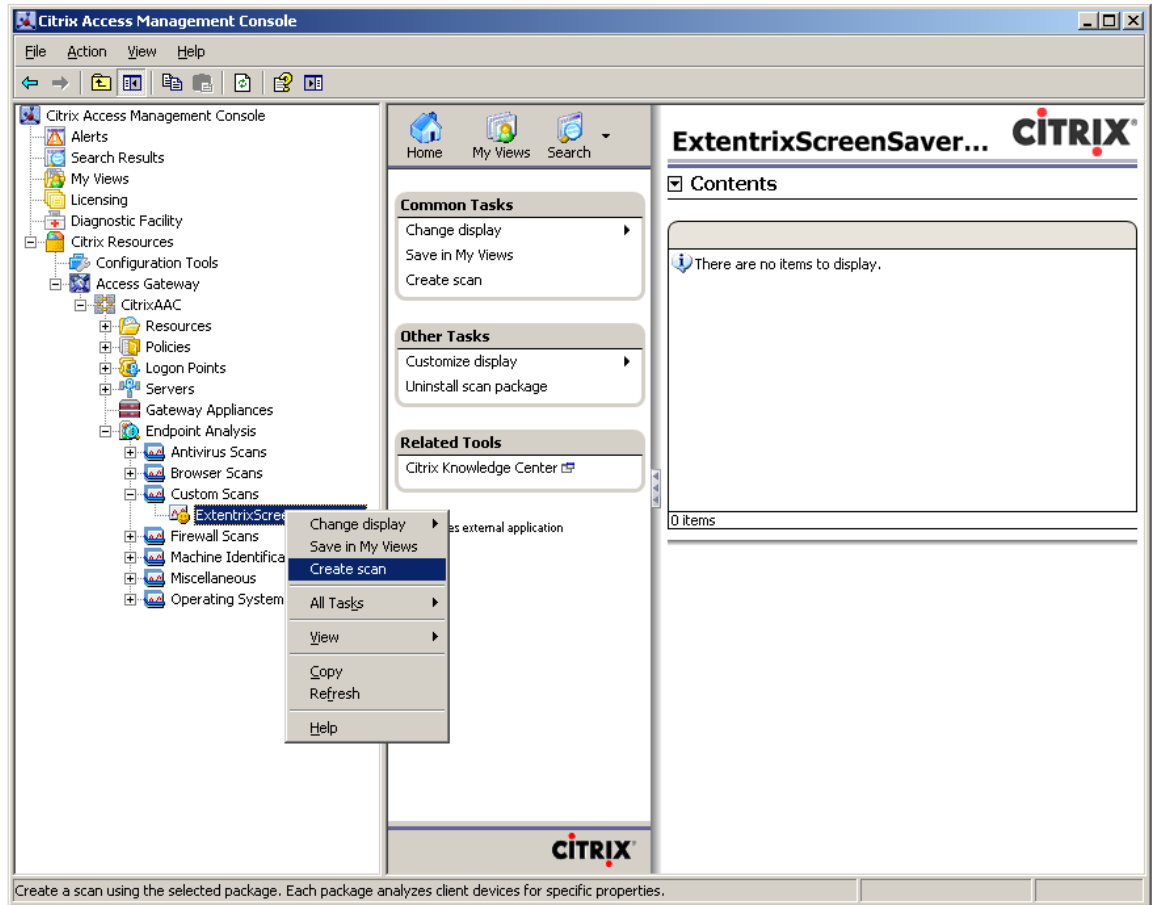
The package will be displayed in the console as shown in the following picture:



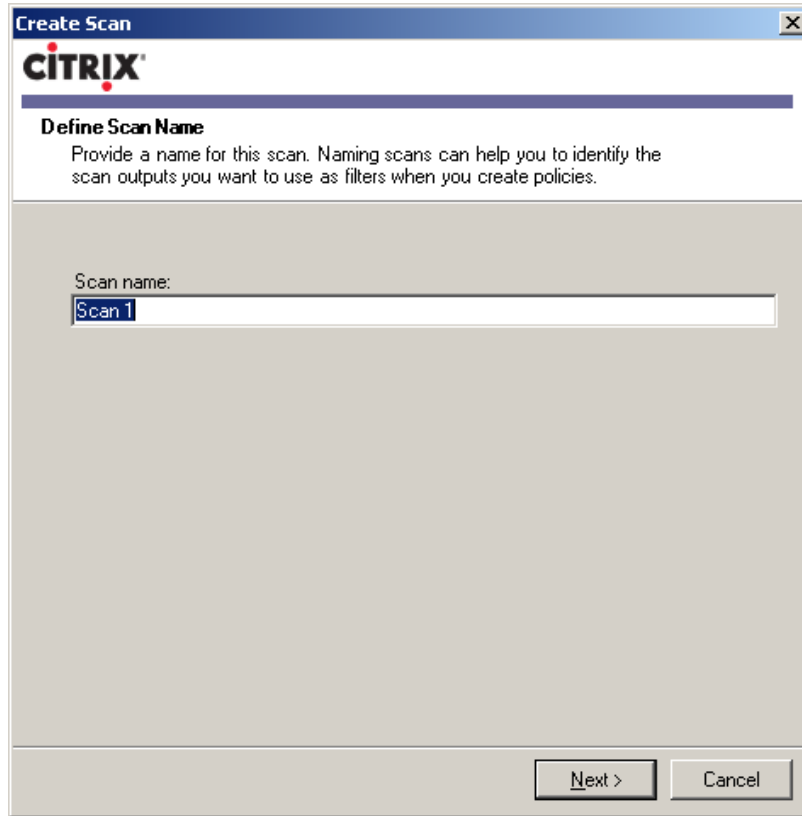
INSTALLING THE SCAN PACKAGE

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

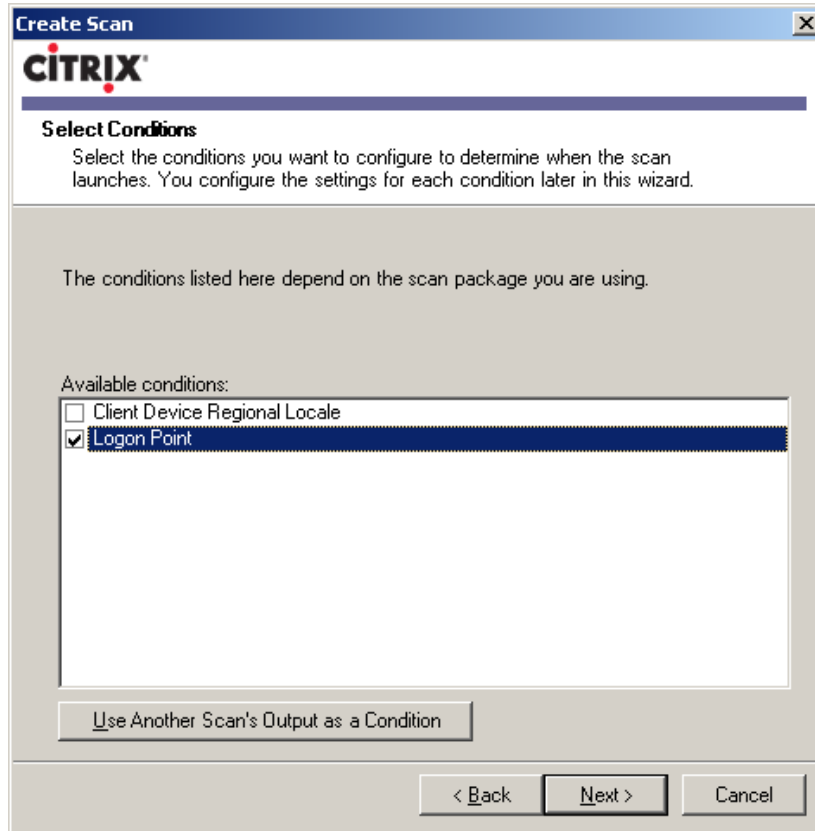
1. Select **ExtentrixScreenSaverScan** to create scan for it, right click the icon and choose **Create Scan**.



2. Type a name for the scan:



3. Set the scan conditions:



4. Type rule name and set rule conditions:

Create Scan

CITRIX

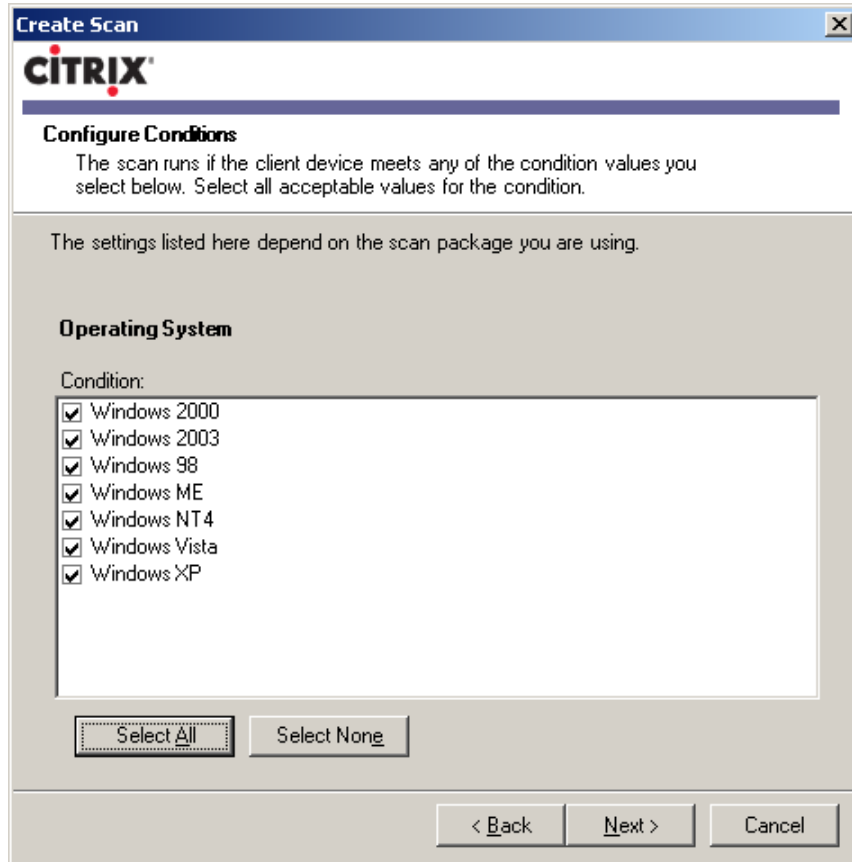
Define Rule
Rules are a combined set of conditions under which a scan is run.

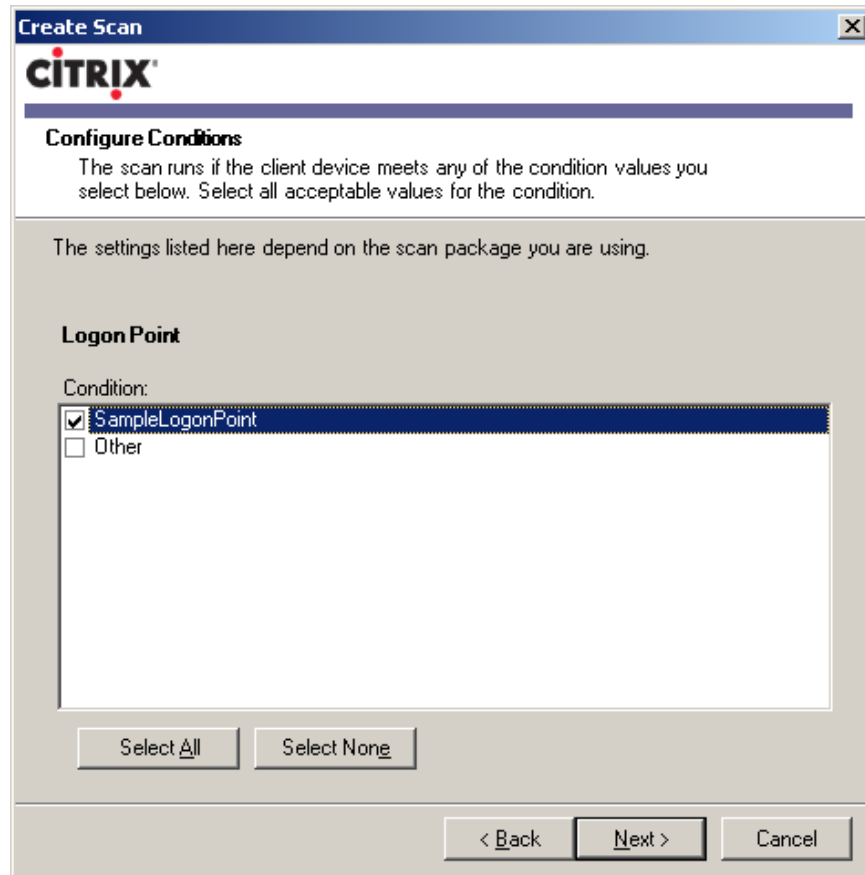
For example, your rule might be to use Scan X when the client device is running Operating System Y and Browser Version Z.

You can create multiple rules for any scan.

Rule name:

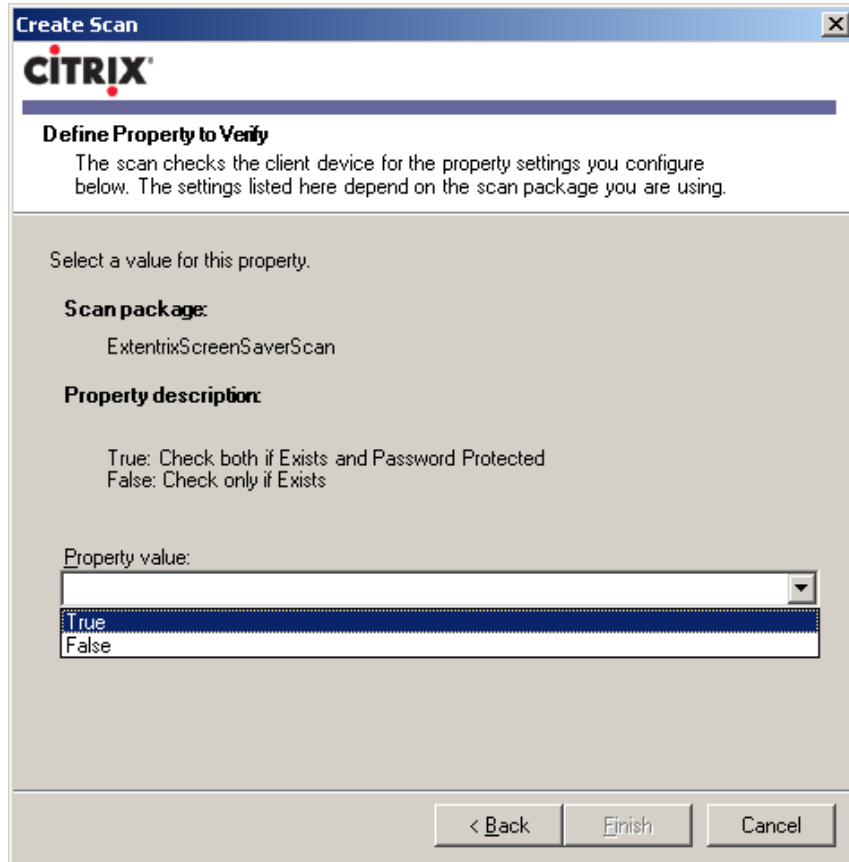
< Back Next > Cancel





5. Choose the desired condition to take one of two scenarios:

- First Scenario: Detects the presence of the screen saver and if it is password protected. You should choose **True** option.
- Second Scenario: Detects the presence of the screen saver only. You should choose **False** option.



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

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.

Select a value for this property.

Scan package:
ExtentrixScreenSaverScan

Property description:
True: Check both if Exists and Password Protected
False: Check only if Exists

Property value:
True

Map to Scan Output

< Back Finish Cancel

4. EXTENTRIX SERVICES CHECKER SCAN

SCAN DESCRIPTION

Scan Name: Extentrix Services Checker.

Description: This scan enables administrators to scan the client's machine and verify that the windows services specified by the administrator exist and running on the client's machine. For example, suppose that the administrator wants the windows service *W32Time* which stands for Windows Time Service to be running on the client machine. The user will be denied the access to XenApp if the scan result indicates that W32Time is not running.

Parameter:

- List of Services: Dataset type includes all of Services names to be checked if they exist and running.

Scan Output:

- Allow Access - a Boolean output which indicates whether all of the Services exist and running or not.

TRUE – indicates that all Services are running on the client's machine.

FALSE – indicates that at least one Service is not exist or is not running on the client's machine.
- 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.

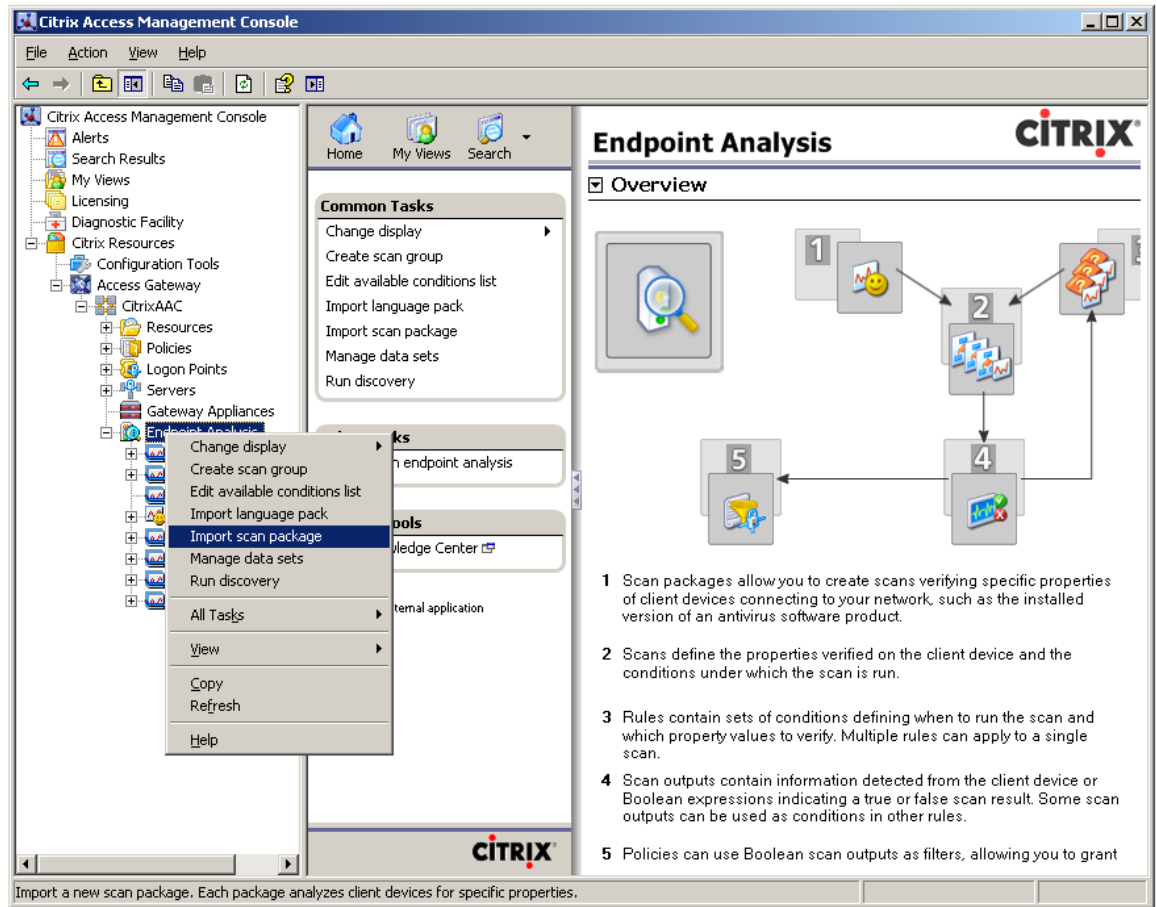
Note: If the License Status has an Invalid License value, the Allow Access will be false.

INSTALLATION AND CONFIGURATION

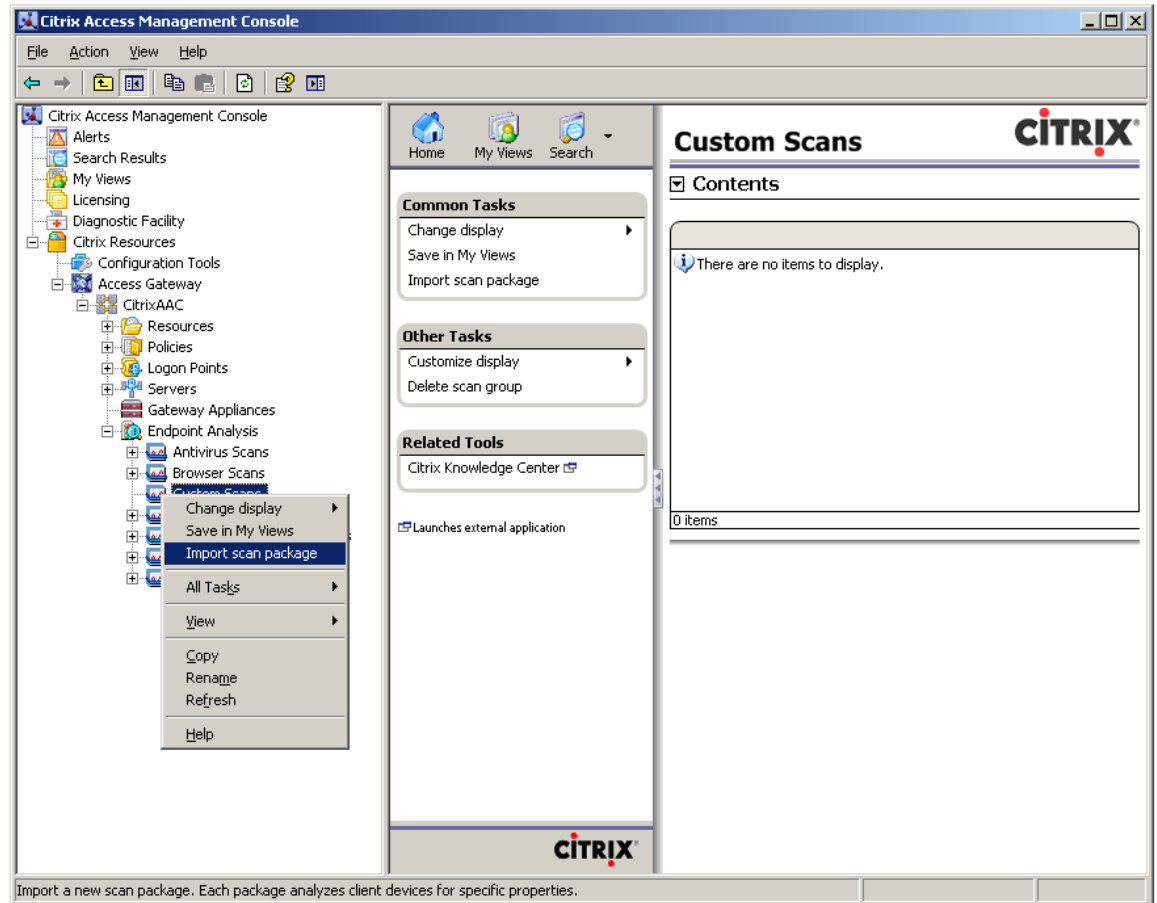
IMPORTING SCAN PACKAGES

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

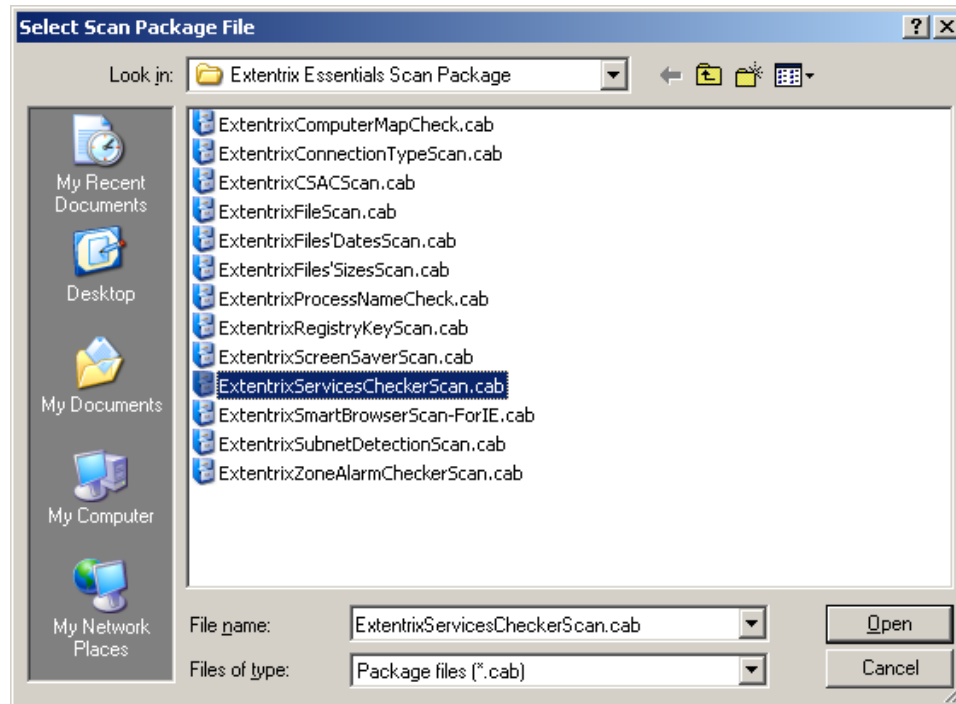
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



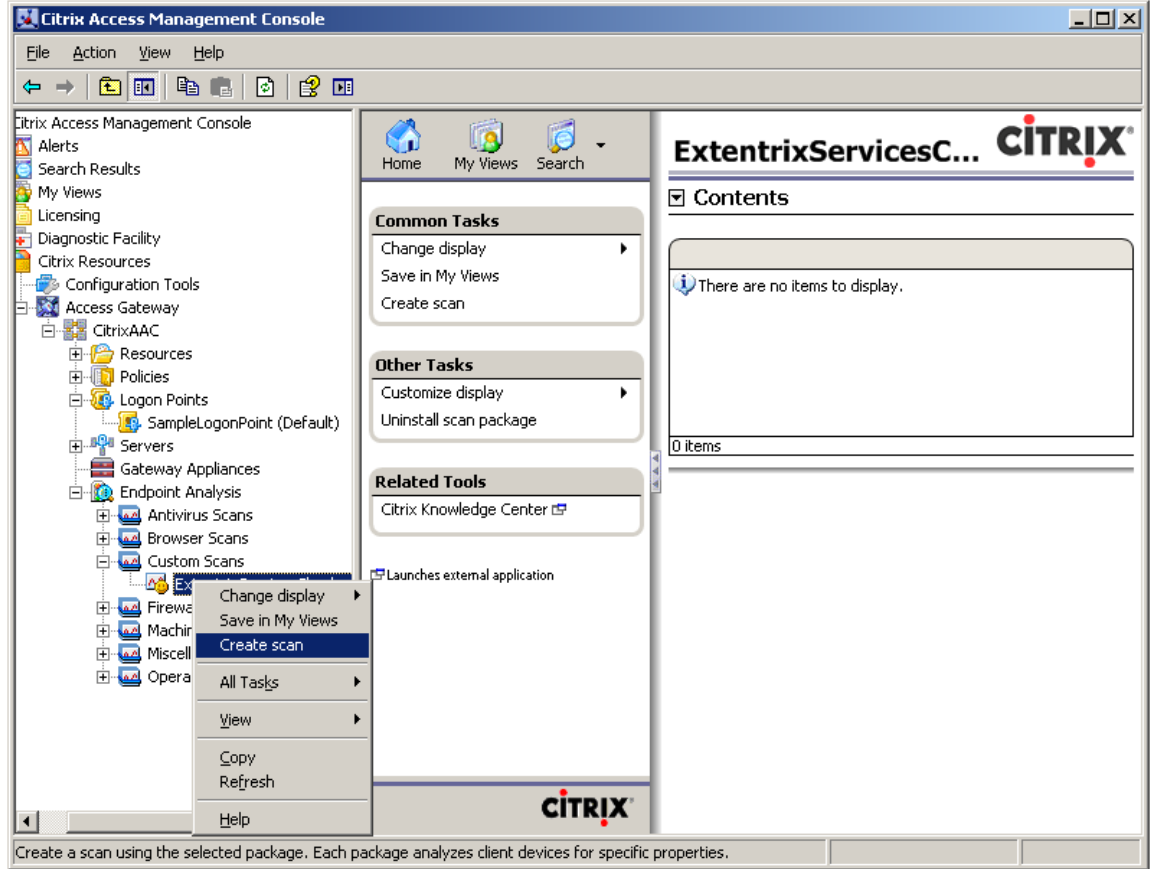
Also you can choose to insert the scan package to any scan category listed in the tree as shown in the following picture:



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



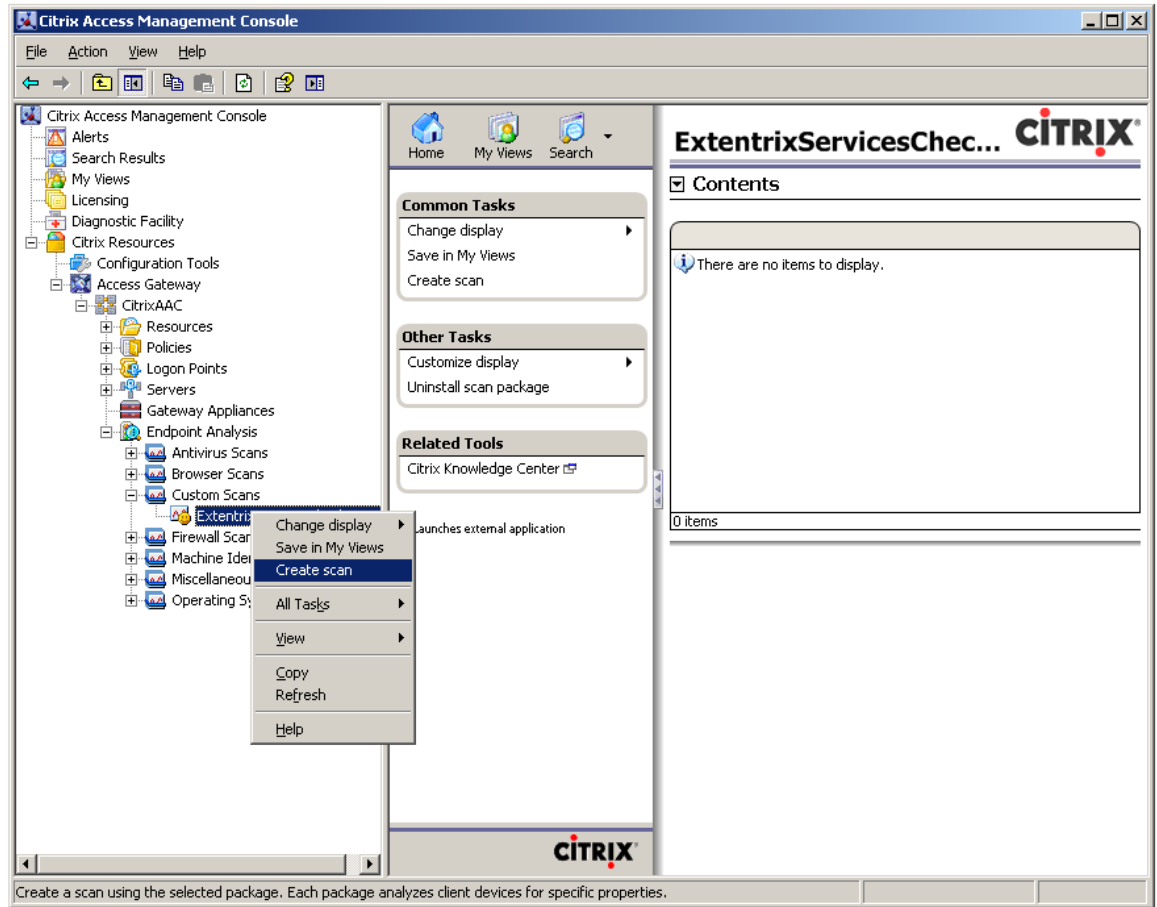
The package will be displayed in the console as shown in the following picture:



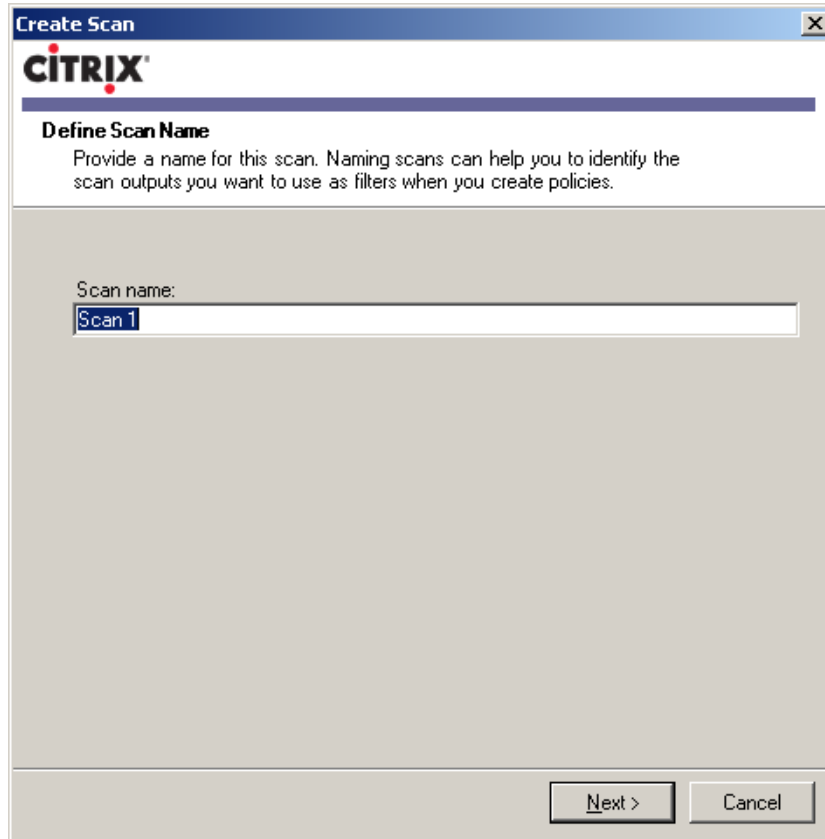
INSTALLING THE SCAN PACKAGE

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

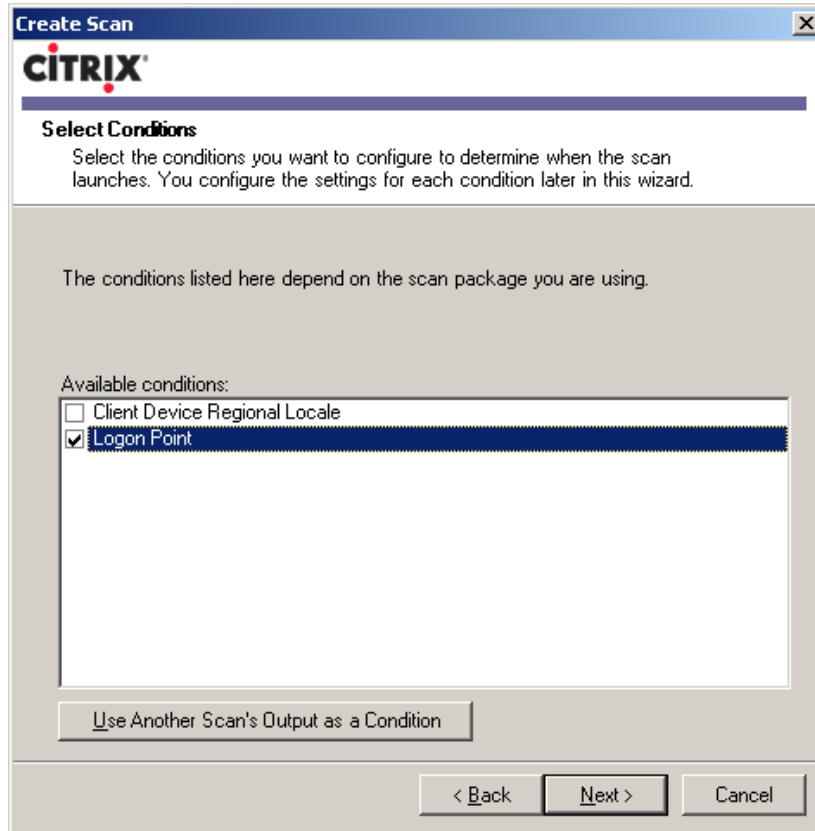
1. Select **ExtentrixServicesCheckerScan** to create scan for it, right click the icon and choose **Create Scan**.



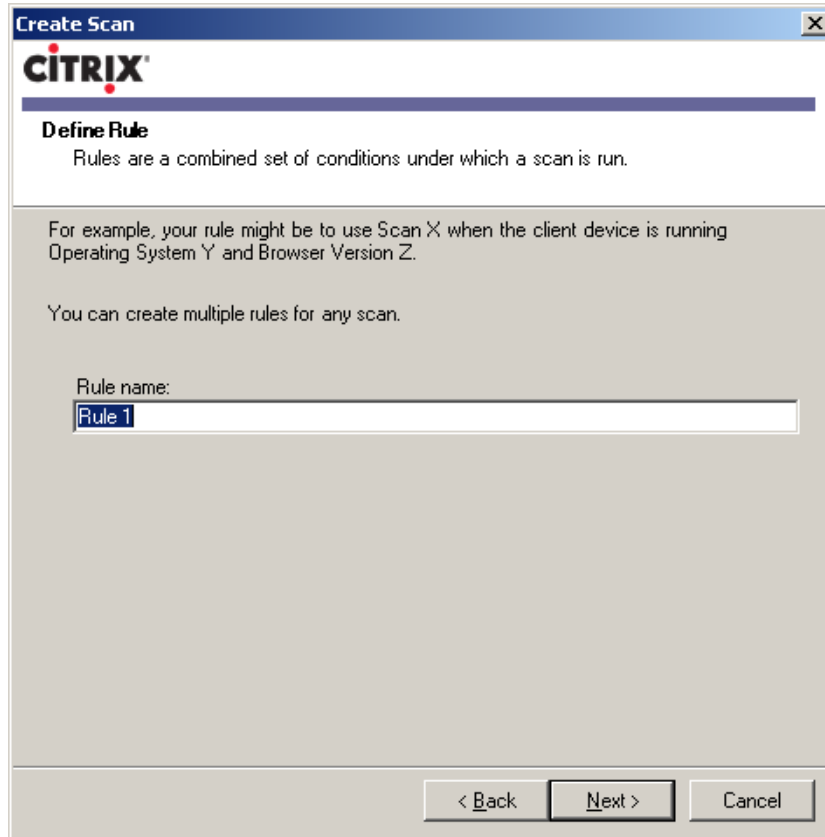
2. Type a name for the scan:

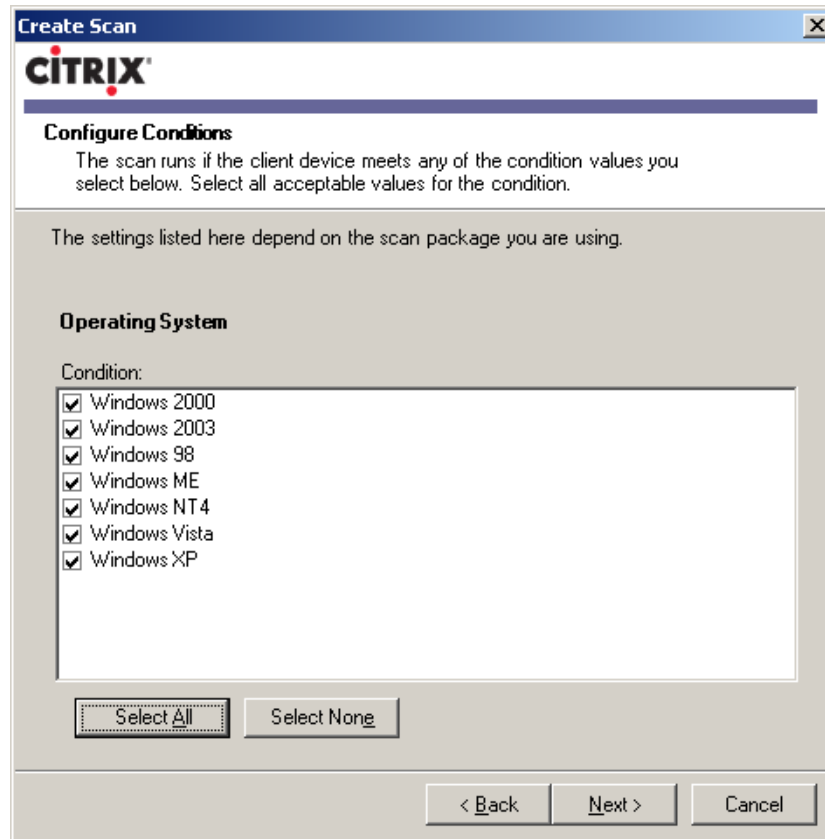


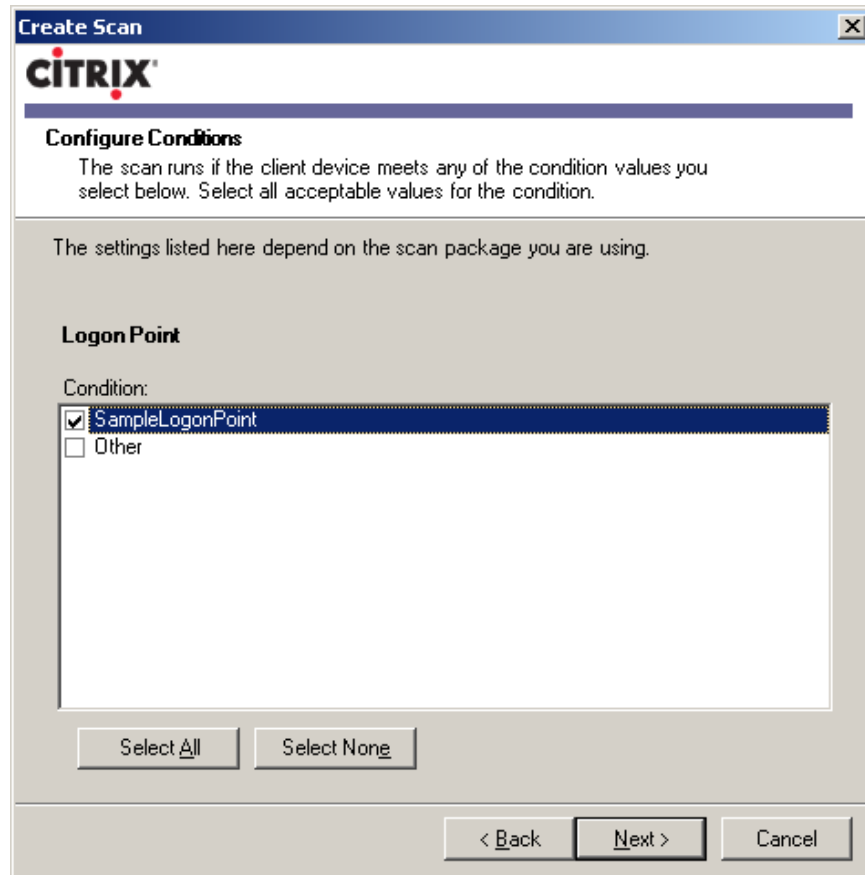
3. Set the scan conditions:



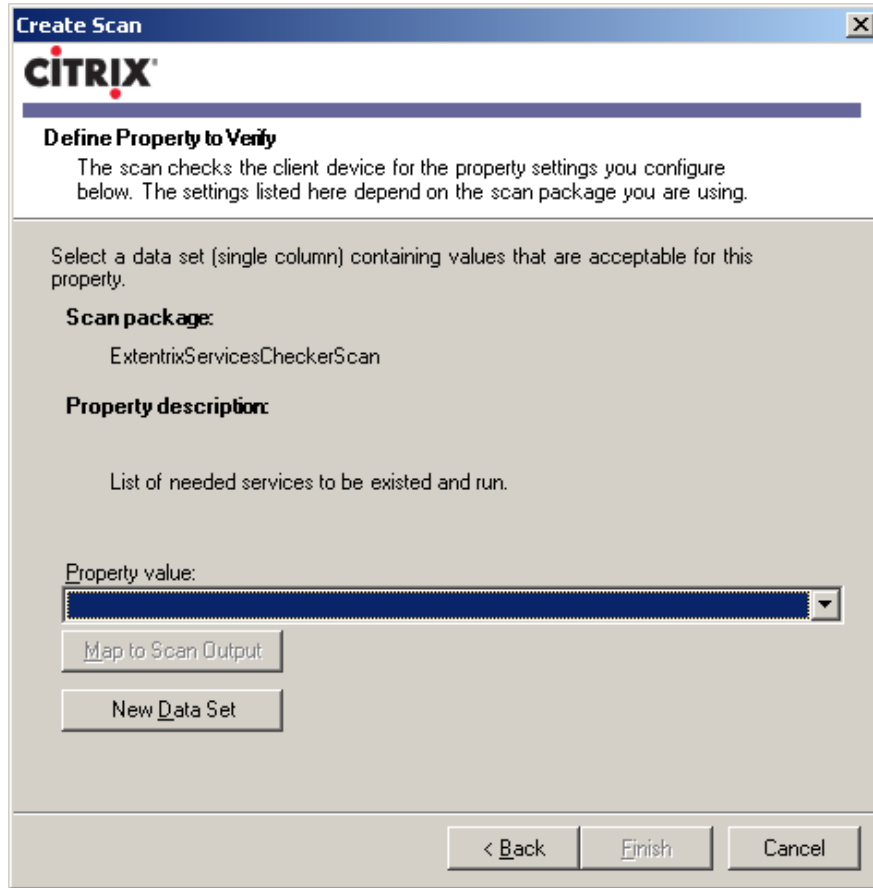
4. Type rule name and set rule conditions:



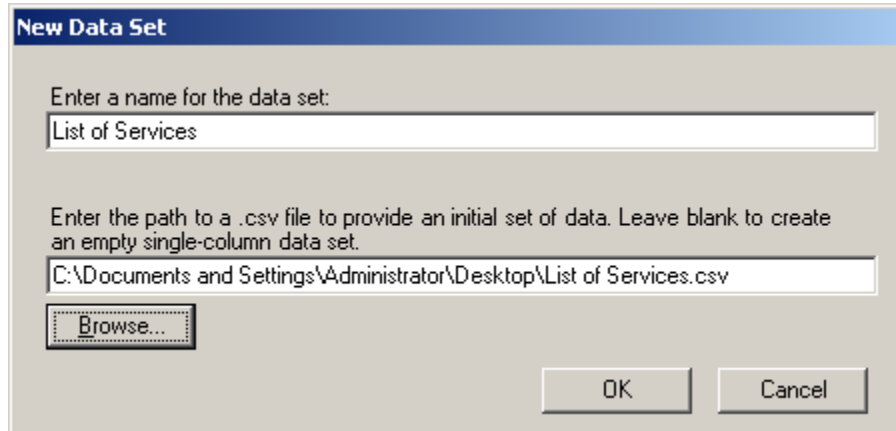




5. Define a data set using a comma delimited .csv file or choose **New Data Set** button. To do that, click on **New Data Set** to import the file. The file will have a list of services names to check if they are running or not. An example of service name is *W32Time* which stands for Windows Time Service.



6. 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.



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

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.

Select a data set (single column) containing values that are acceptable for this property.

Scan package:
ExtentrixServicesCheckerScan

Property description:
List of needed services to be existed and run.

Property value:
List of Services

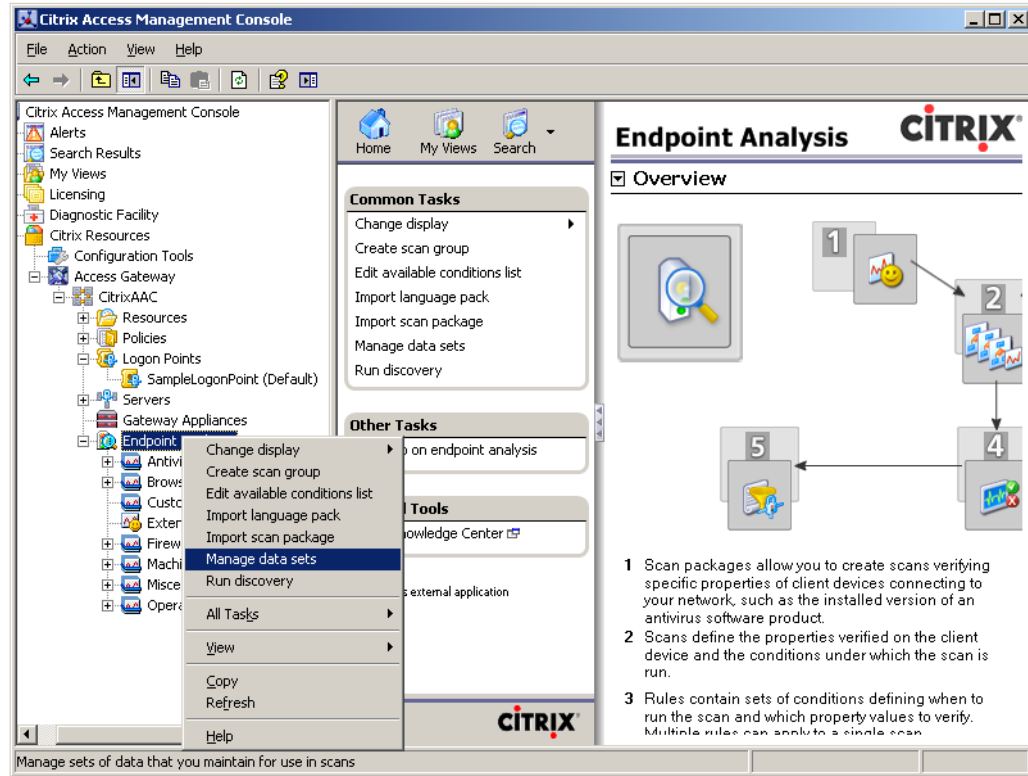
Map to Scan Output

New Data Set

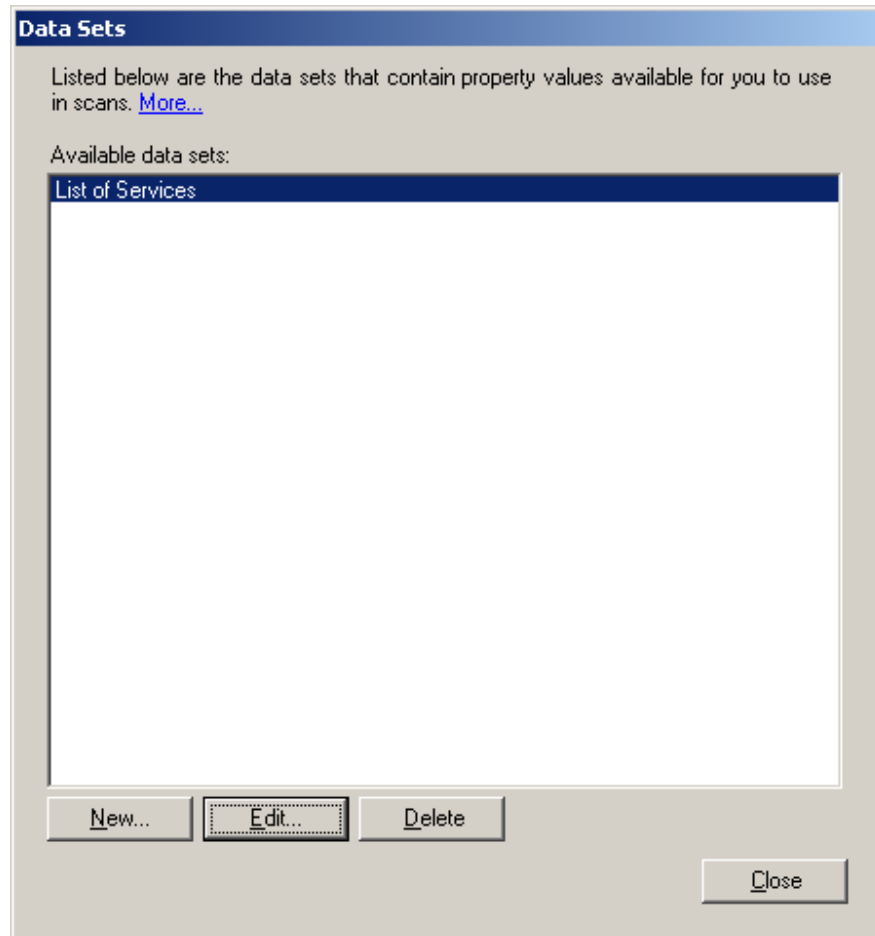
< Back Finish Cancel

Note: You can leave the path of the file empty to create an empty single-column data set. You can edit the value later after you create the data set. To edit the data set:

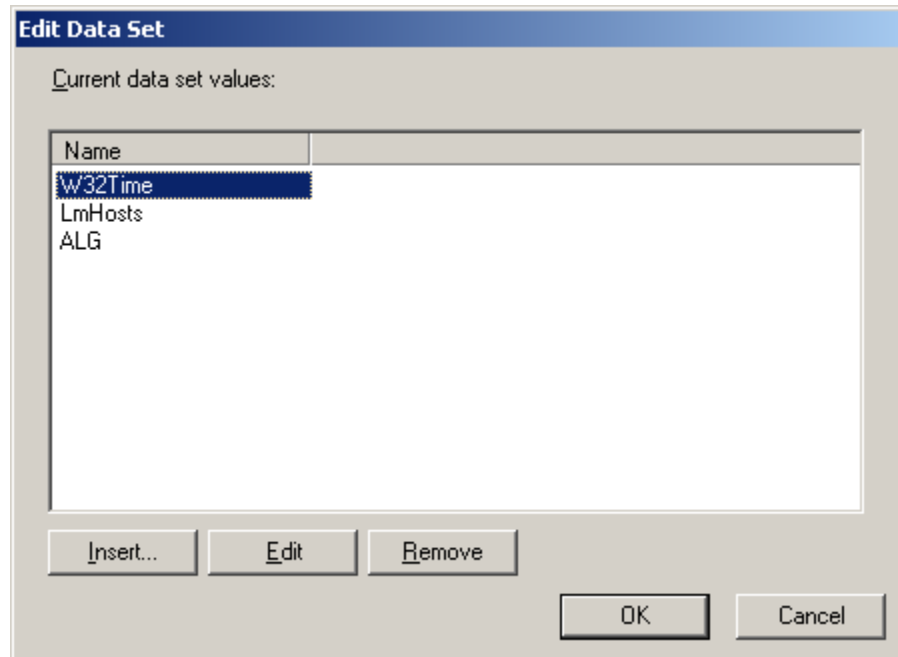
- Right click **Endpoint Analysis** in the console tree and select **Manage Data Set** from the action menu.



- 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 FILES' DATE SCAN

SCAN DESCRIPTION

Scan Name: Extentrix Files' Dates. It's included in Extentrix File Scan Combo.

Description: This scan is designed to scan the client's machine for a map (List) of files and check if they exist and match the date specified by the administrator before allowing the Client to access the corporate network. For example, the administrator may require that the client has a certain file created on 3/20/2007 (Month/Day/Year). The scan will check for that file date and grant access upon meeting that condition.

Parameters:

- Map (List) file: an excel .CSV file that contains two columns, one for file path and other for file creation date in form (3/20/2007).

Scan Output:

- Allow Access- a Boolean output which indicates whether the files in the map file exist and match their dates or not.
 - TRUE – indicates that all Files in the map file exist and match their Dates.
 - FALSE – indicates that at least one of the files doesn't exist or does not match its Date.
- 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.

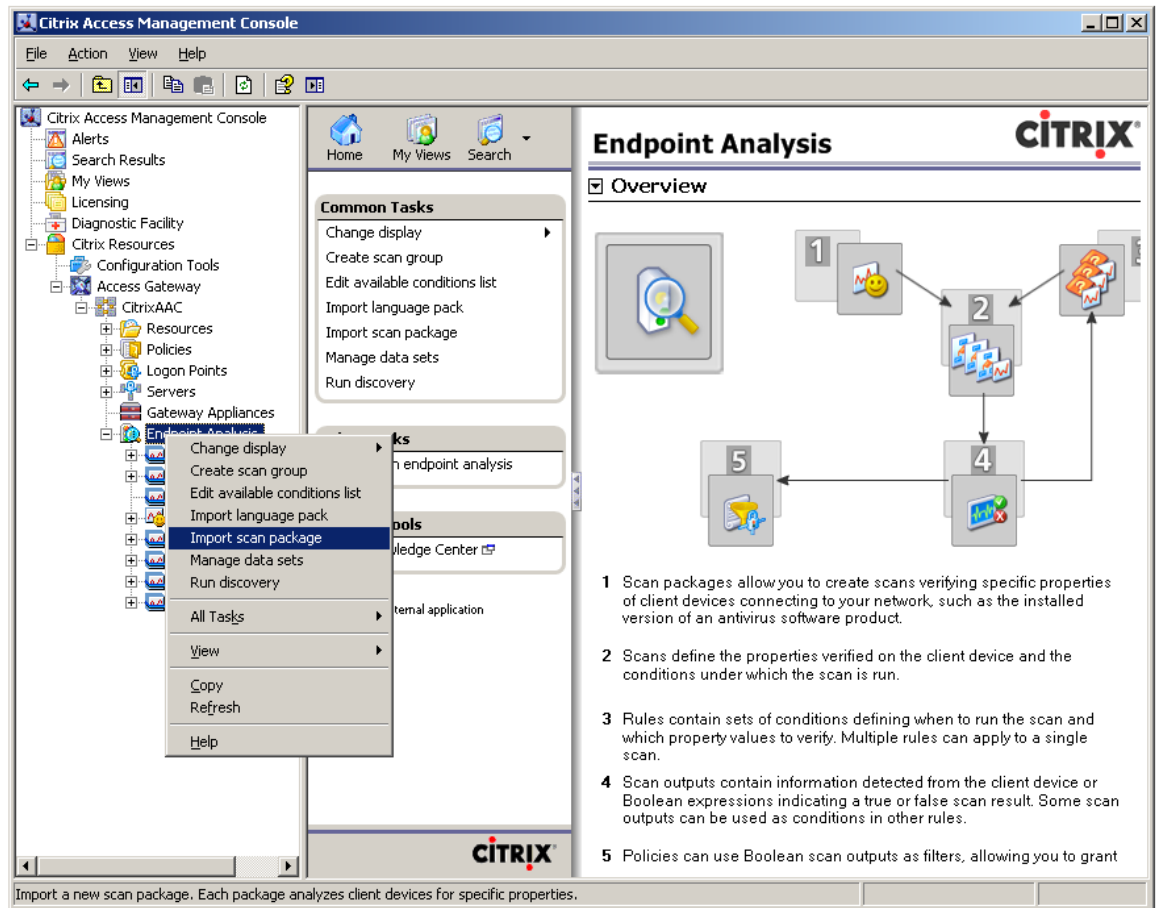
Note: If the License Status has an Invalid License value, the Allow Access will be false.

INSTALLATION AND CONFIGURATION

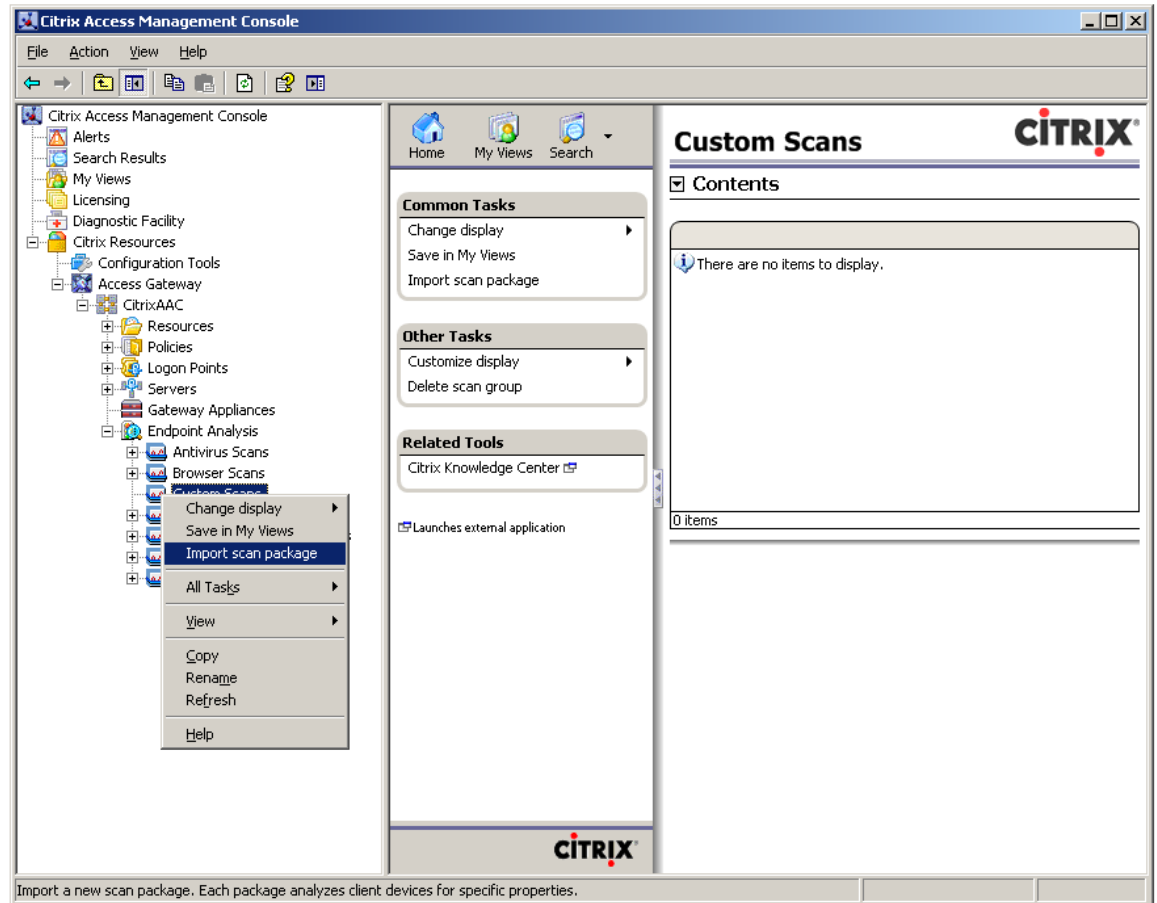
IMPORTING SCAN PACKAGES

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

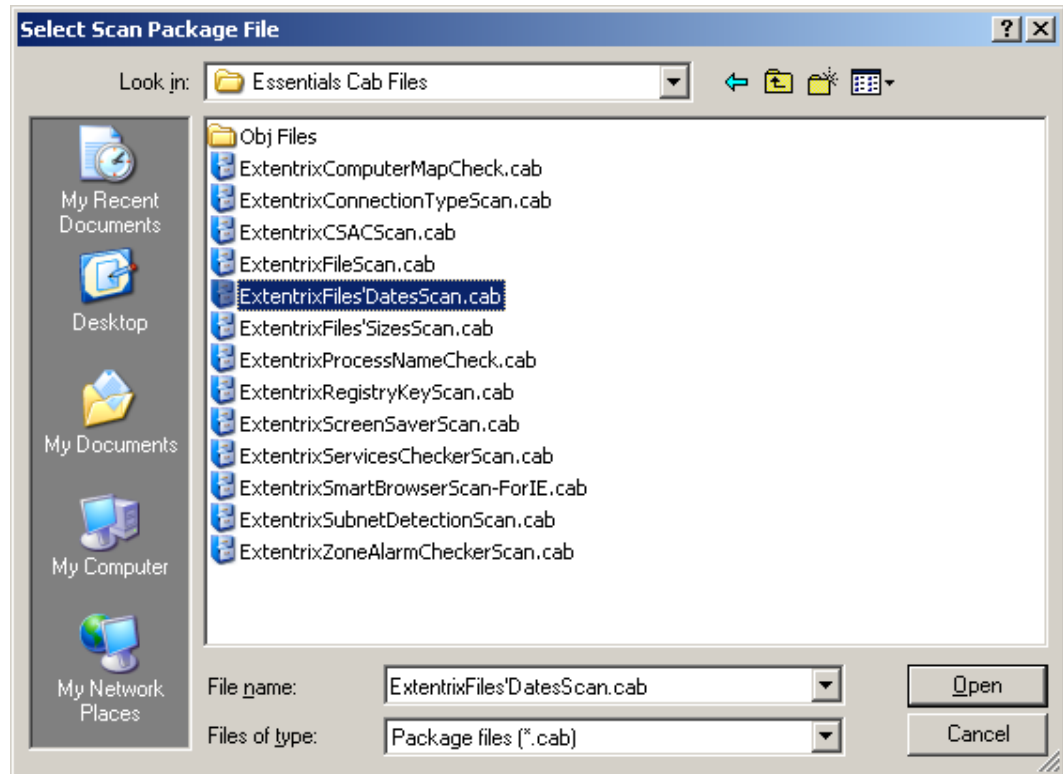
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



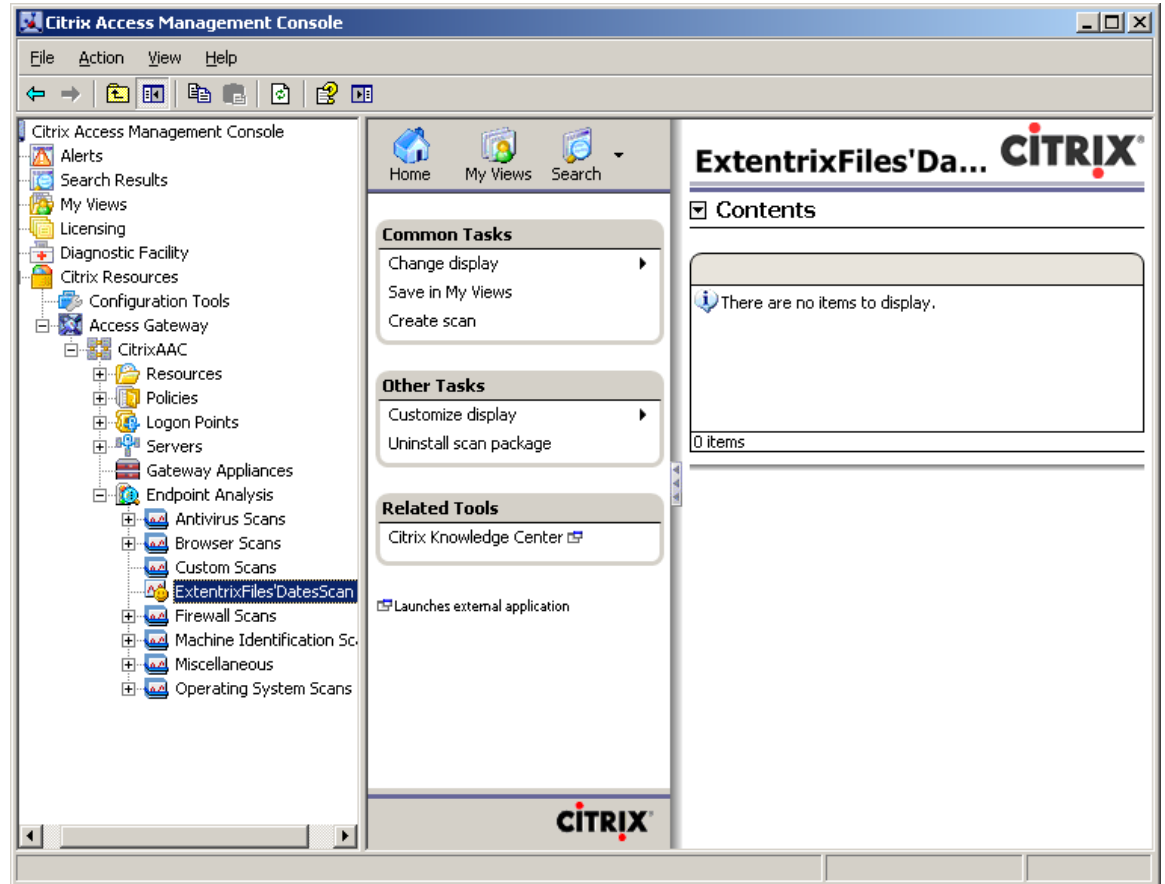
Also you can choose to insert the scan package to any scan category listed in the tree as shown in the following picture:



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



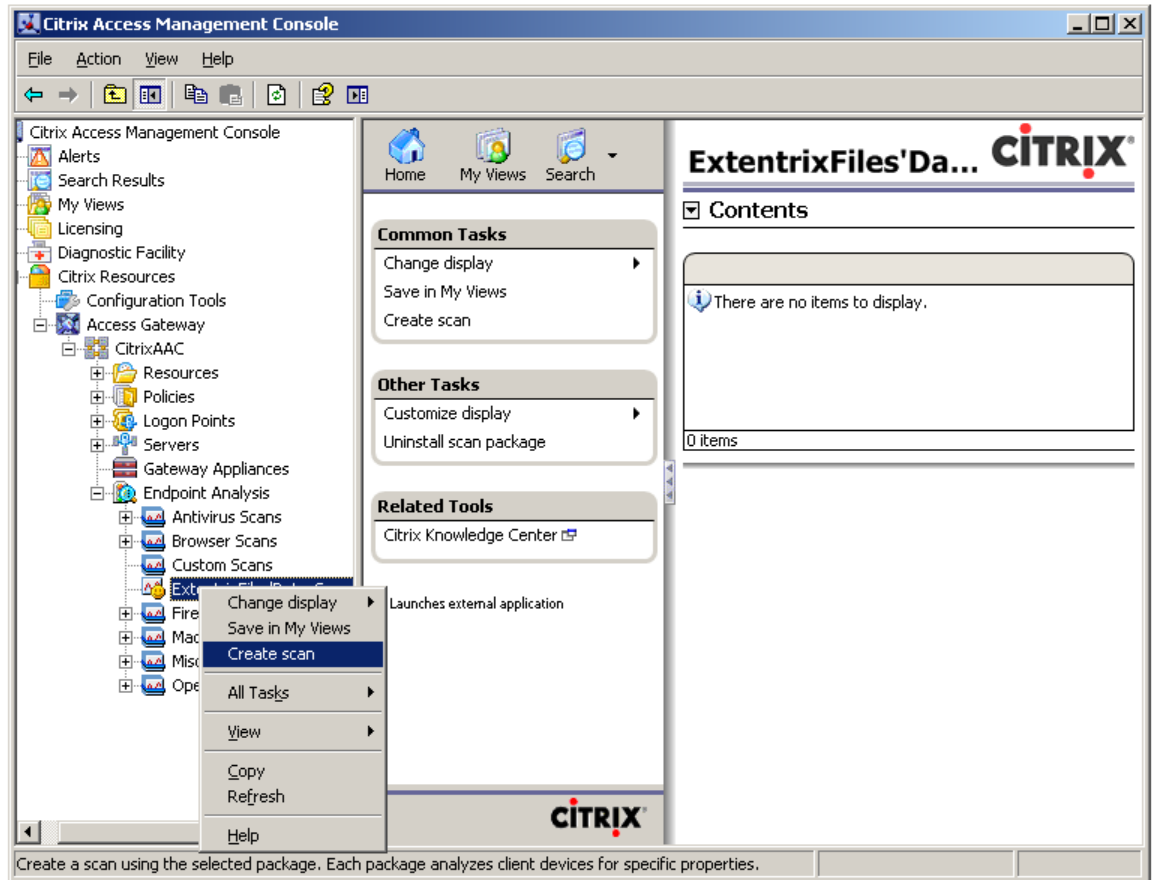
The package will be displayed in the console as shown in the following picture:



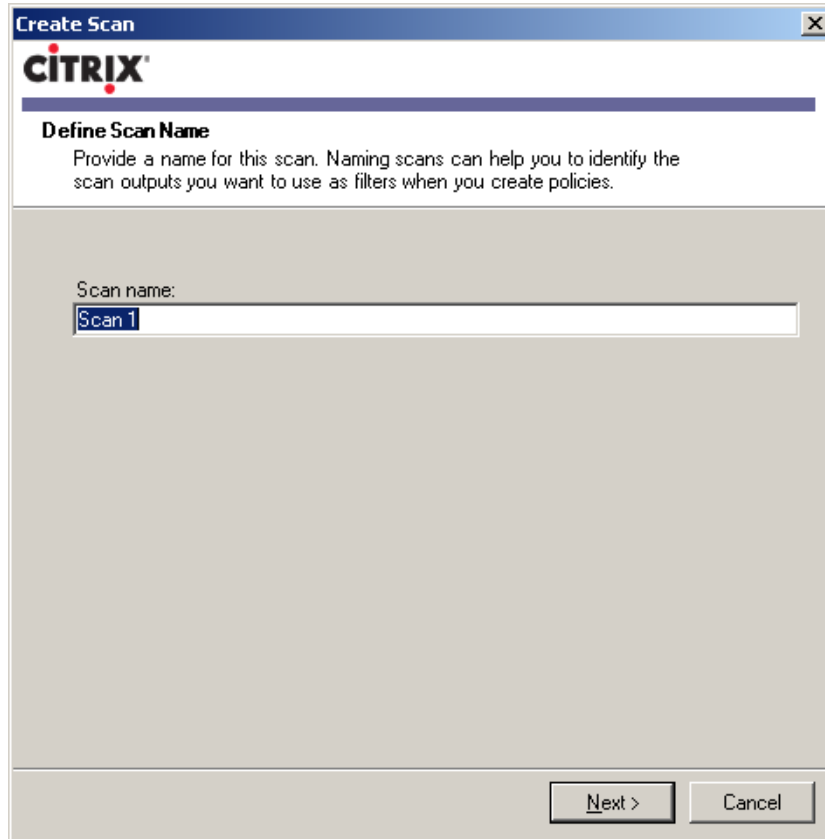
INSTALLING THE SCAN PACKAGE

Please follow the steps below to create scans and rules for the **Extentrix File's Date Scan**.

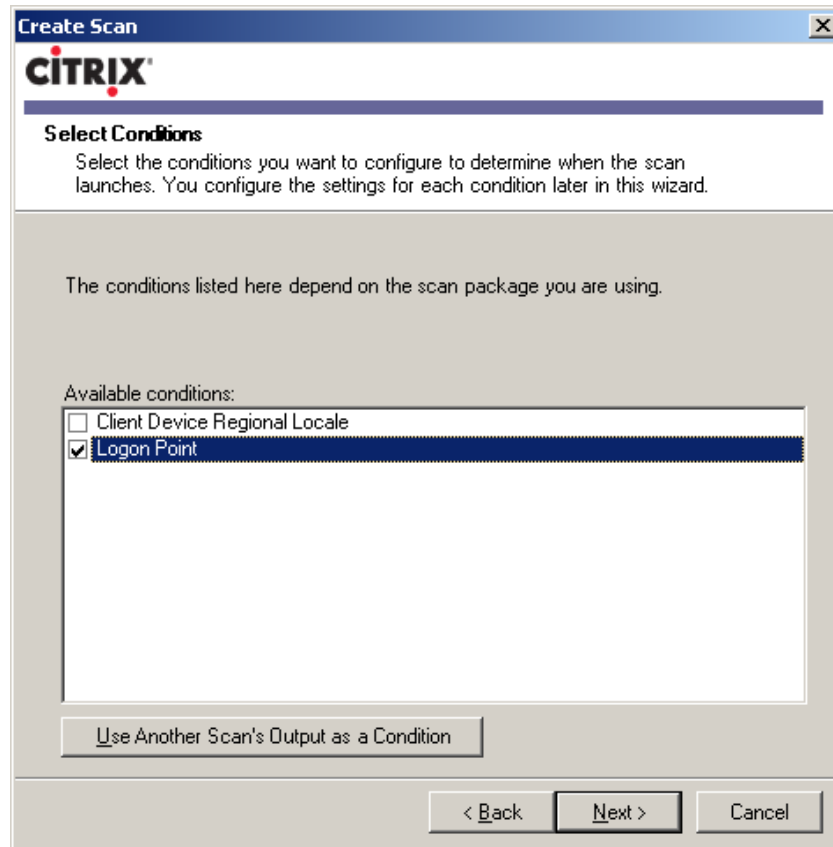
1. Select **ExtentrixFile'sDatesScan** to create scan for it, right click the icon and choose **Create Scan**.



2. Type a name for the scan:



3. Set the scan conditions:



4. Type rule name and set rule conditions:

Create Scan

CITRIX

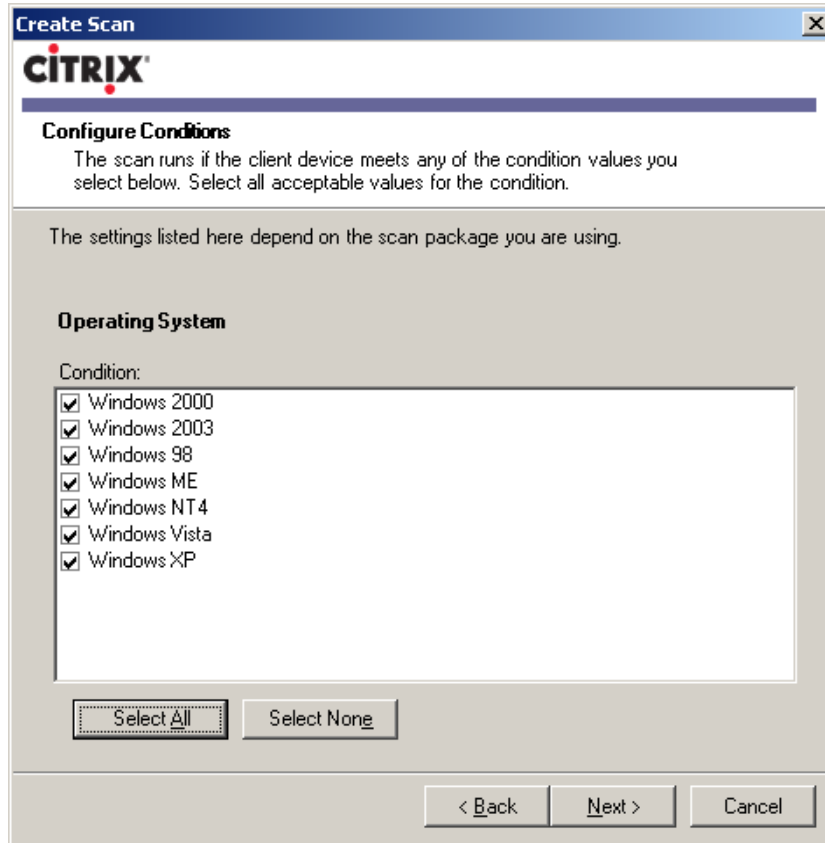
Define Rule
Rules are a combined set of conditions under which a scan is run.

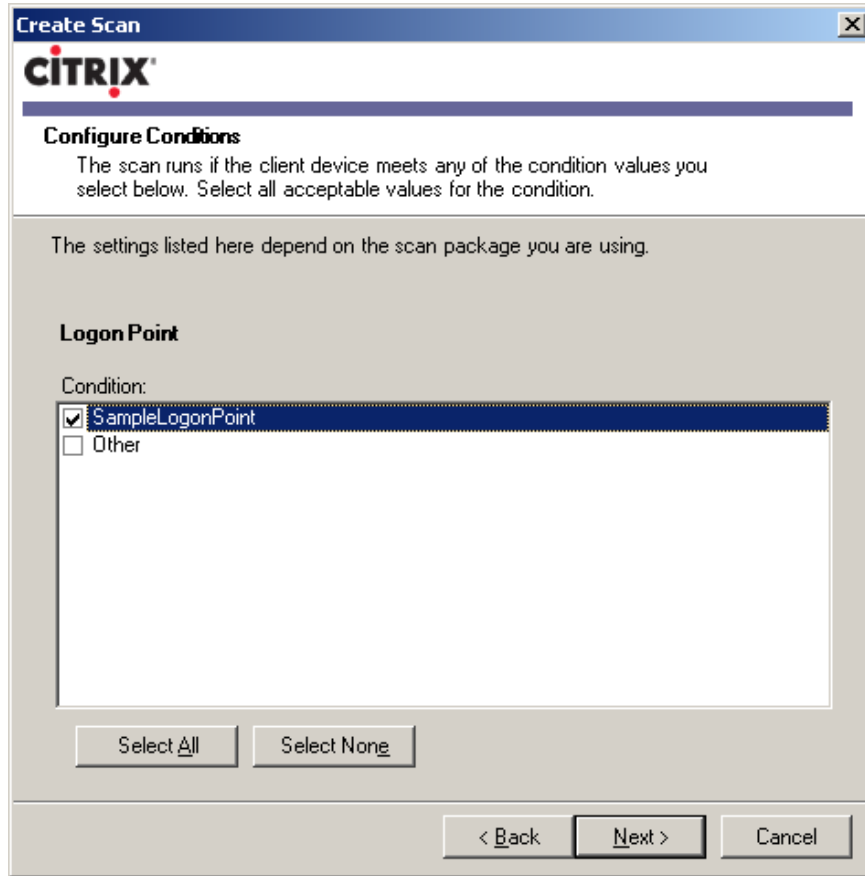
For example, your rule might be to use Scan X when the client device is running Operating System Y and Browser Version Z.

You can create multiple rules for any scan.

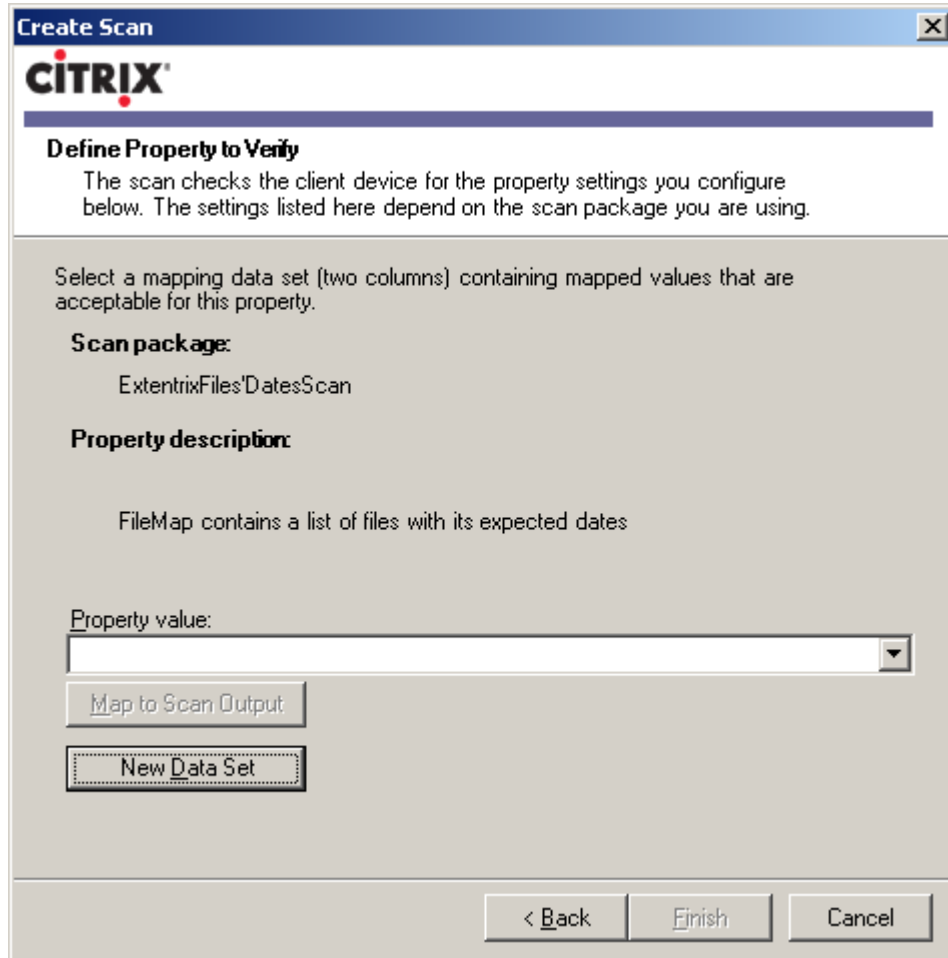
Rule name:

< Back Next > Cancel

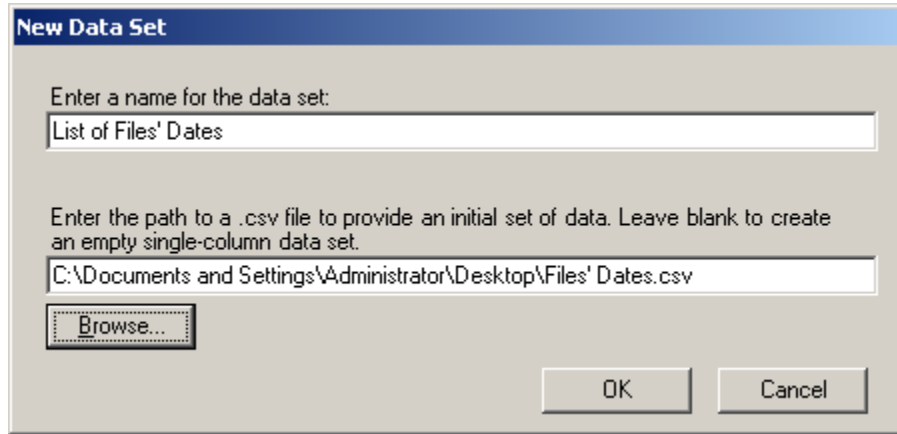




5. Define a data set (map) using a comma delimited .csv file. To do that, click on **New Data Set** to import the file. The file will have a list of all the files' dates to be scanned.



6. 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.



The image shows a 'New Data Set' dialog box with a blue title bar. It contains two text input fields and two buttons. The first field is labeled 'Enter a name for the data set:' and contains the text 'List of Files' Dates'. The second field is labeled 'Enter the path to a .csv file to provide an initial set of data. Leave blank to create an empty single-column data set.' and contains the path 'C:\Documents and Settings\Administrator\Desktop\Files' Dates.csv'. Below the second field is a 'Browse...' button. At the bottom right are 'OK' and 'Cancel' buttons.

New Data Set

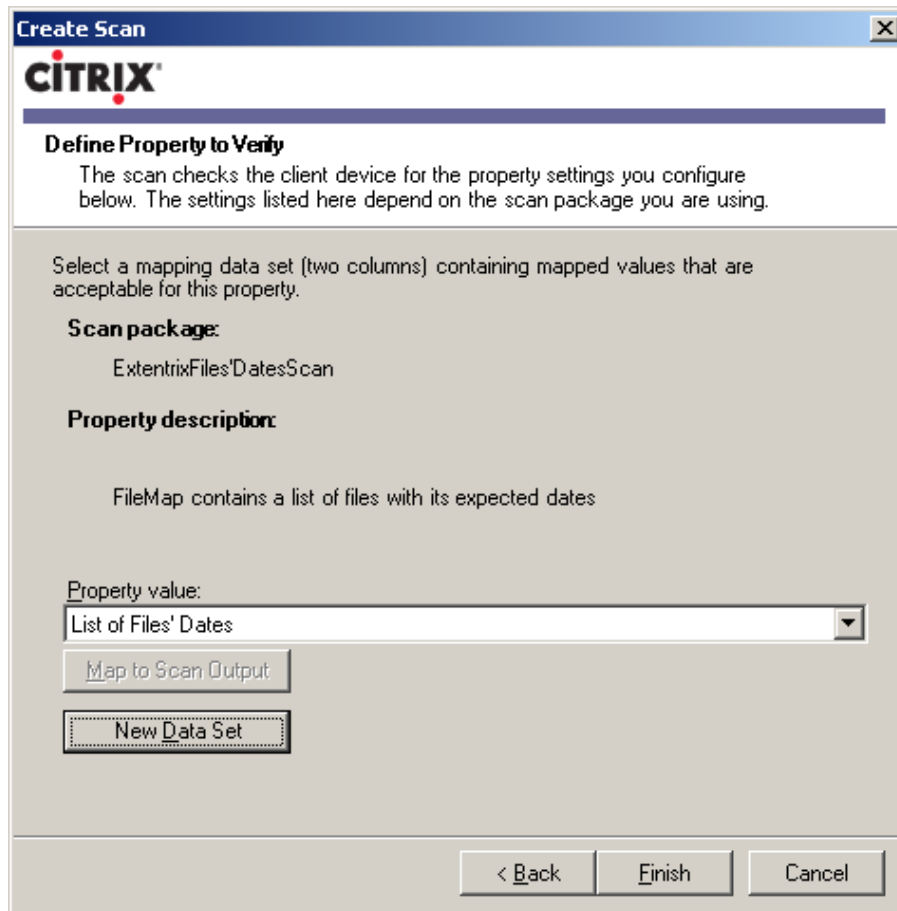
Enter a name for the data set:
List of Files' Dates

Enter the path to a .csv file to provide an initial set of data. Leave blank to create an empty single-column data set.
C:\Documents and Settings\Administrator\Desktop\Files' Dates.csv

Browse...

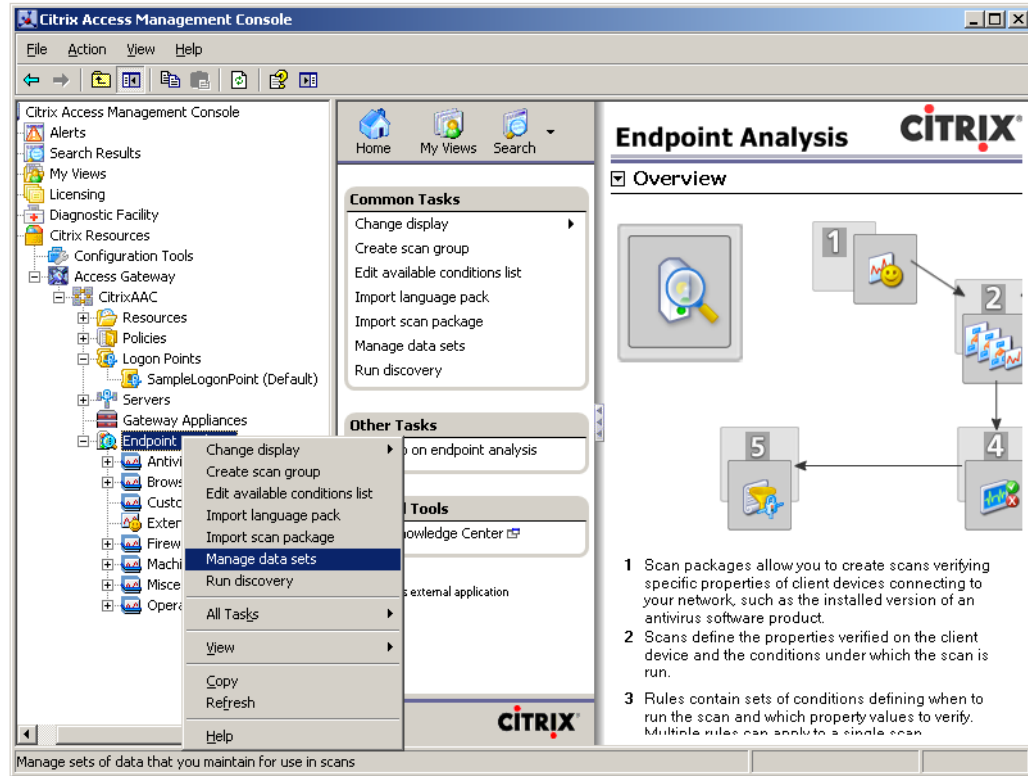
OK Cancel

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

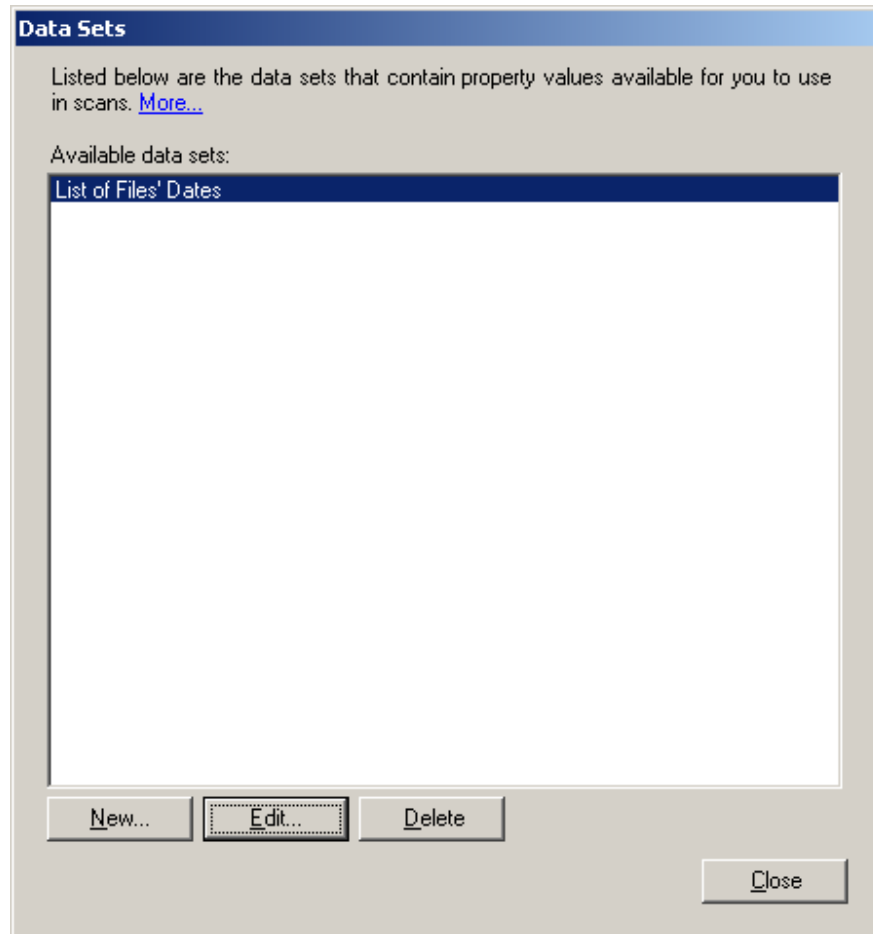


Note: The path of the file in map should be less than 64 characters. You can leave the path of the file empty to create an empty single-column data set. You can edit the value later after you create the data set. To edit the data set:

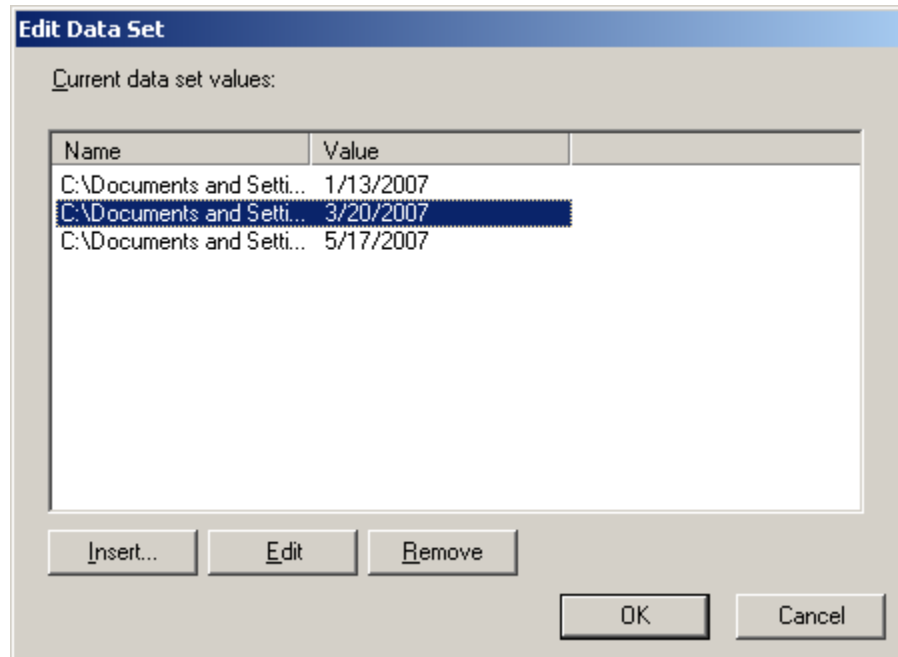
- Right click **Endpoint Analysis** in the console tree and select **Manage Data Set** from the action menu.



- 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**.

6. EXTENTRIX FILES' SIZES SCAN

SCAN DESCRIPTION

Scan Name: Extentrix Files' Size. It's included in Extentrix File Scan Combo.

Description: This scan grants administrators a higher security over the resources accessed. It scans the client's machine for a map (List) of files and checks if they exist and match the size determined by the administrator before allowing the Client to access the corporate network.

Parameters:

- Map (List) file: an excel .CSV file that contains two columns, one for file path and other for file size.

Scan Output:

- Allow Access- a Boolean output which indicates whether the files in the map file exist and match their size or not.
 - TRUE – indicates that all Files in the map file exist and match their sizes.
 - FALSE – indicates that at least one of the files doesn't exist or does not match its size.
- 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.

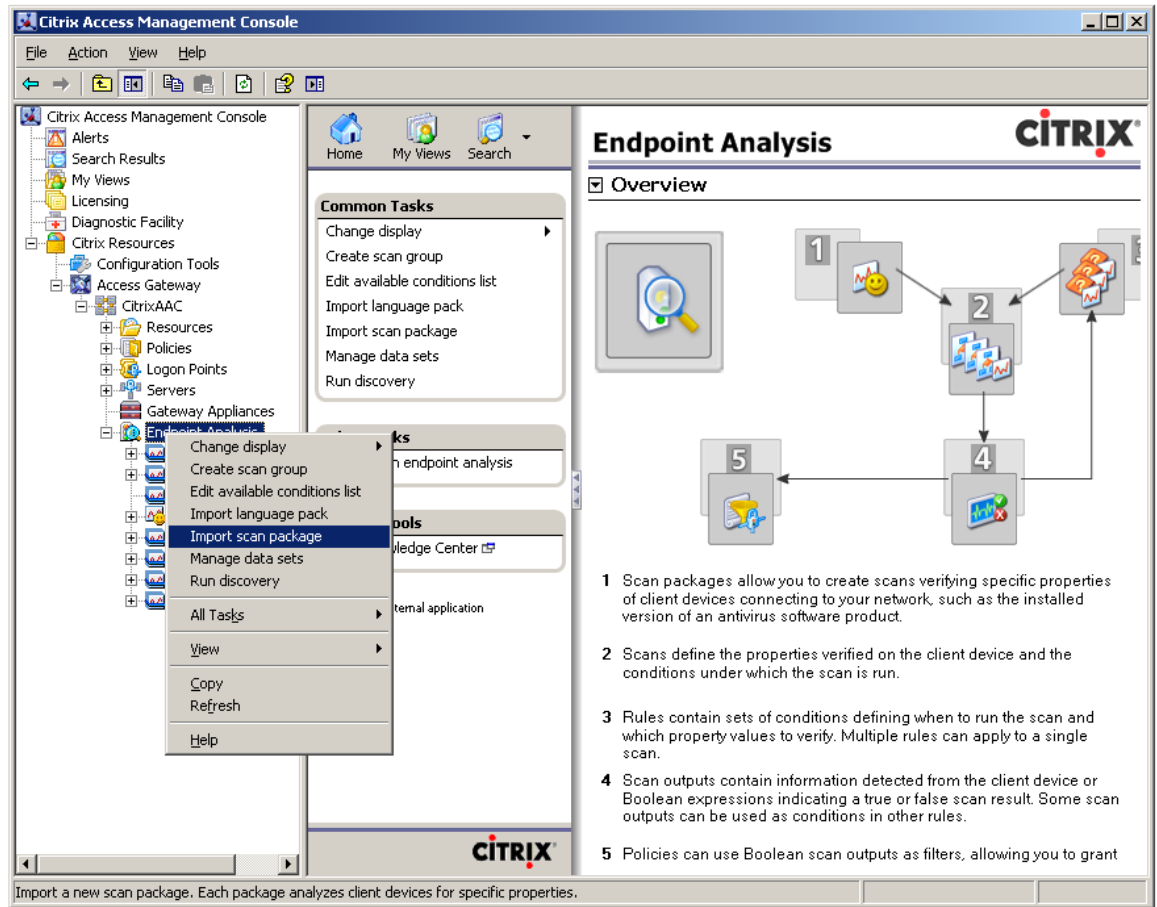
Note: If the License Status has an Invalid License value, the Allow Access will be false.

INSTALLATION AND CONFIGURATION

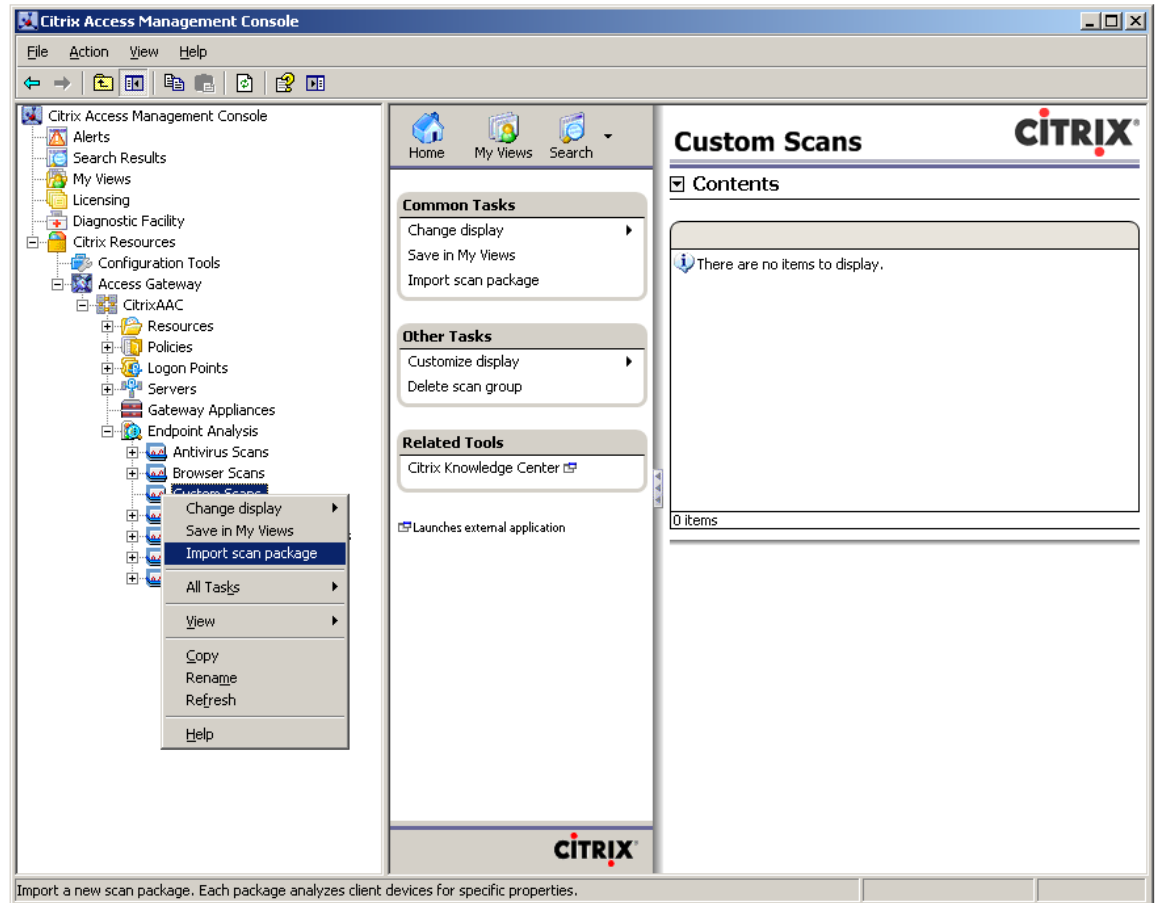
IMPORTING SCAN PACKAGES

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

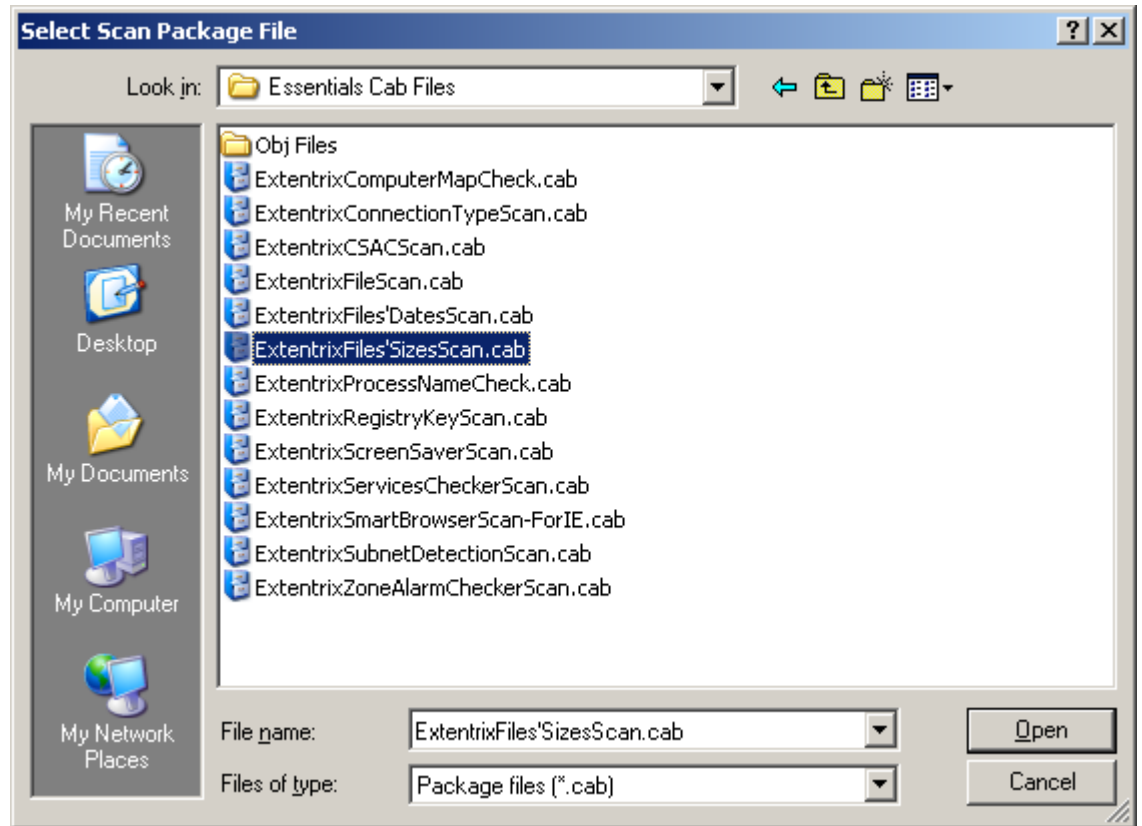
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



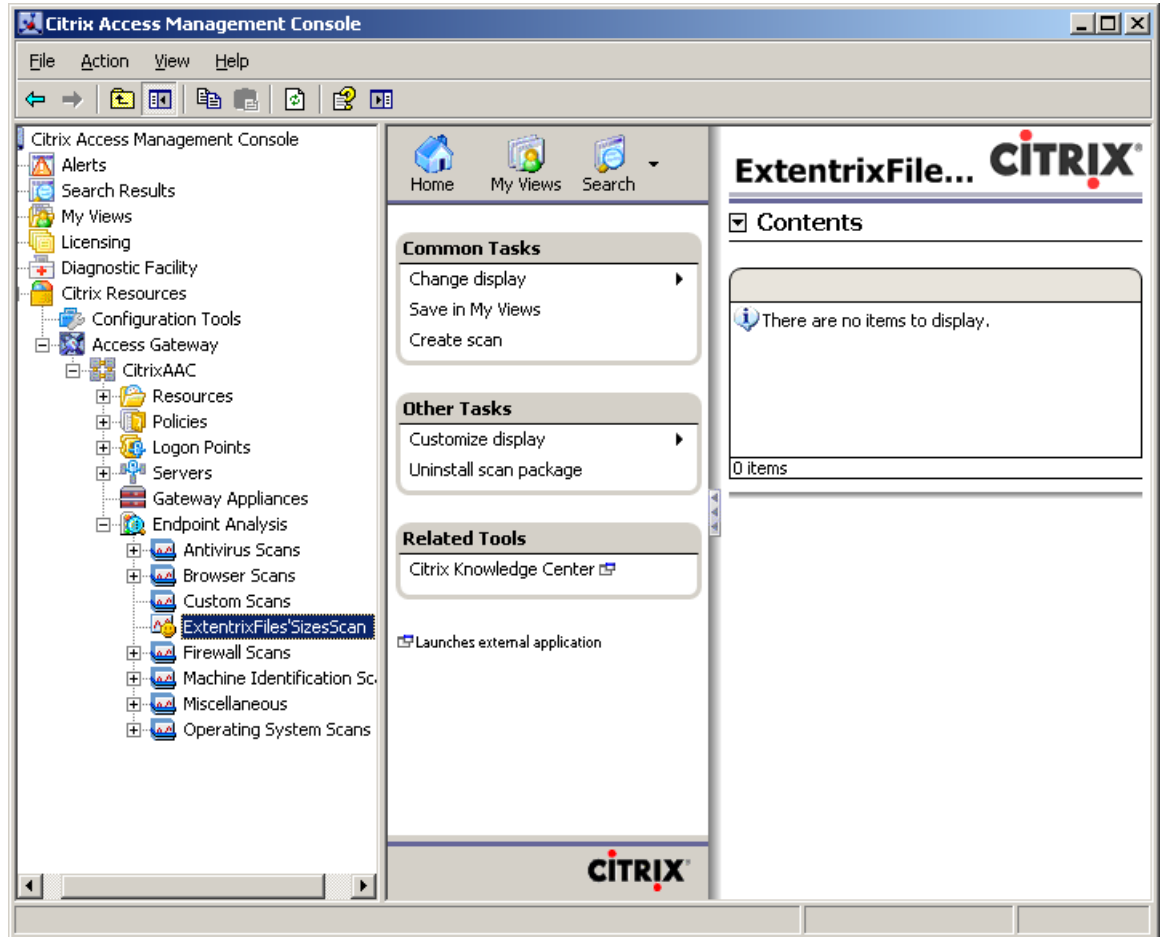
Also you can choose to insert the scan package to a specific scan package group as shown in the following picture:



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



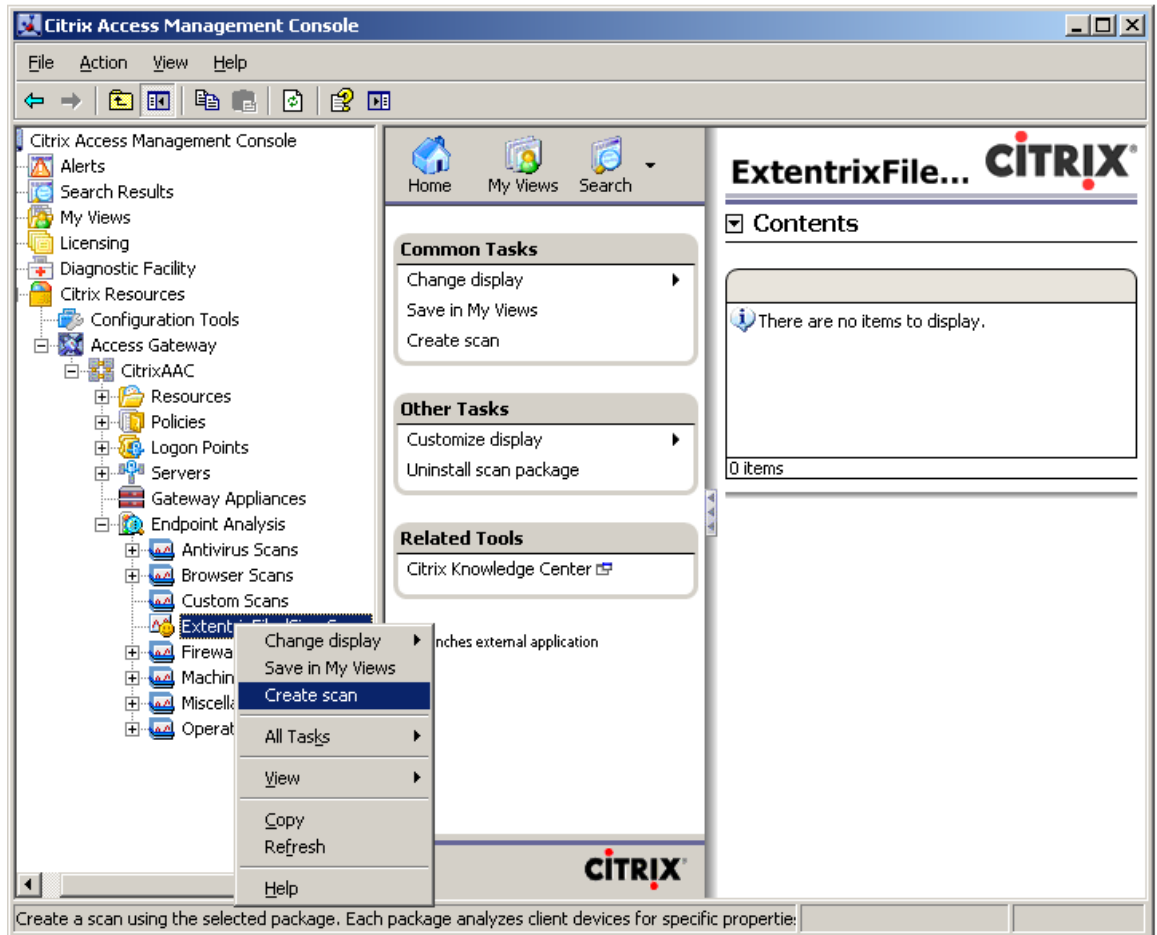
The package will be displayed in the console as shown in the following picture:



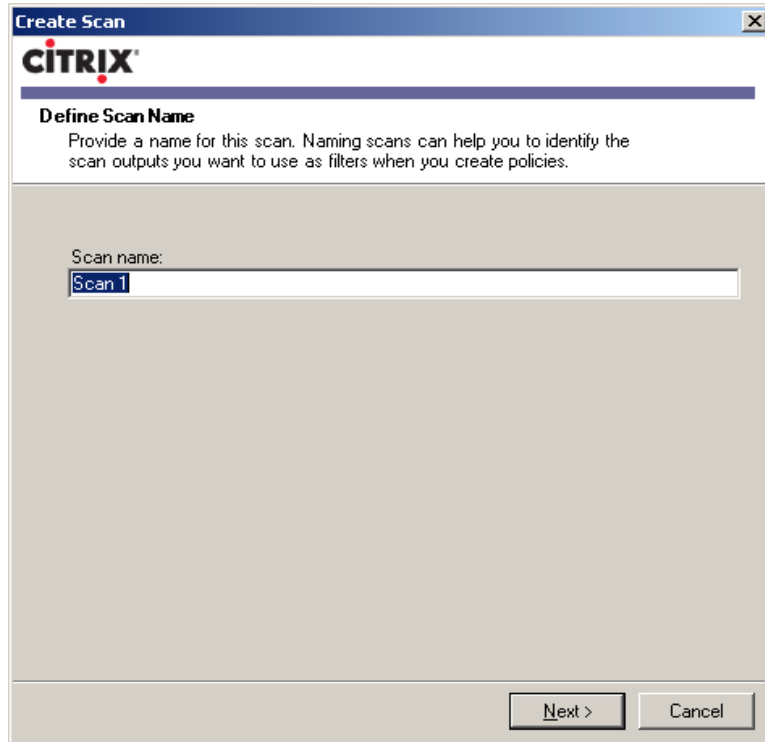
INSTALLING THE SCAN PACKAGE

Please follow the steps below to create scans and rules for the **Extentrix Files' Sizes Scan**.

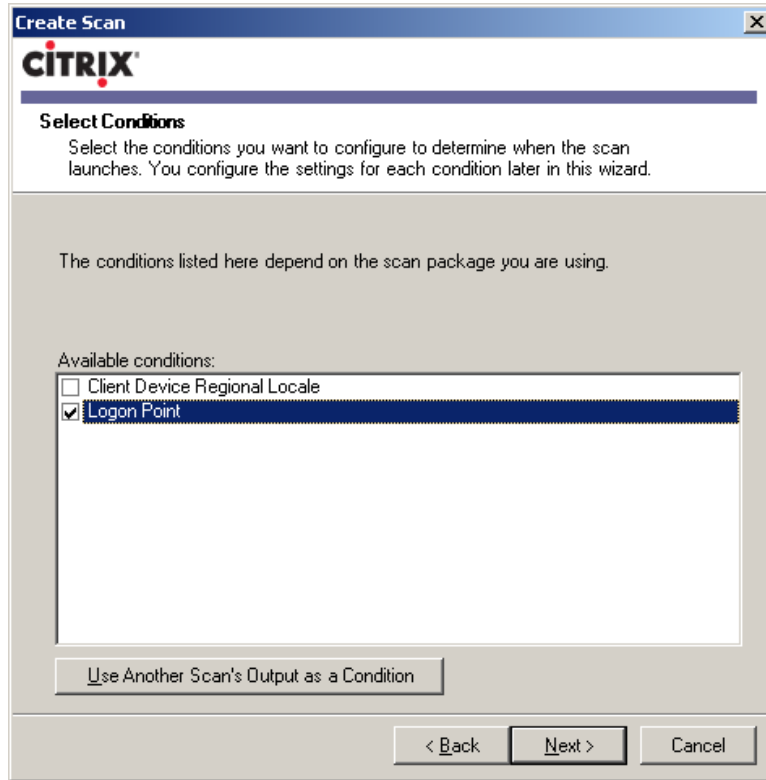
1. Select **Extentrix Files' Sizes Scan** to create scan for it, right click the icon and choose **Create Scan**.



2. Type a name for the scan:



3. Set the scan conditions:



4. Type rule name and set rule conditions:

Create Scan

CITRIX

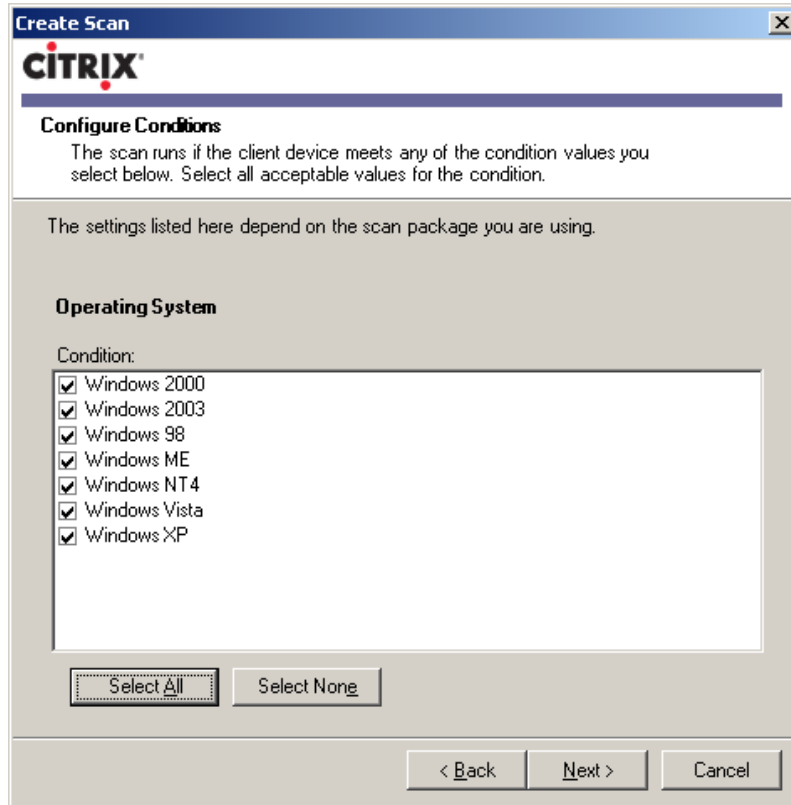
Define Rule
Rules are a combined set of conditions under which a scan is run.

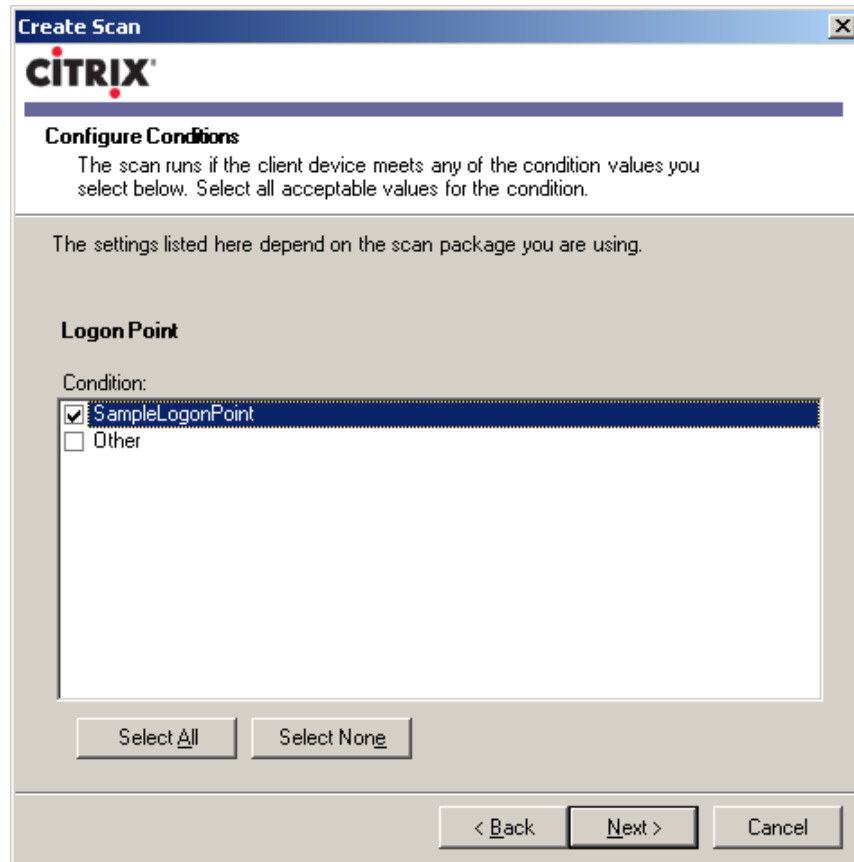
For example, your rule might be to use Scan X when the client device is running Operating System Y and Browser Version Z.

You can create multiple rules for any scan.

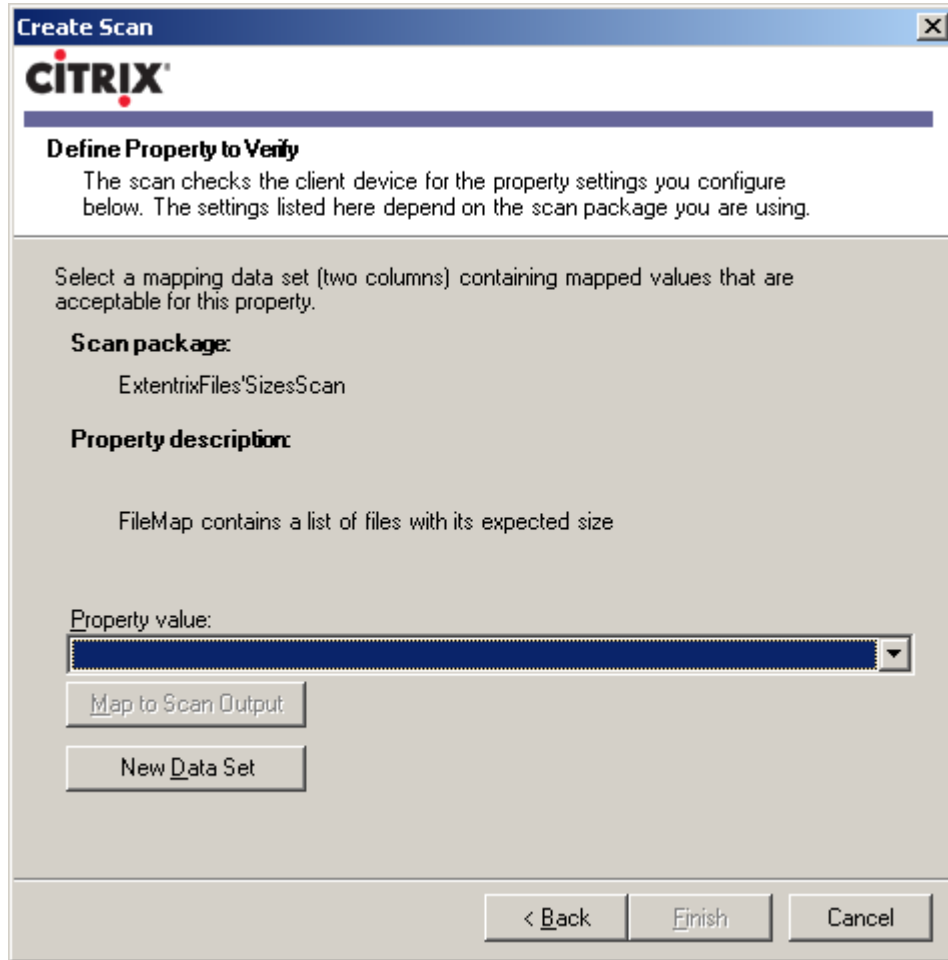
Rule name:

< Back Next > Cancel

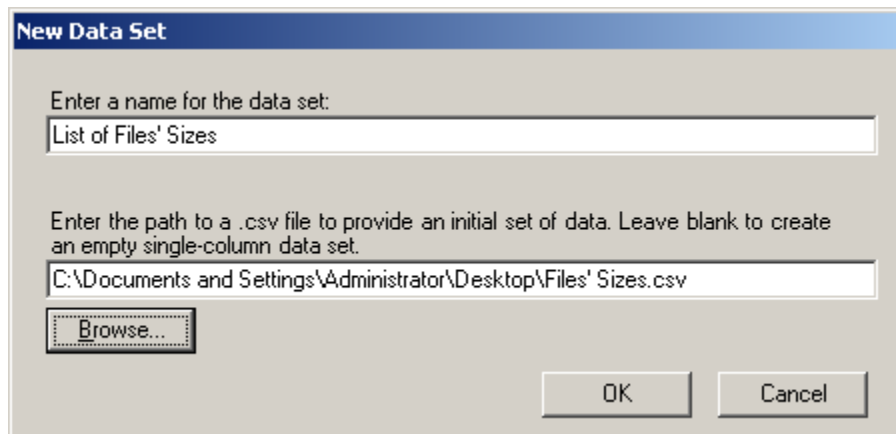




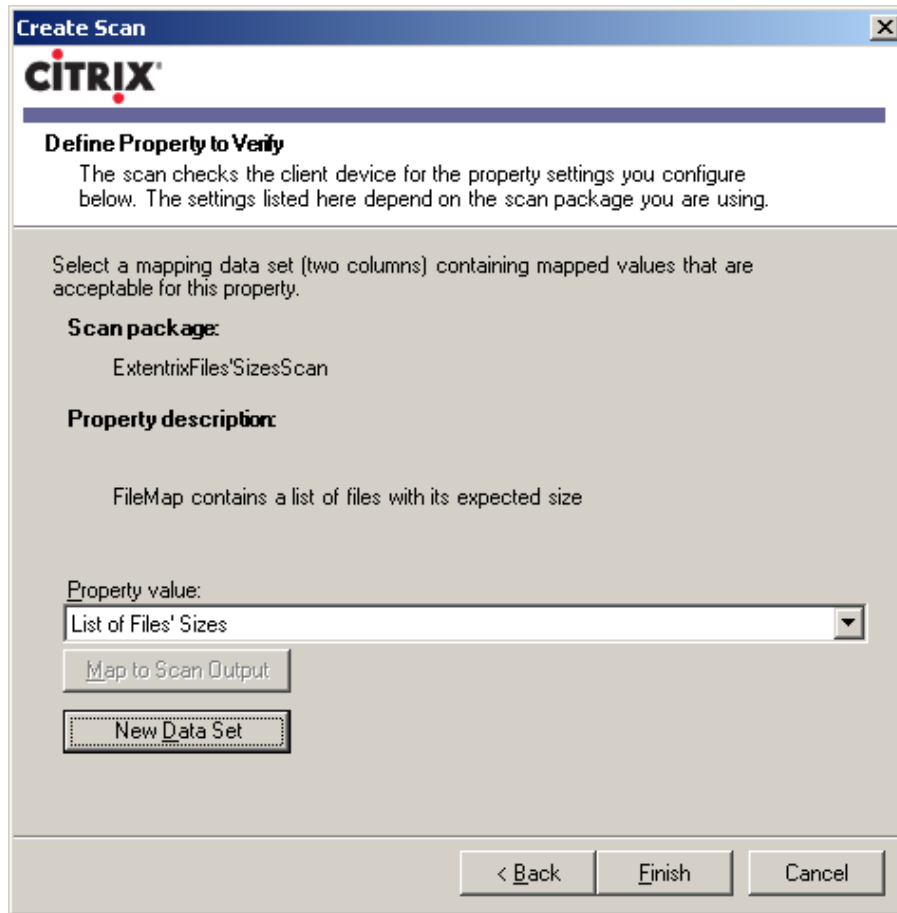
5. Define a data set (map) using a comma delimited .csv file. To do that, click on **New Data Set** to import the file. The file will have a list of files' sizes to be scanned.



6. 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.

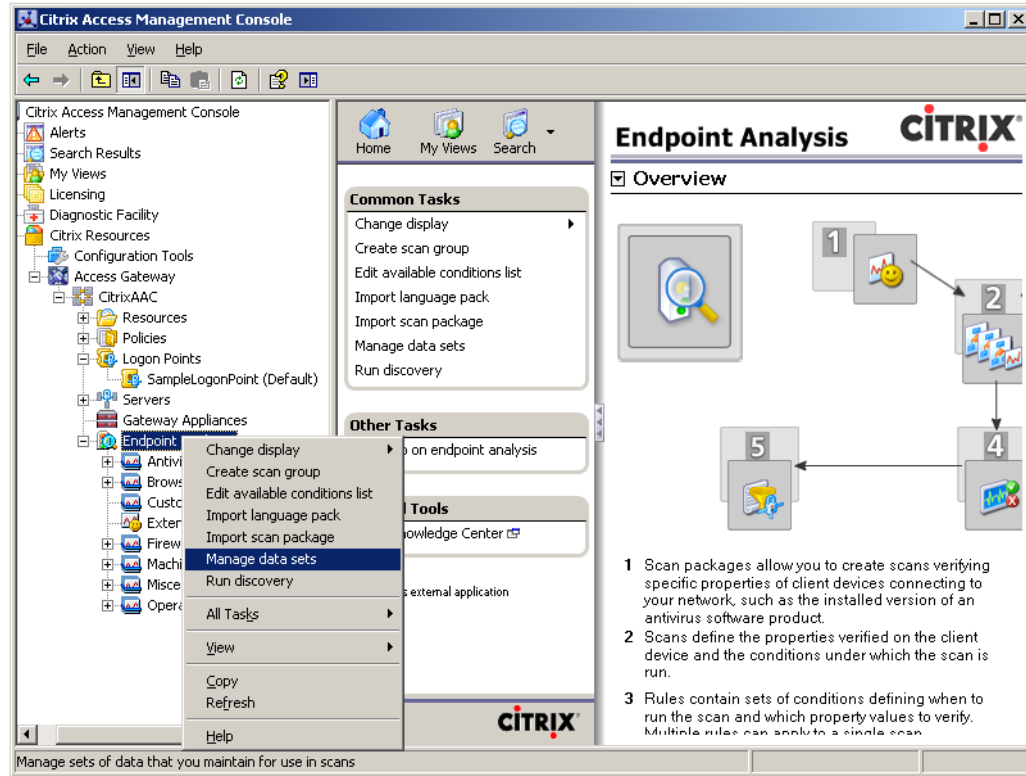


7. When you are done, click **Finish**.

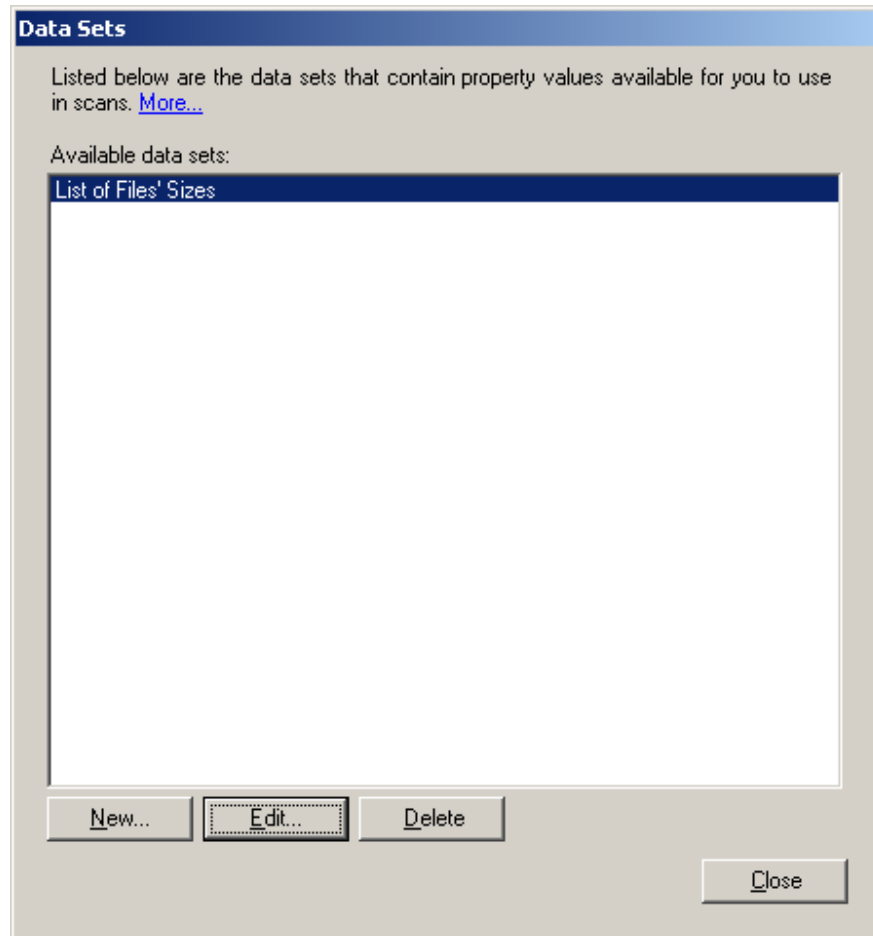


Note: You can leave the path of the file empty to create an empty single-column data set. You can edit the value later after you create the data set. To edit the data set:

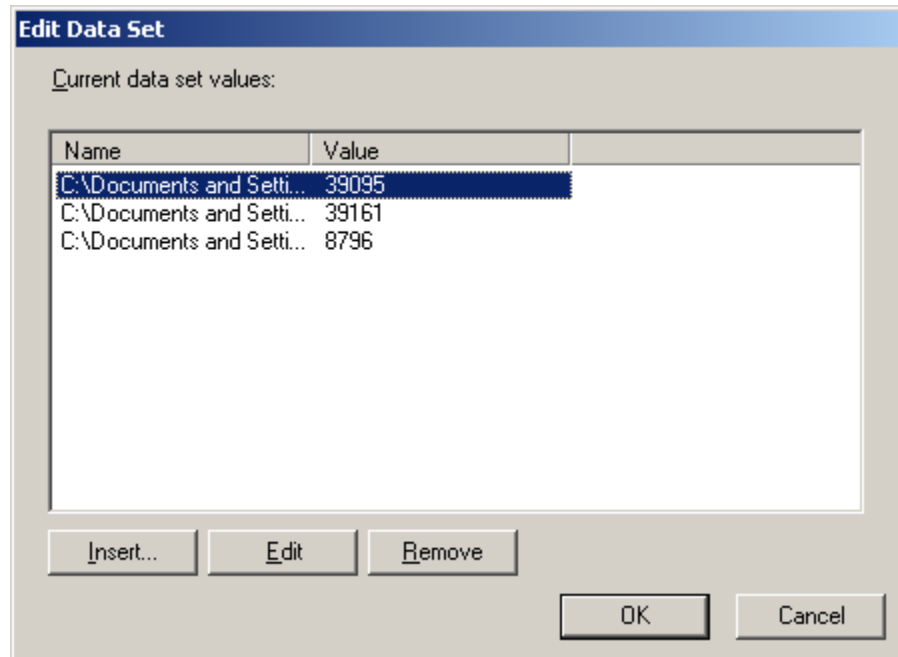
- Right click **Endpoint Analysis** in the console tree and select **Manage Data Set** from the action menu.



- 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**.

7. EXTENTRIX FILE SCAN

SCAN DESCRIPTION

Scan Name: Extentrix File. It's included in Extentrix File Scan Combo.

Description: Scans the client's machine for a certain file name, size, and creation date. As an example, IT administrators may want to make sure that the client machine accessing XenApp has a file existed in the path *C:\Documents and Settings\Administrator\Desktop\Example.doc* with the size of 6450 bytes created on 10/20/2007. This scan performs the check for all these conditions and grant access if they are all met and deny the access if not.

Parameters:

- File path: a string describes the path of the file you want.
- File size: a string describes file size.
- File creation date (Month, Day, and Year): three integers describe the creation date of the file you want.

Scan Output:

- Allow Access- a Boolean output which indicates whether the file you specify matches the client environment.
 - TRUE – indicates that File path, File creation date, and file size match client machine.
 - FALSE – indicates that at least one of the last parameter does not match client machine.
- 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.

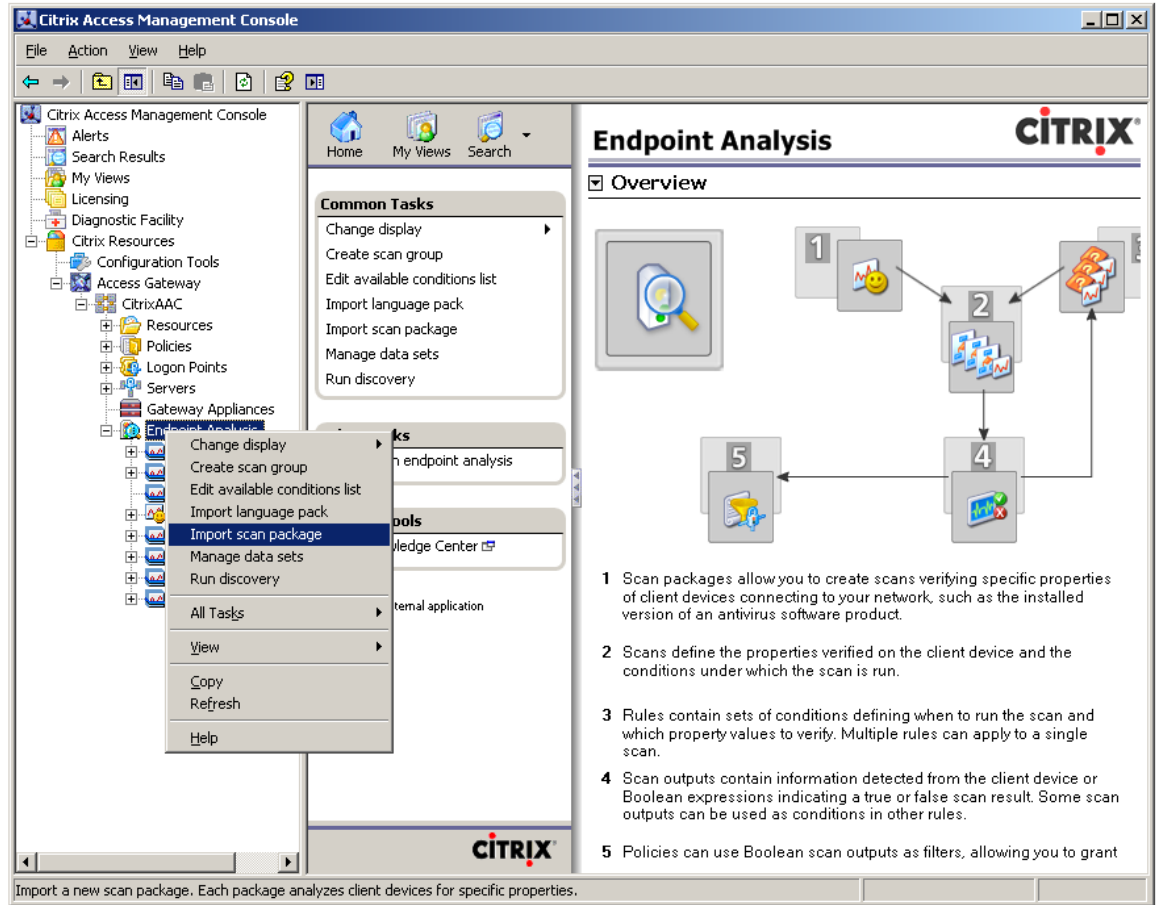
Note: If the License Status has an Invalid License value, the Allow Access will be false.

INSTALLATION AND CONFIGURATION

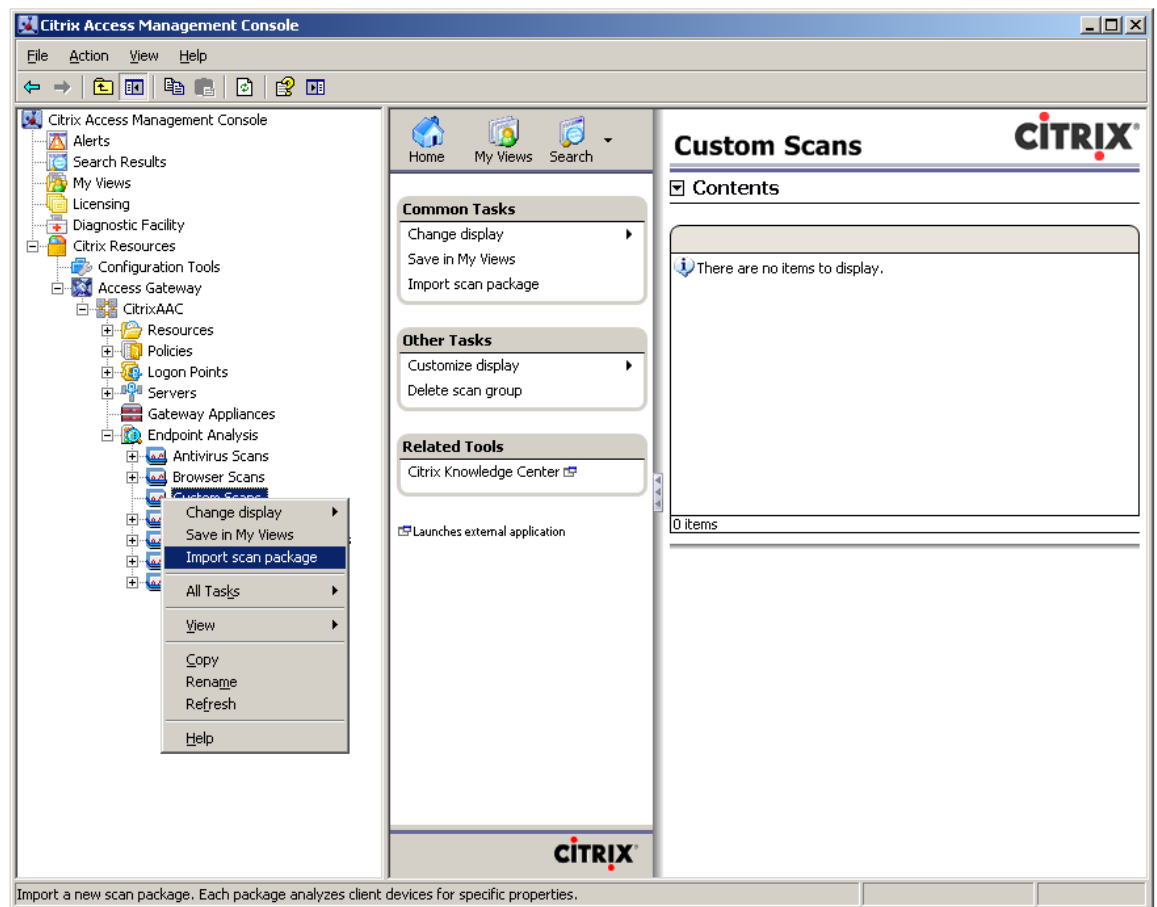
IMPORTING SCAN PACKAGES

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

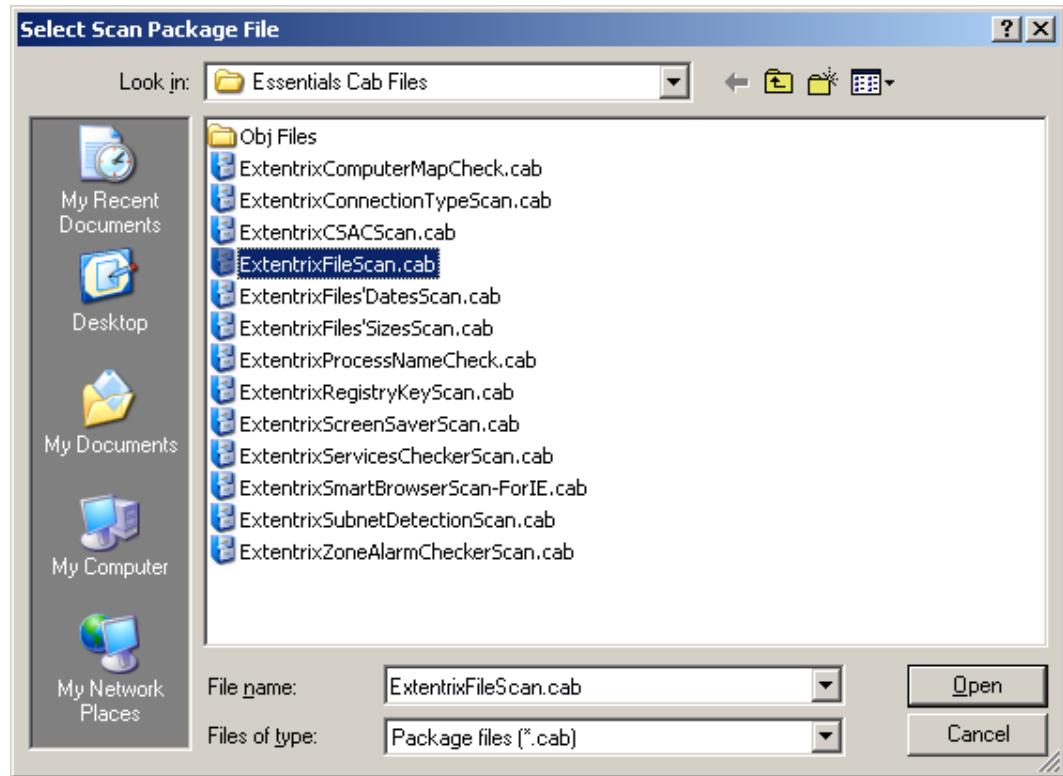
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



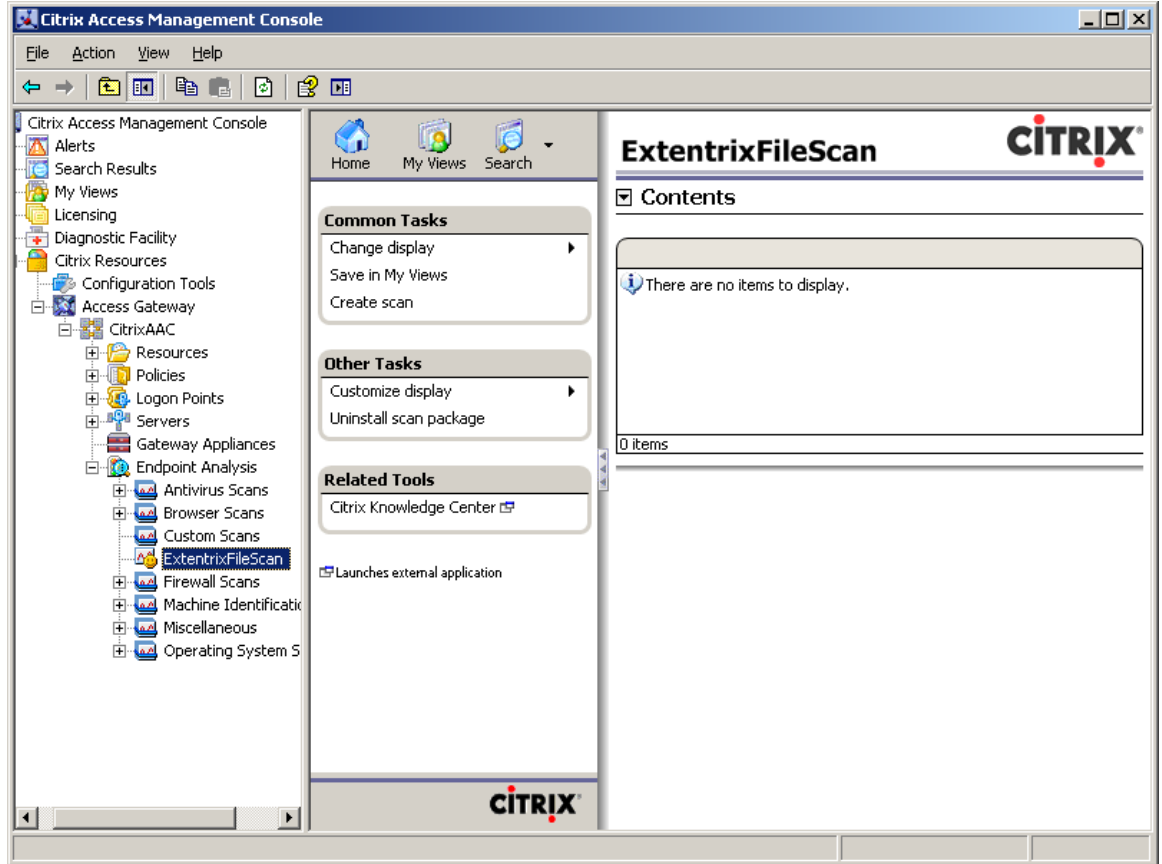
Also you can choose to insert the scan package to a specific scan package group as shown in the following picture:



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



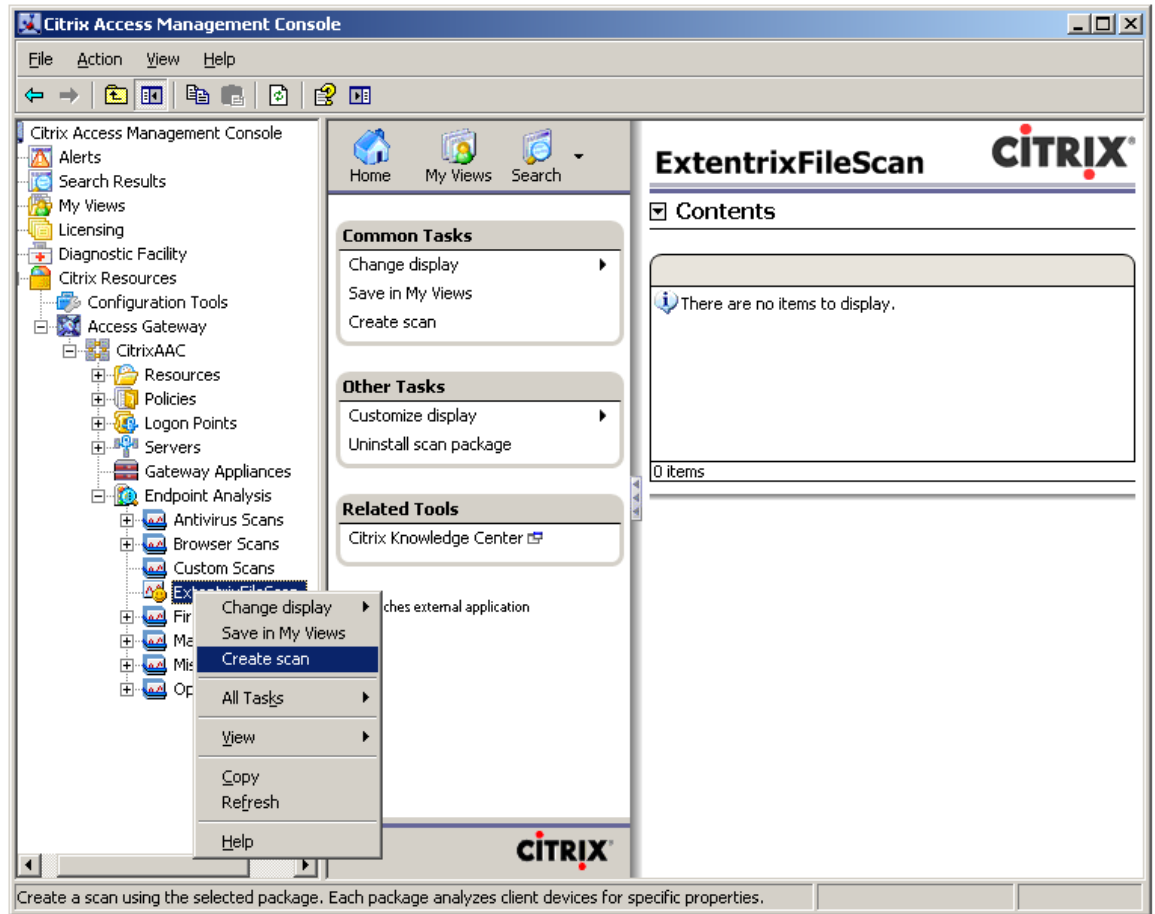
The package will be displayed in the console as shown in the following picture:



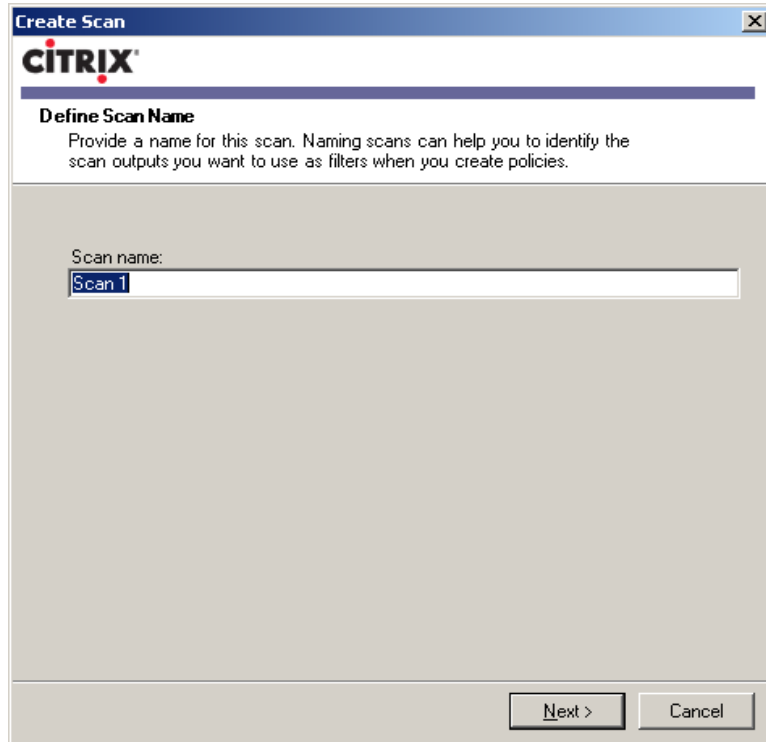
INSTALLING THE SCAN PACKAGE

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

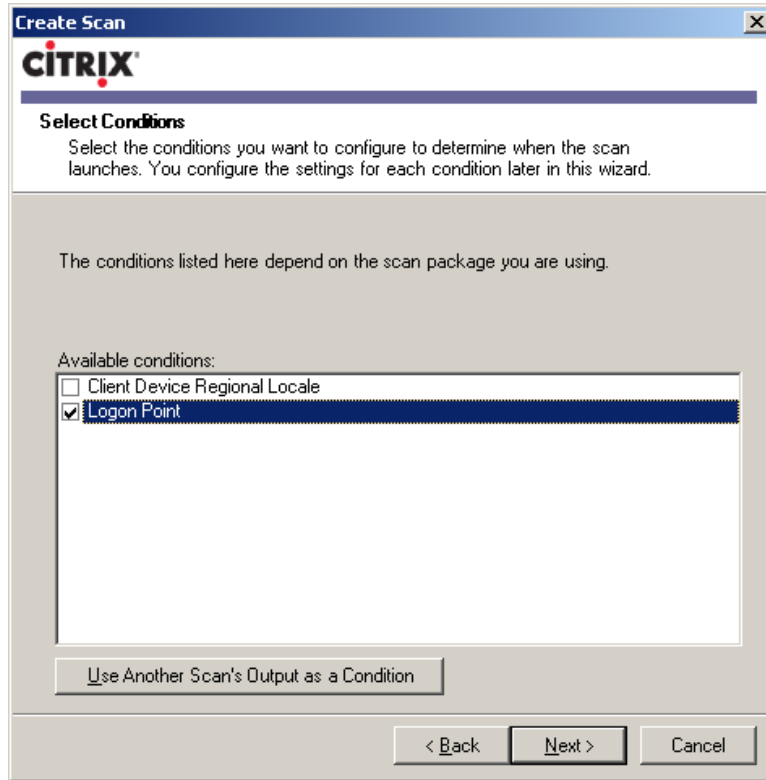
1. Select **Extentrix File Scan** to create scan for it, right click the icon and choose **Create scan**.



2. Type a name for the scan:



3. Set the scan conditions:



4. Type rule name and set rule conditions:

Create Scan

CITRIX

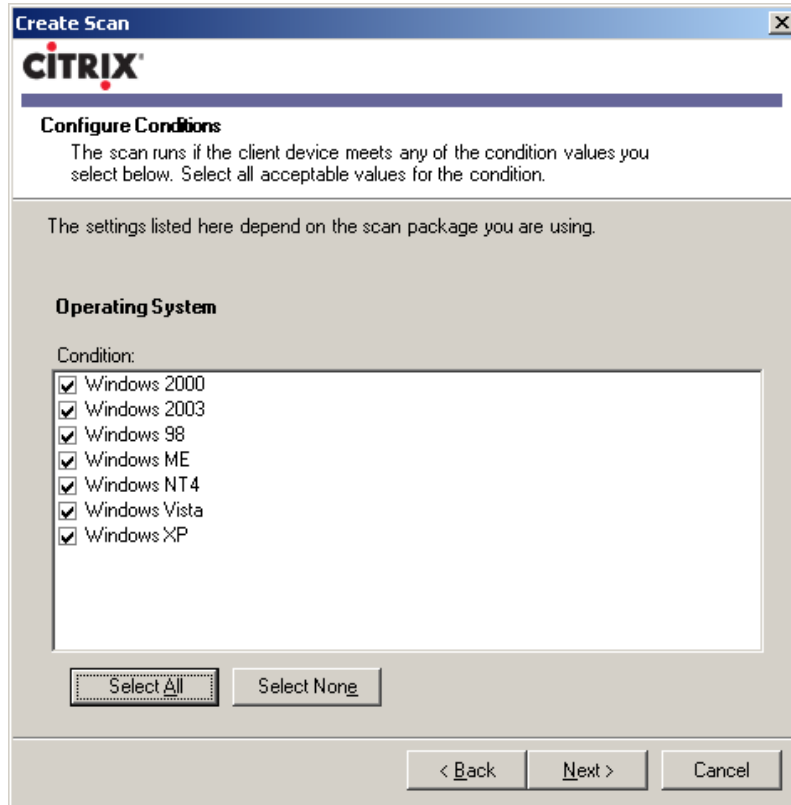
Define Rule
Rules are a combined set of conditions under which a scan is run.

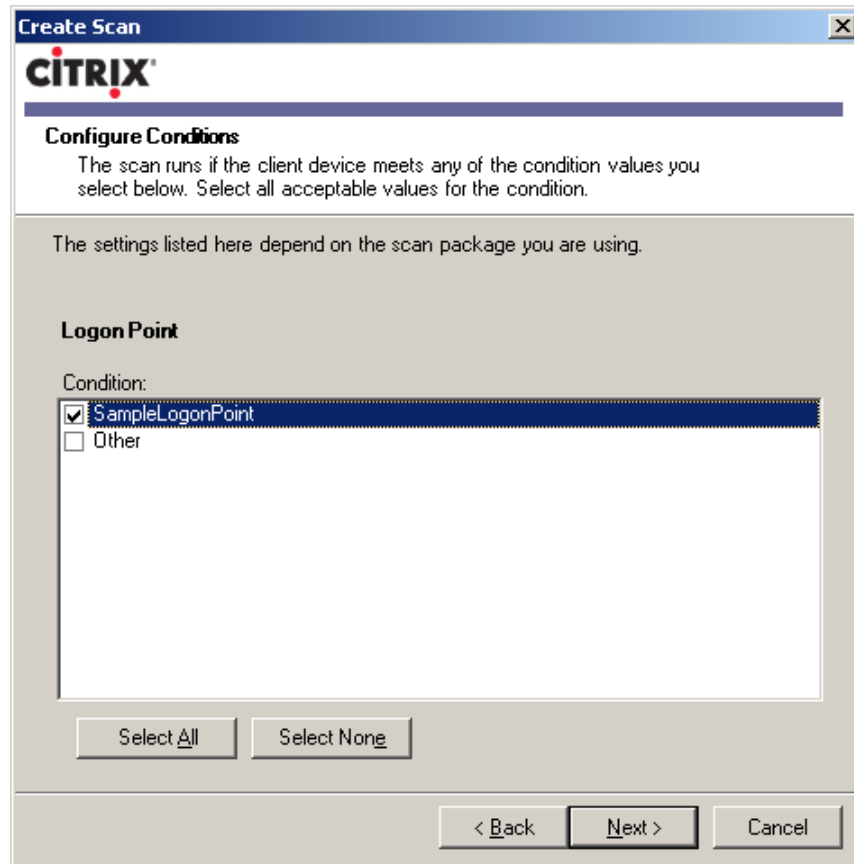
For example, your rule might be to use Scan X when the client device is running Operating System Y and Browser Version Z.

You can create multiple rules for any scan.

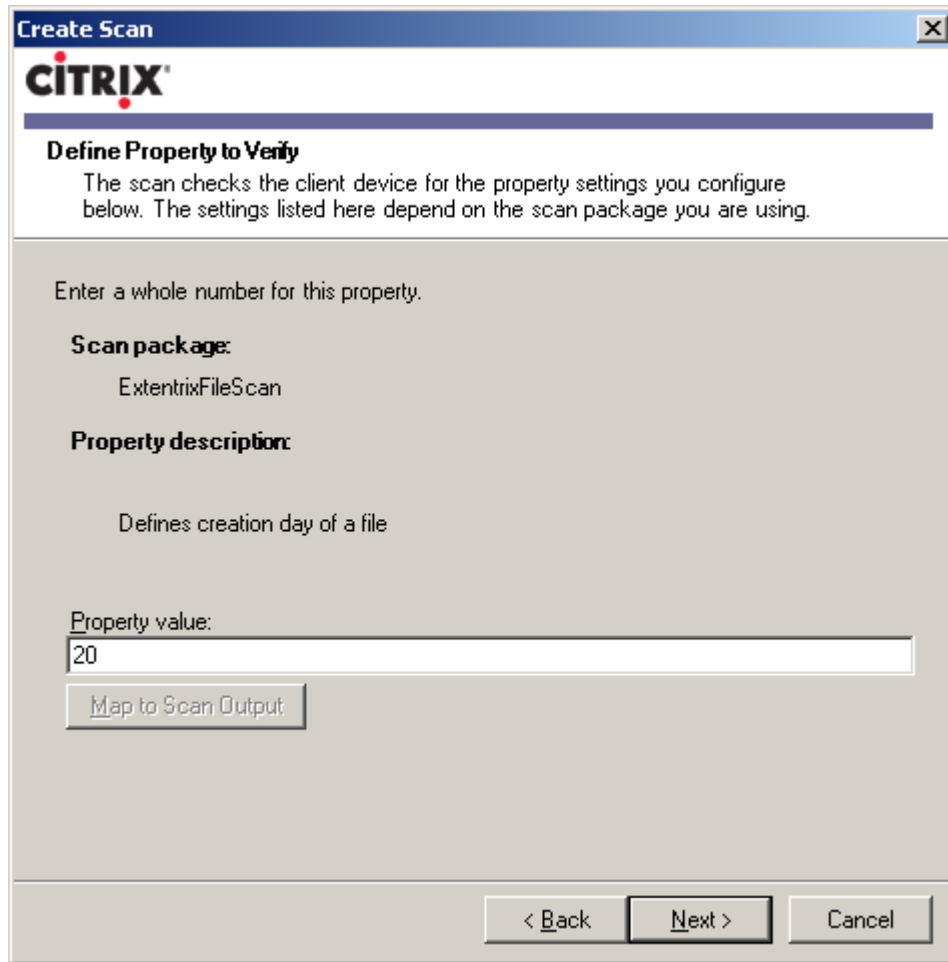
Rule name:

< Back Next > Cancel





5. Type the creation Day of the file you want as integer value.



6. Type the creation Month of the file you want as integer 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:
ExtentrixFileScan

Property description:
Defines the creation month of a given file

Property value:
10

Map to Scan Output

< Back Next > Cancel

7. Type the creation Year of the file you want as integer 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:
ExtentrixFileScan

Property description:
Defines the creation year of a given file.

Property value:
2007

Map to Scan Output

< Back Next > Cancel

8. Type file path of the file you want as simple string.

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 string value for this property.

Scan package:
ExtentrixFileScan

Property description:
Defines the Path of a given file. ex:C:\\MyCompany\\test.txt

Property value:
C:\\Documents and Settings\\Administrator\\Desktop\\Example.doc

Map to Scan Output

< Back Next > Cancel

9. Type file size of the file you want as long integer.

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 string value for this property.

Scan package:
ExtentrixFileScan

Property description:
Defines Size of a file in bytes

Property value:
6450

Map to Scan Output

< Back Finish Cancel

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

8. EXTENTRIX EXTENDED REGISTRY KEY SCAN

SCAN DESCRIPTION

Scan Name: Extentrix Extended Registry Key.

Description: It allows IT administrators to create a list of data for the key registry value and check if any of the client's machines have one of these values. For example, IT administrators can create scan to verify whether the client's machine name (stored in the registry) match any of its allowed list machine names. This will reduce the need to create a scan for each machine name.

Parameters:

- Base Registry Key: specifies the base registry key.
- Sub Key: specifies the sub key ex: Software\Extentrix.
- Value Name: specifies the name of the value.
- Value Type: specifies the type of the value.
- Value Data list: specifies the data of the value, it's a comma separator file contains data depend on search type; it could be, REG_SZ → String, REG_BINARY → Binary, REG_DWORD → Double Word.

Note: If the data is binary or dword, it should be written as hexadecimal without space ex:05f47e.

Note: If the data is string, then the WILD CHARACTER (?,*) is supported as well as the exact string.

Scan Output:

- Allow Access - a Boolean output which indicates whether the key or the value is registered on the client's machine or not.
 - TRUE – indicates that a given key/value is registered on the client's machine.
 - FALSE – indicates that a given key/value is not registered on the client's machine or contains wrong information.

- 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.

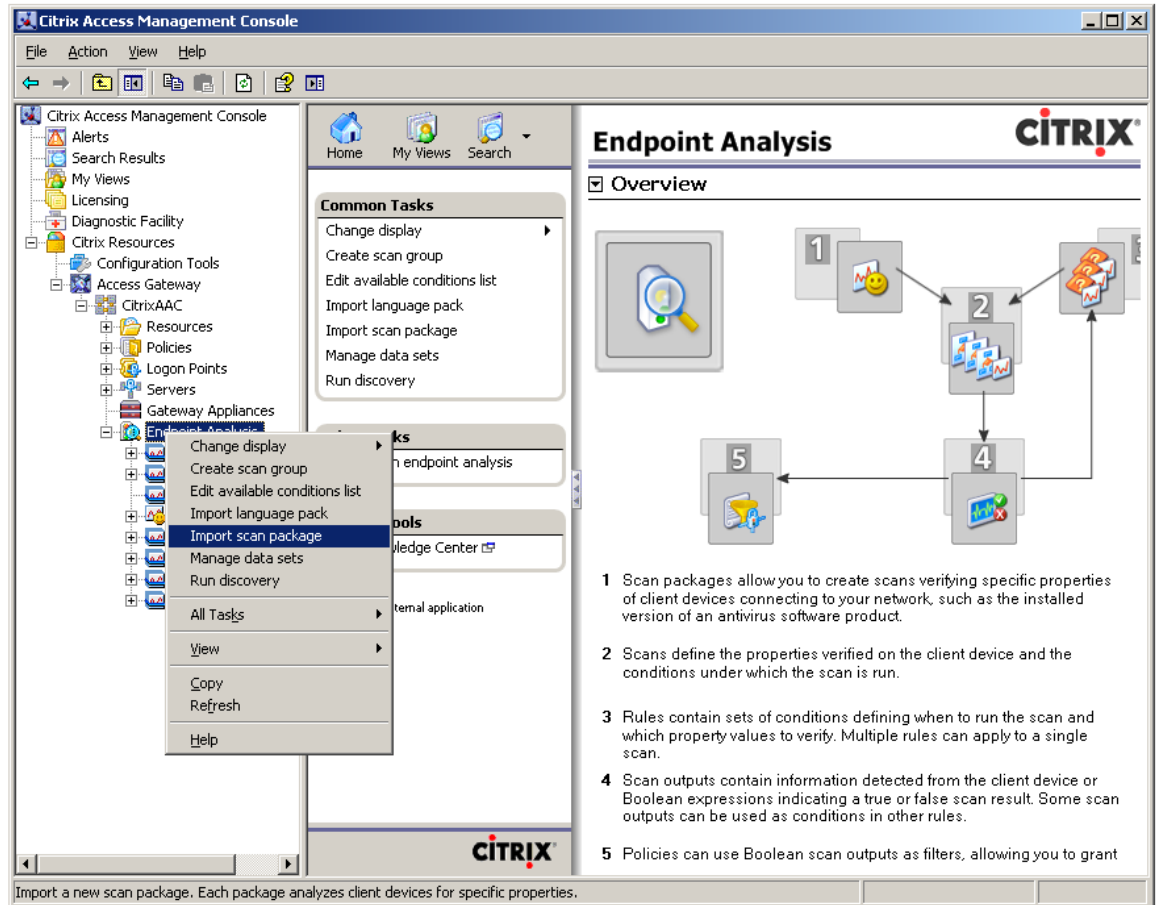
Note: If the License Status has an Invalid License value, the Allow Access will be false.

INSTALLATION AND CONFIGURATION

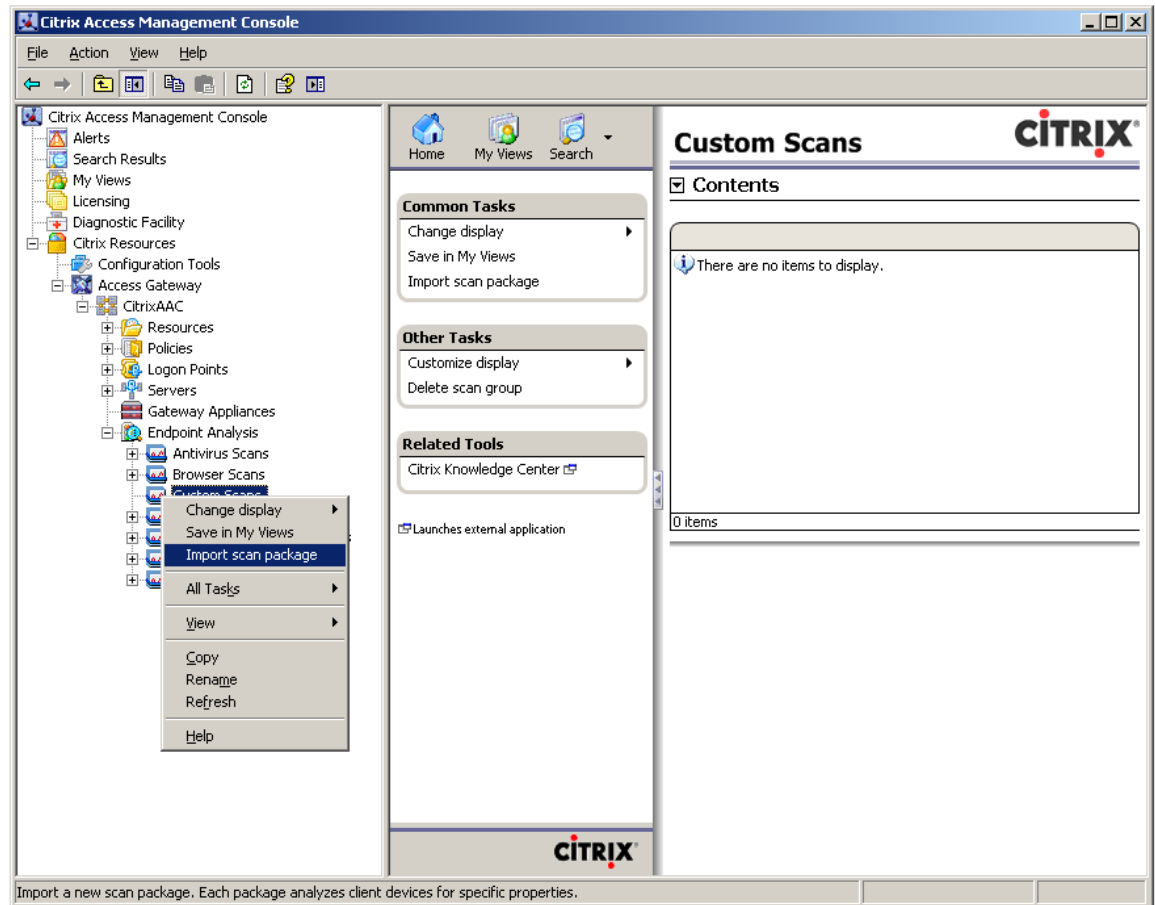
IMPORTING SCAN PACKAGES

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

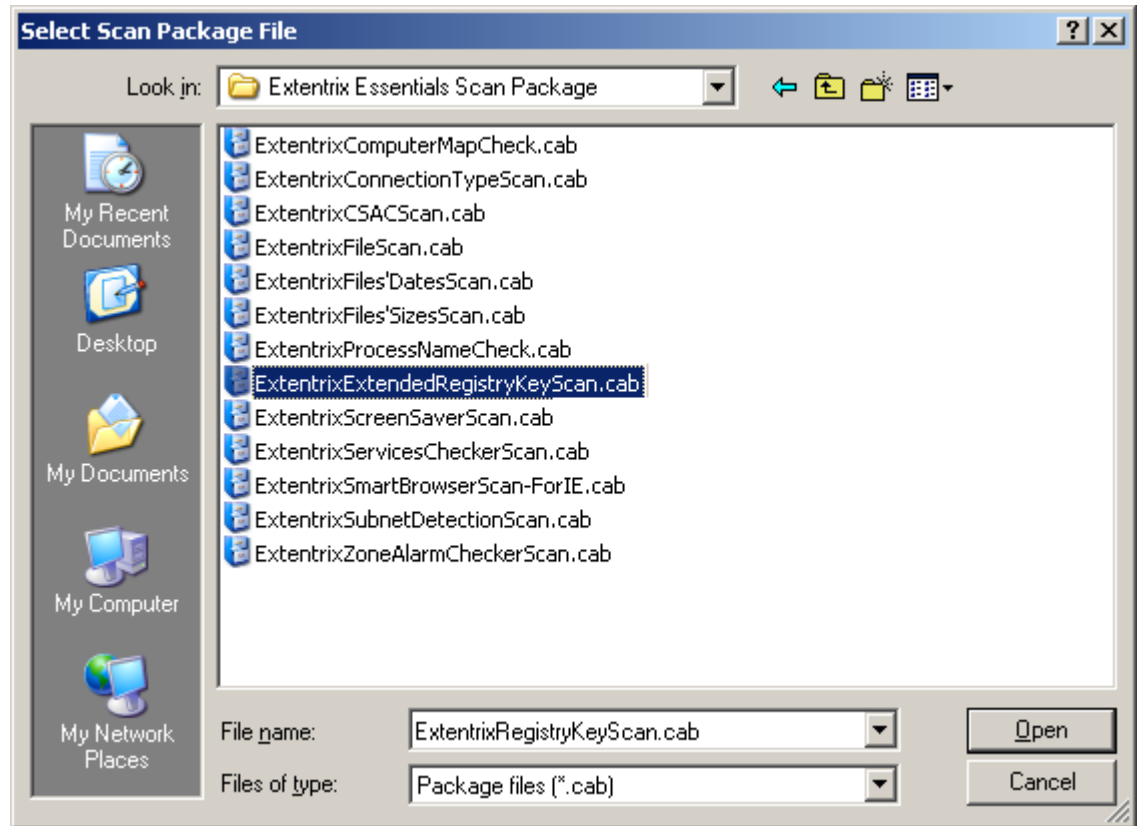
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



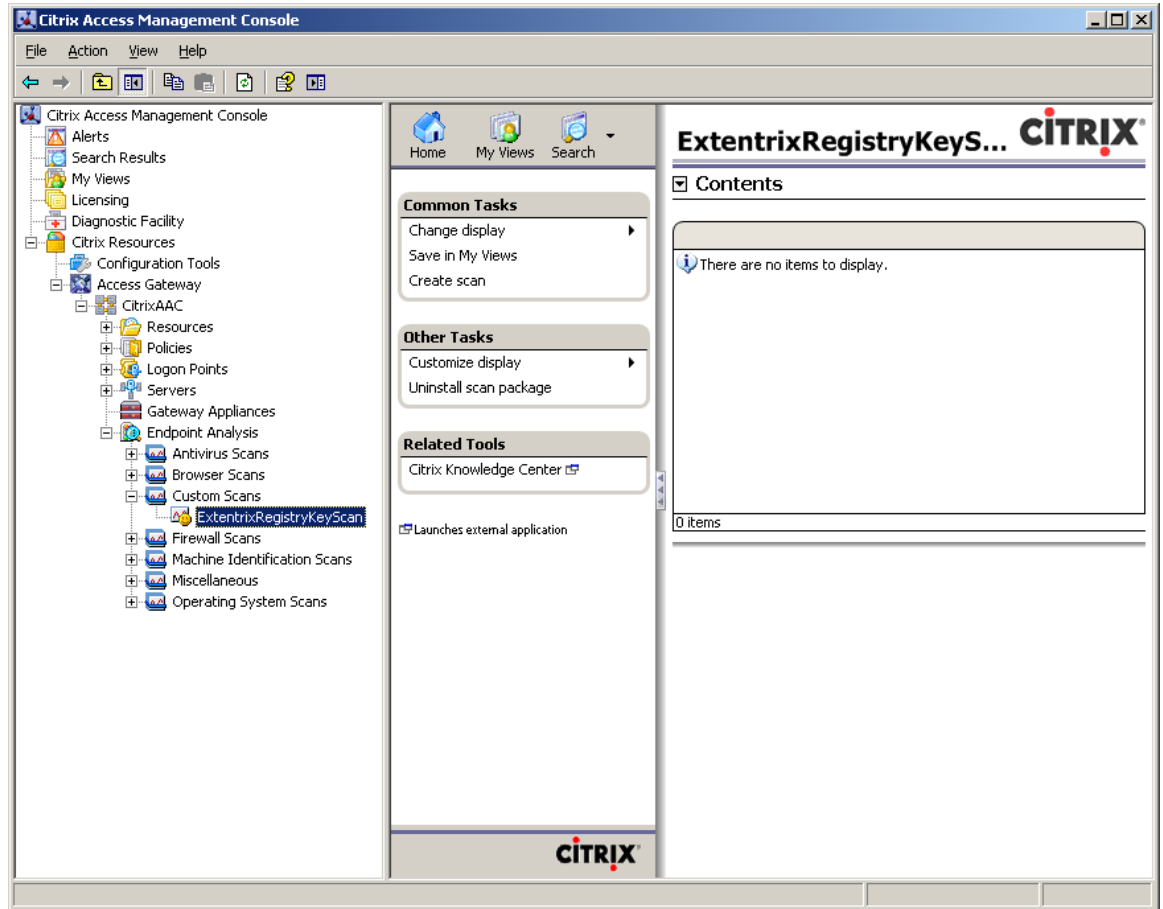
Also you can choose to insert the scan package to any scan category listed in the tree as shown in the following picture:



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



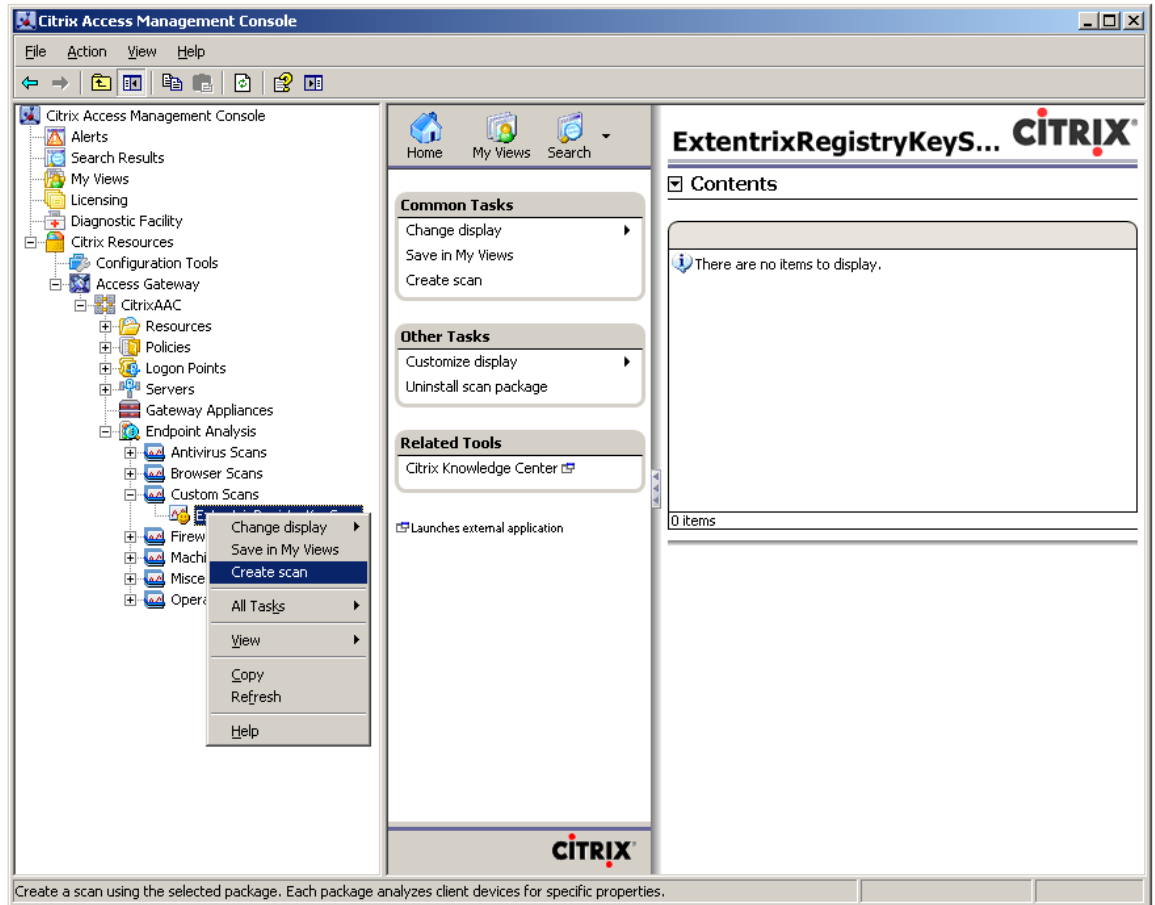
The package will be displayed in the console as shown in the following picture:



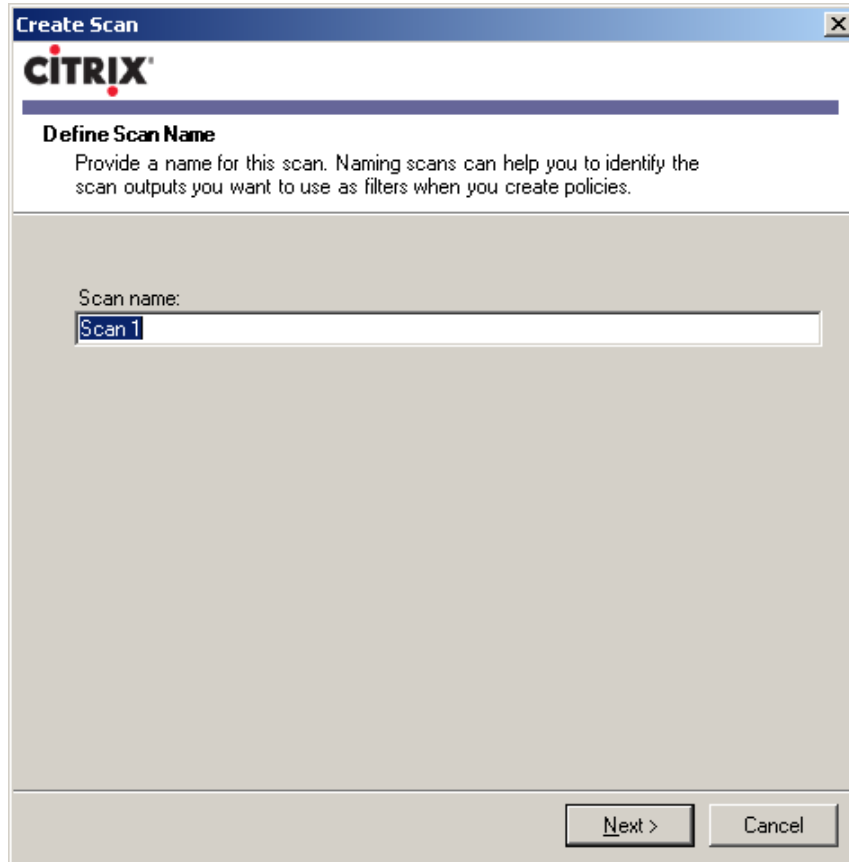
INSTALLING THE SCAN PACKAGE

Please follow the steps below to create scans and rules for the **Extentrix Extended Registry Key Scan**.

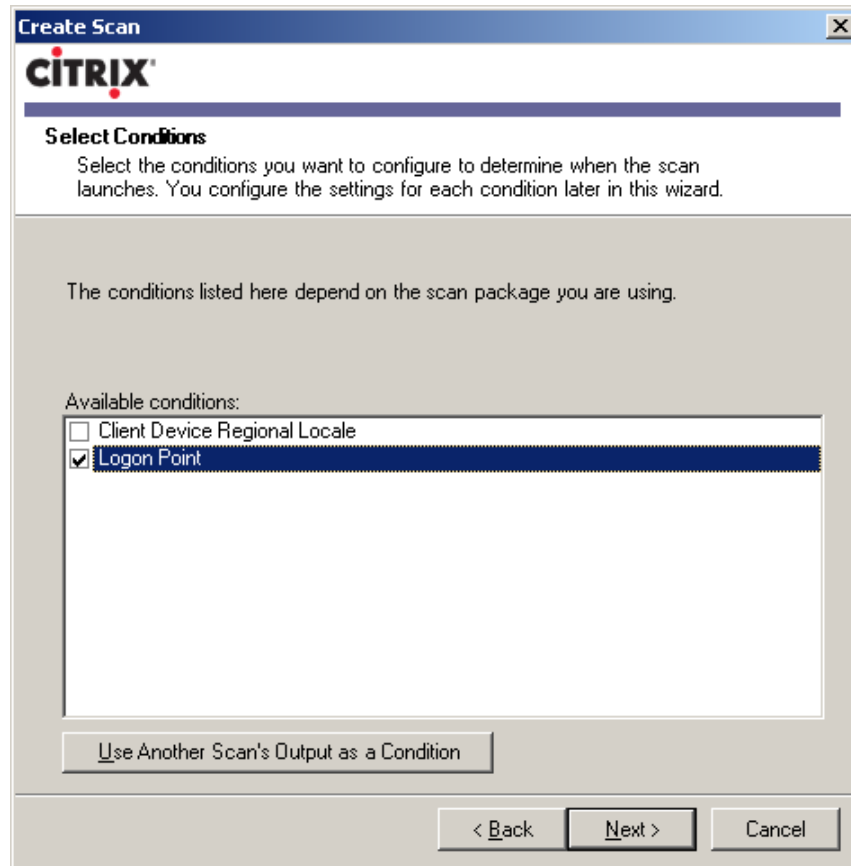
1. Select **ExtentrixExtendedRegistryKeyScan** to create scan for it, right click the icon and choose **Create Scan**.



2. Type a name for the scan:



3. Set the scan conditions:



4. Type rule name and set rule conditions:

Create Scan

CITRIX

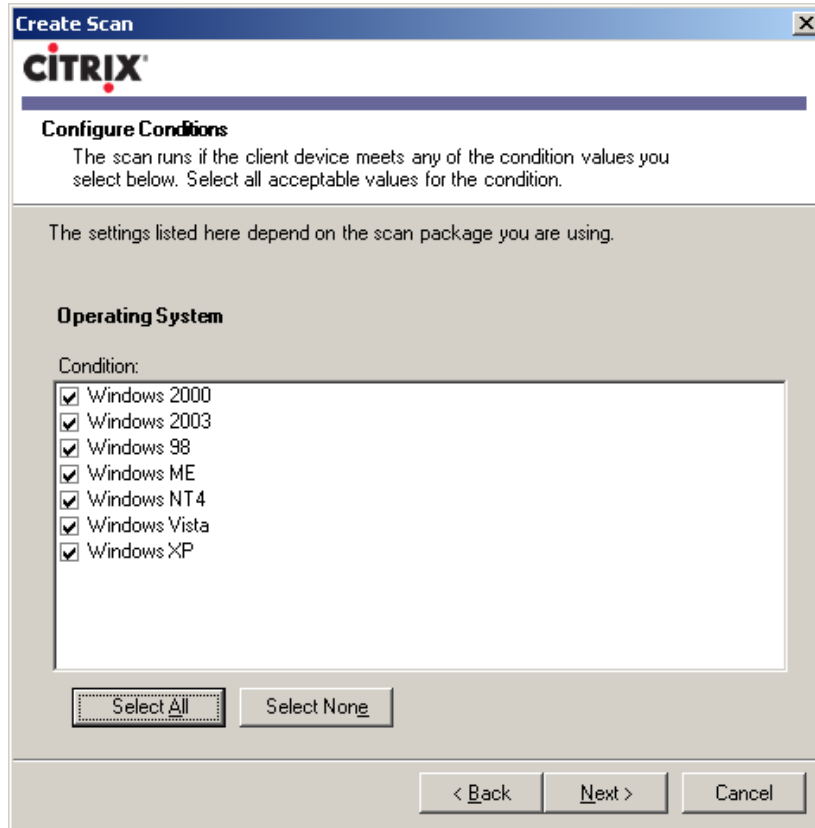
Define Rule
Rules are a combined set of conditions under which a scan is run.

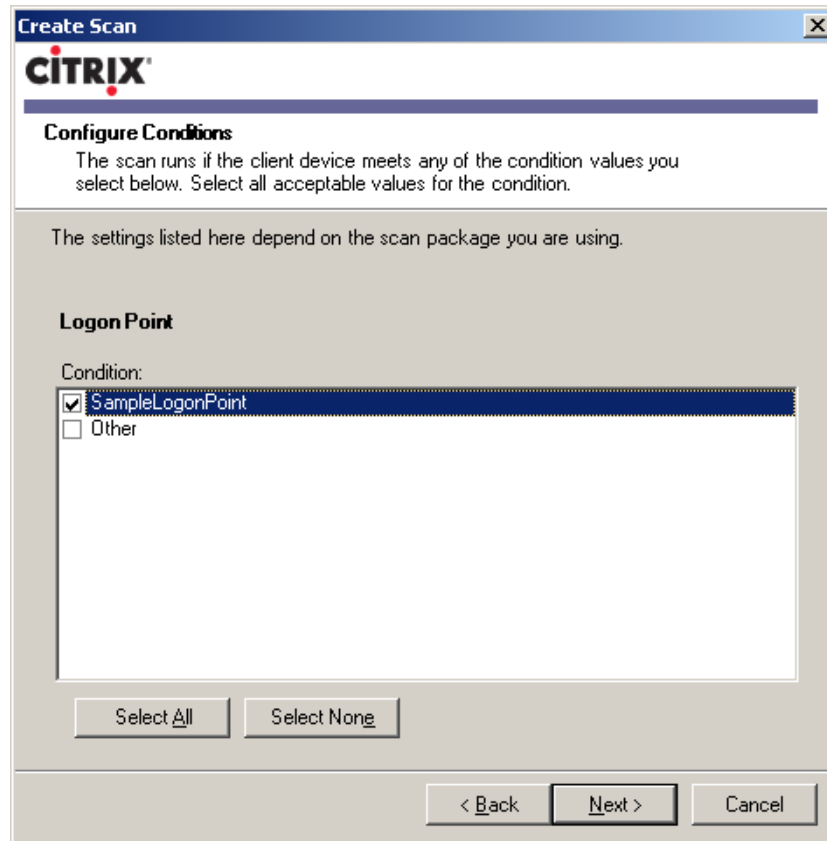
For example, your rule might be to use Scan X when the client device is running Operating System Y and Browser Version Z.

You can create multiple rules for any scan.

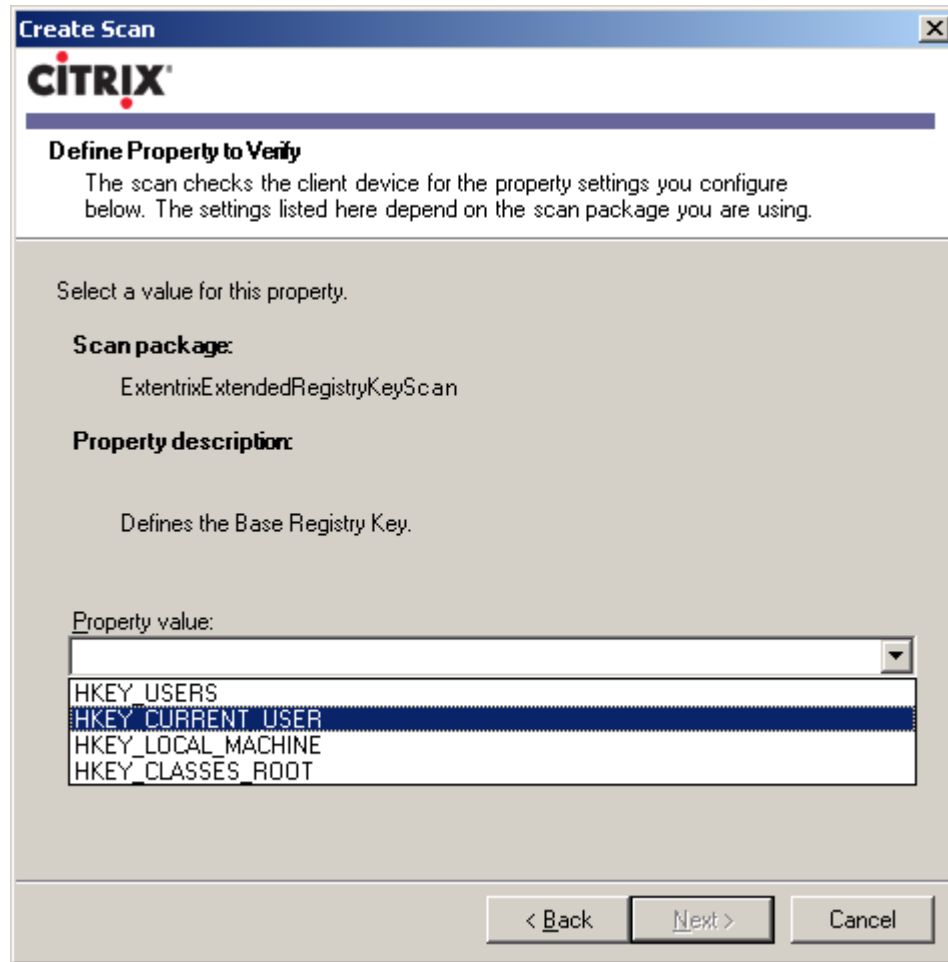
Rule name:

< Back Next > Cancel

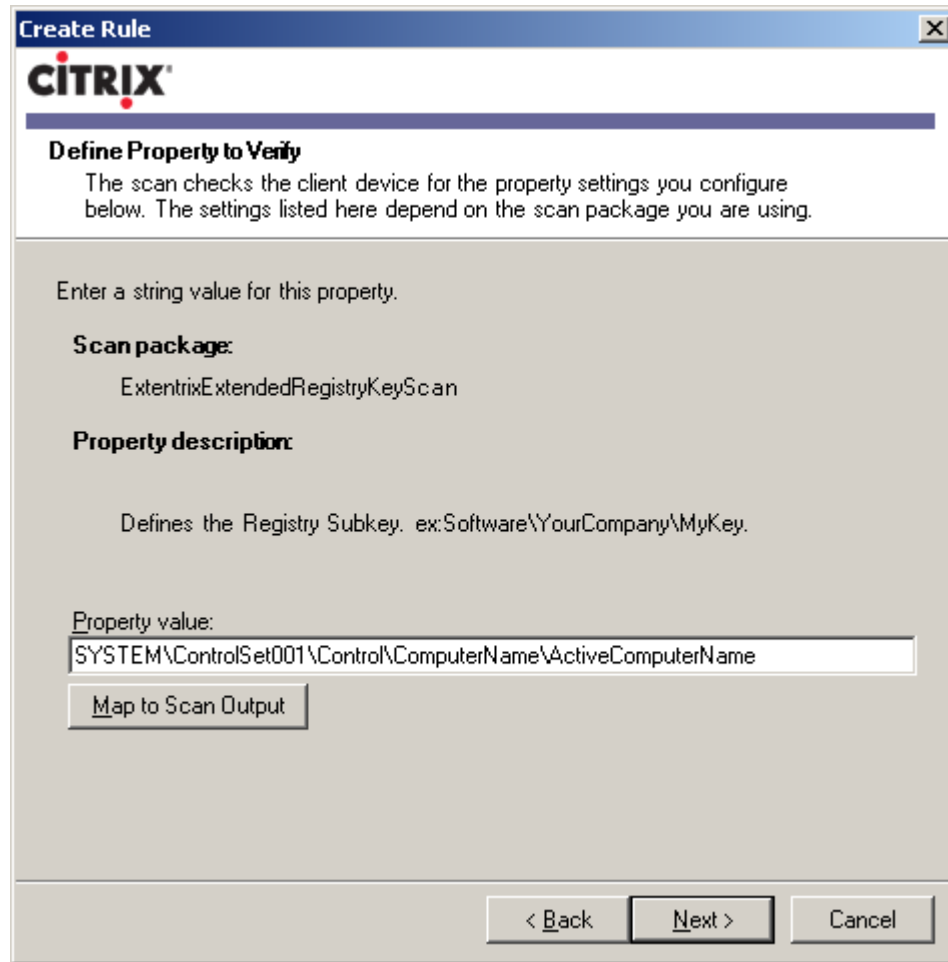




5. Choose a base registry key from the list:



6. Type the sub key to be checked.



7. Type the Value Name if you will check the value or NULL if you will not.

Create Rule

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 string value for this property.

Scan package:
 ExtentrixExtendedRegistryKeyScan

Property description:
 Defines the Name of the Value.

Property value:

< Back Next > Cancel

8. Choose the Type of the data from the list:

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.

Select a value for this property.

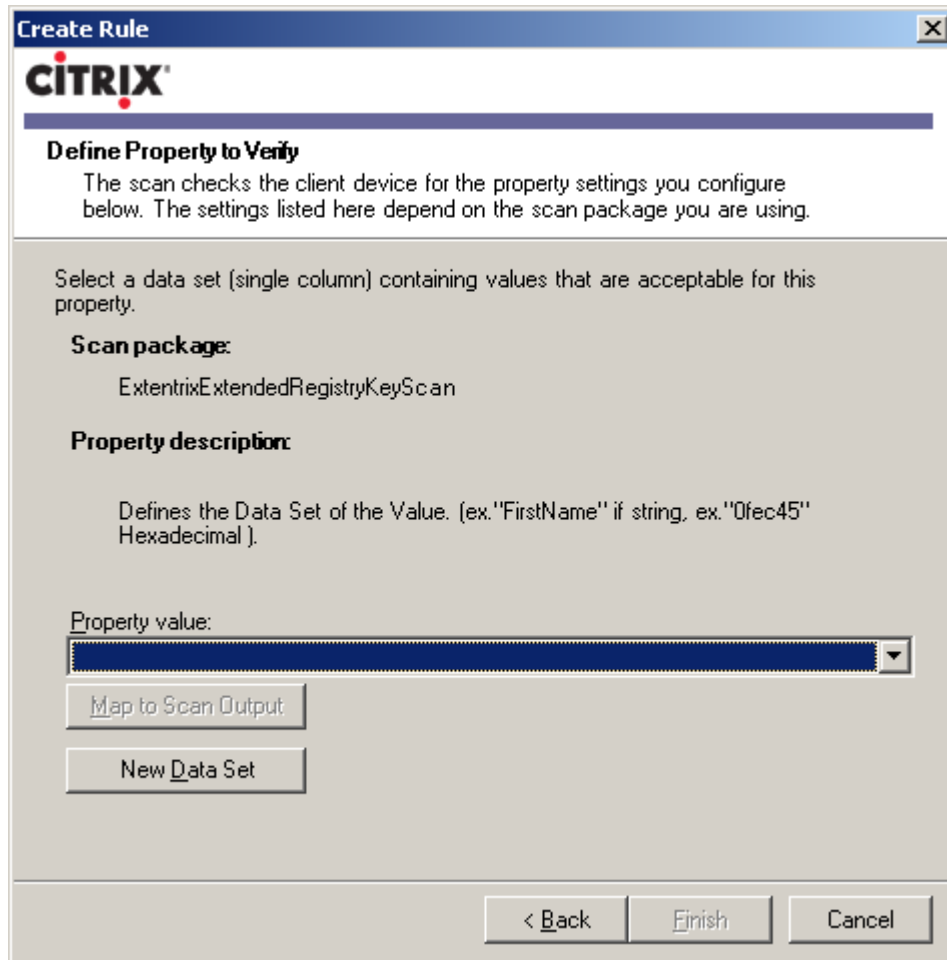
Scan package:
ExtentrixExtendedRegistryKeyScan

Property description:
Defines the Type of the Value.

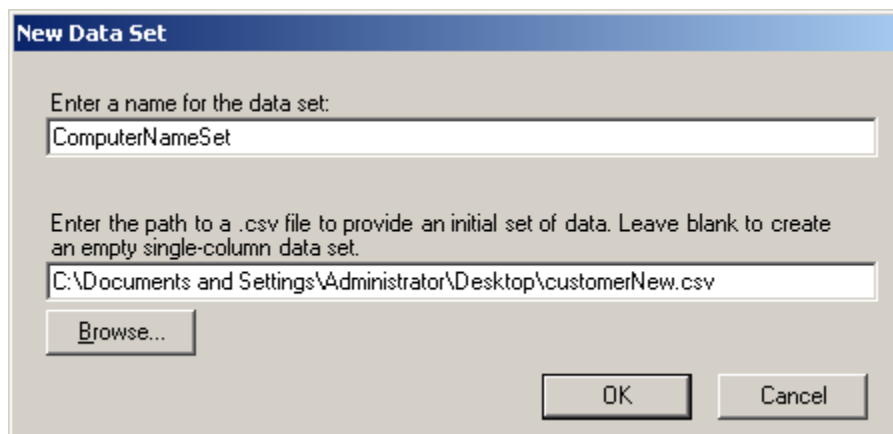
Property value:
REG_DWORD
REG_SZ
REG_BINARY

< Back Next > Cancel

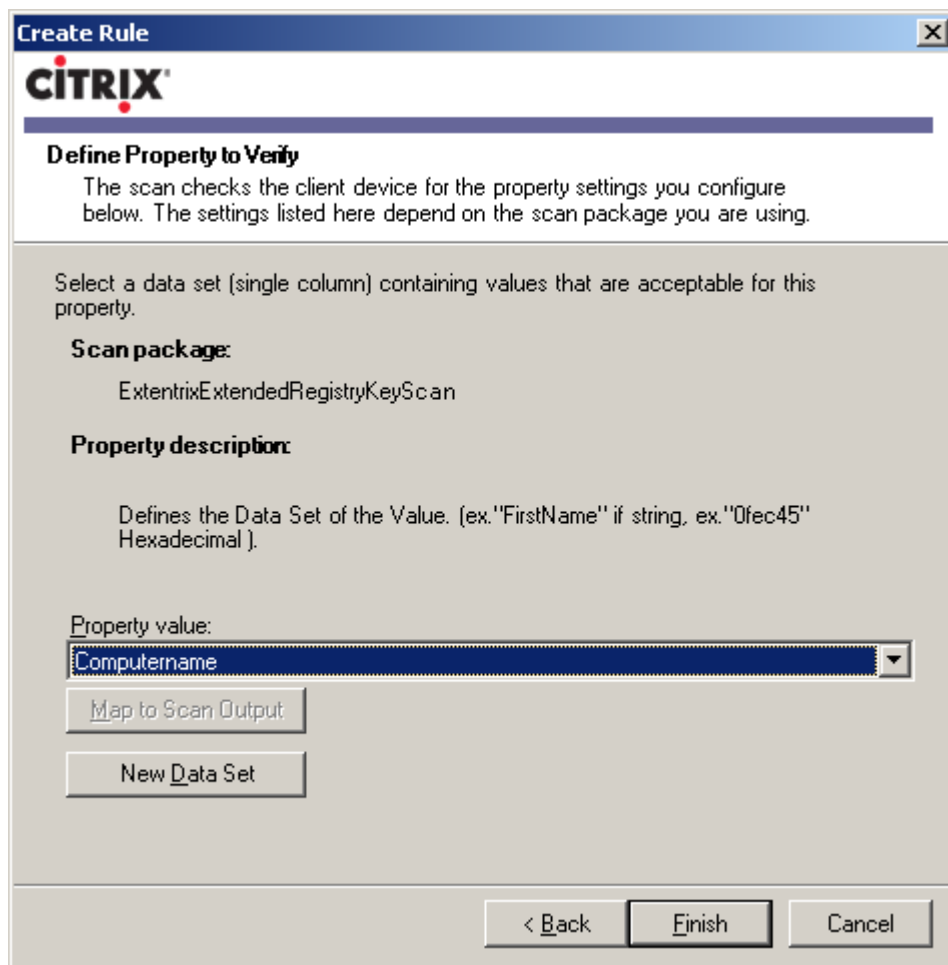
9. Define a data set using a comma delimited .csv file. To do that, click on **New Data Set** to import the file. The file will have a list of valid value for the key "String or Binary or Dword".



10. A dialog box titled “New Data Set” will appear. Type a name for the new data set in the first field then use **Browse** Button to locate the .csv file.



11. After defining the data set, click **Next**.

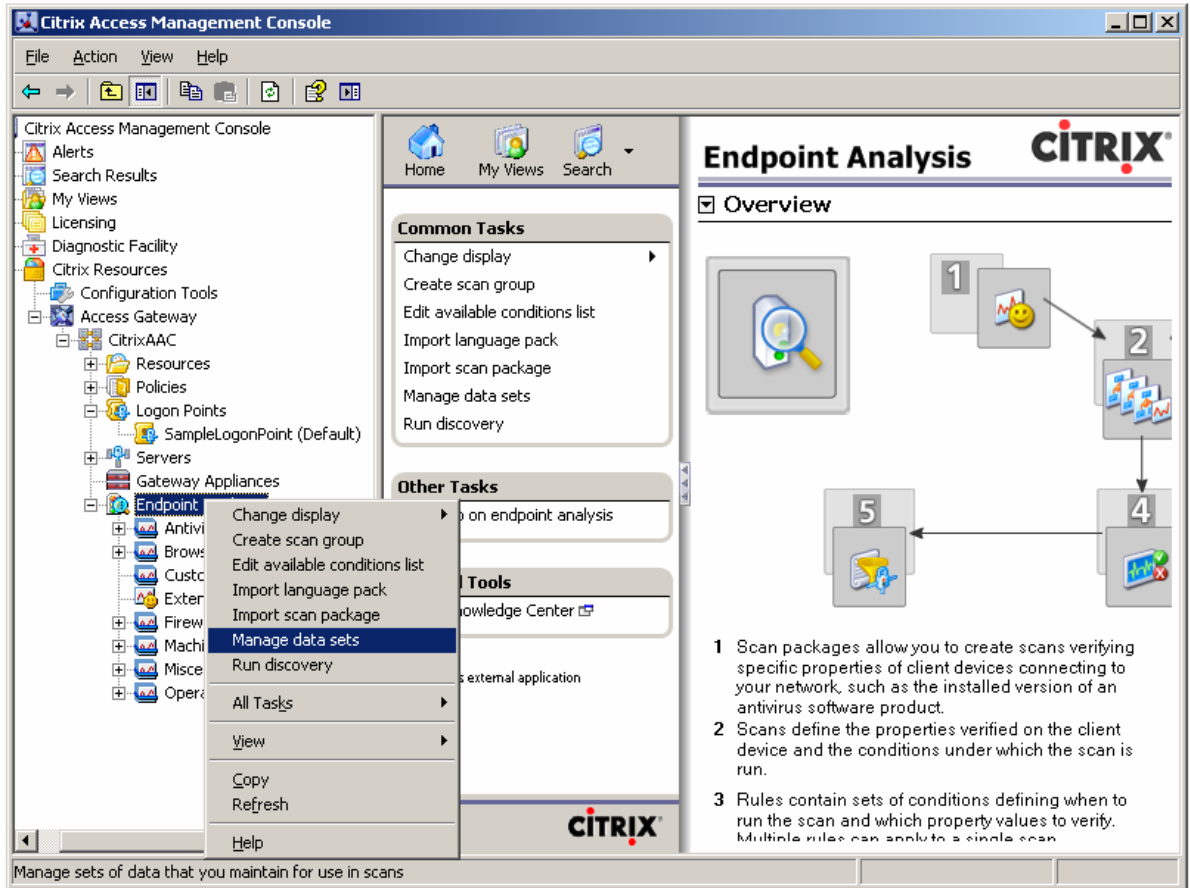


12. When you are done, click **Finish**.

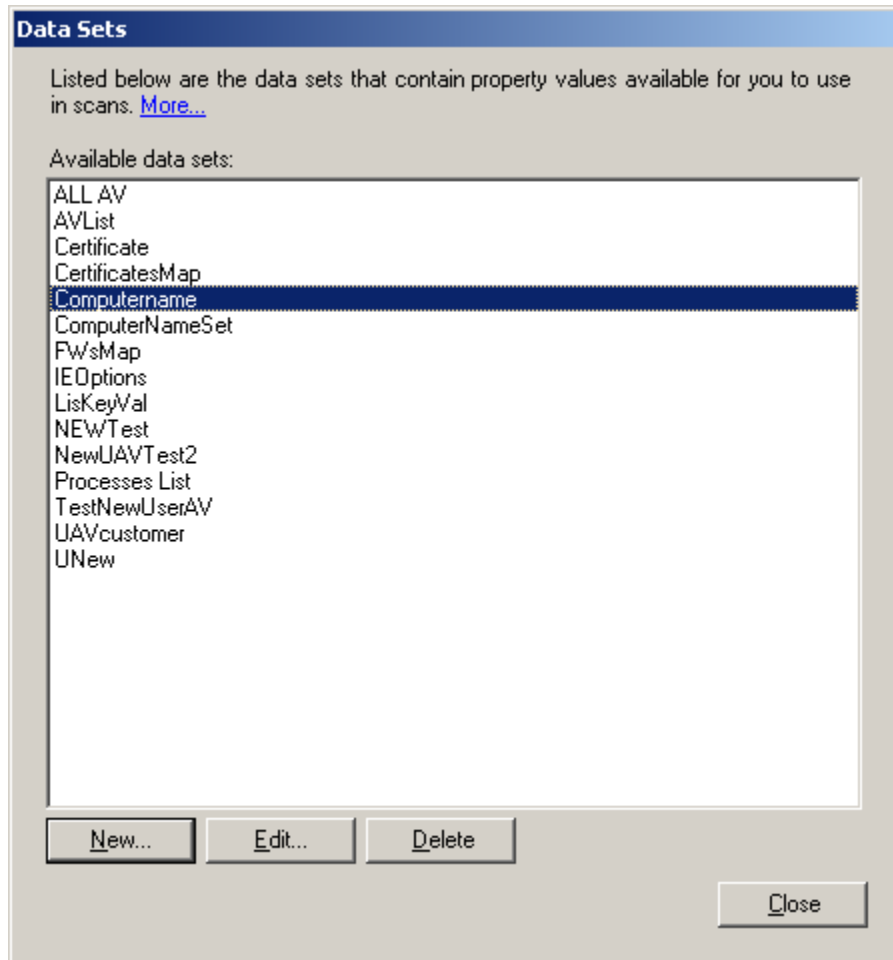
Editing Extentrix Key Register Scan Data Set

You can edit the value of the set later after creating the data set to change values or remove or add options. The following steps demonstrate how you can do that:

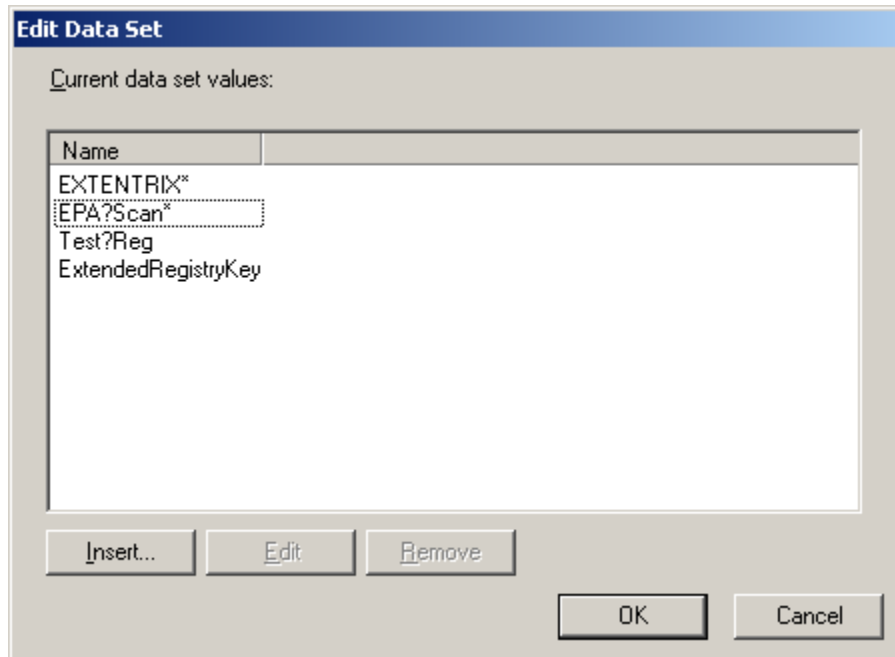
1. Right click **Endpoint Analysis** in the management console tree and select **Manage Data Set** from the action menu.



2. A window titled “Data Sets” will appear. Select the data set you want to edit then click **Edit** button.



3. A window titled **"Edit Data Set"** will appear.



Note: You can use string with wild character (?,*) as well as exact string .

4. In this dialog box, you can insert a new value, edit an existing value or remove unwanted value, then click **OK**.

9. EXTENTRIX WORKING HOURS SCAN

SCAN DESCRIPTION

Scan Name: Extentrix Working Hours Scan.

Description: Extentrix Working Hours Scan by Extentrix Systems will empower administrators with the ability to allow users an access to company resources at predefined Working Hours, so Administrator can predefine working hour (12:15 – 23:55) if user connects to company during this time then the access will be accepted, but if he/she tries to connect in any invalid time then a warning message appears and the access will be denied.

Parameters:

- Working Hours Start at: Defines the start time in 24 formats (HH:MM).
- Working Hours Finish at: Defines the finish time in 24 formats (HH:MM).
- Warning Message: A string value represents a warning message that will be displayed if user had accessed the company's web site outside predefined working hours.

Scan Output:

- Allow Access- a Boolean output which indicates whether the file you specified matches the client environment or not.
 - TRUE – indicates that user connected to company at predefine working hours.
 - FALSE – indicates that user connected to company at invalid time.
- 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.

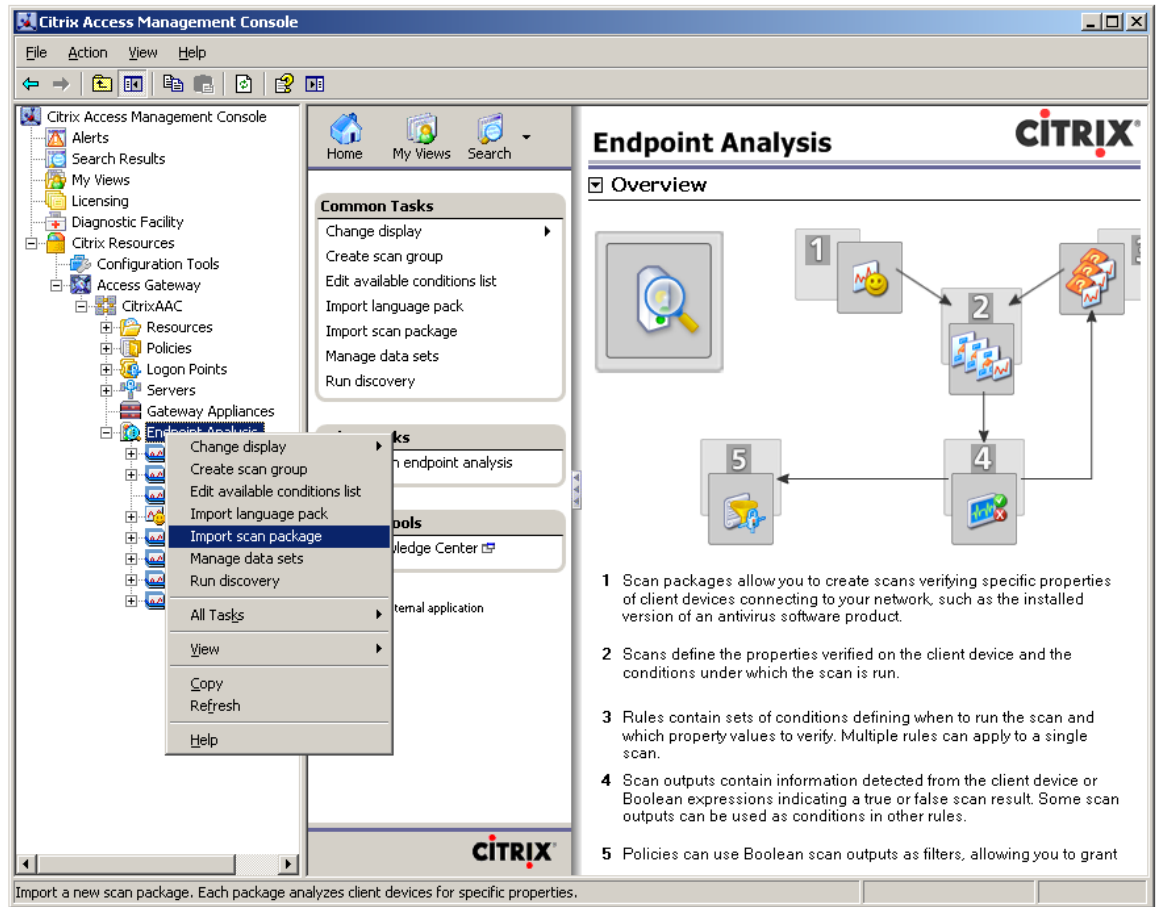
Note: If the license status has an invalid license value, the allow access will be false.

INSTALLATION AND CONFIGURATION

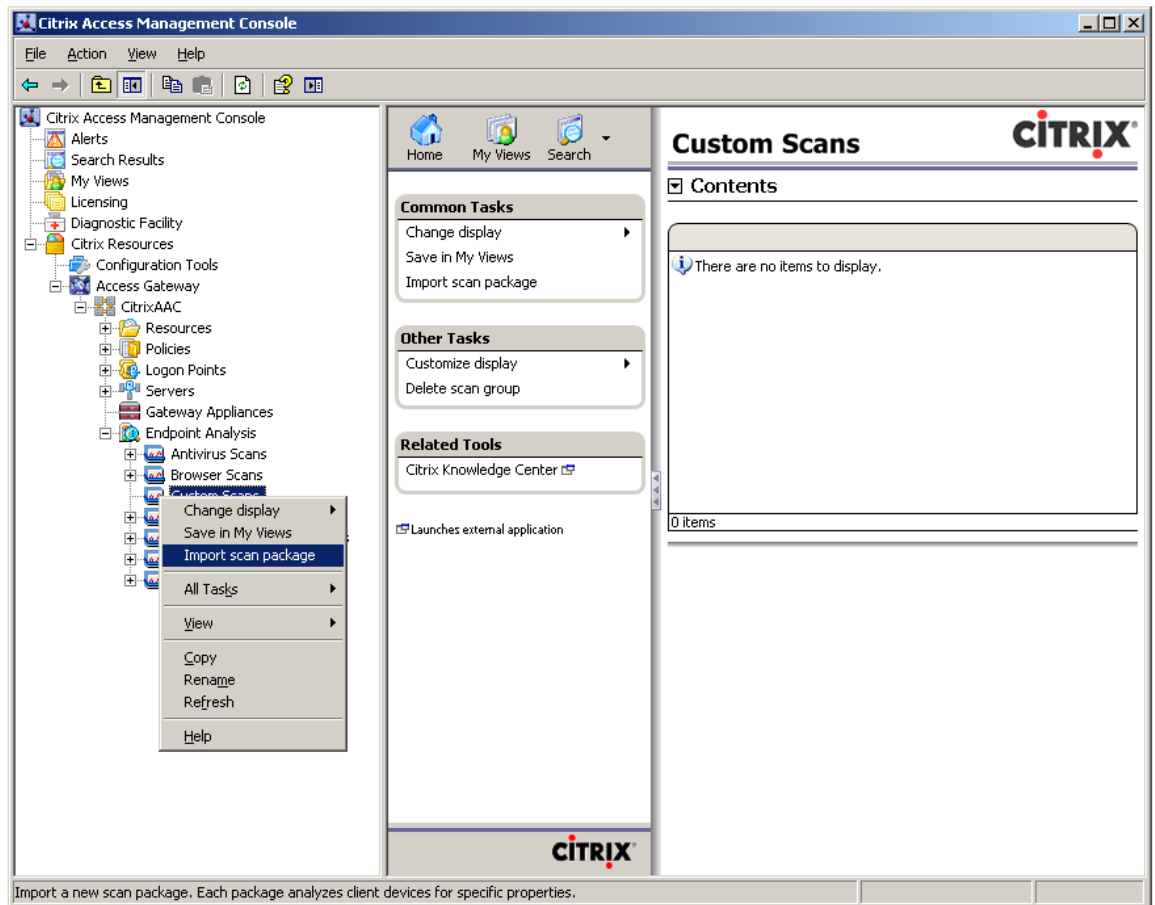
IMPORTING SCAN PACKAGES

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

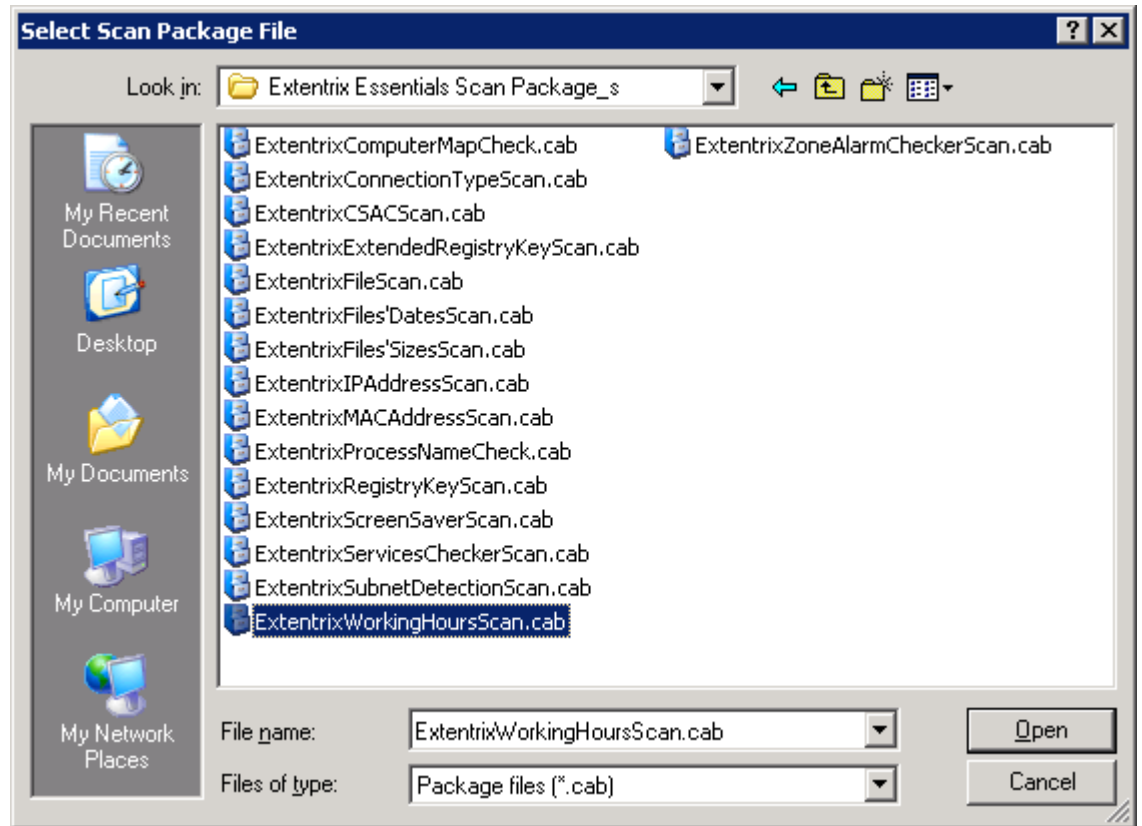
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



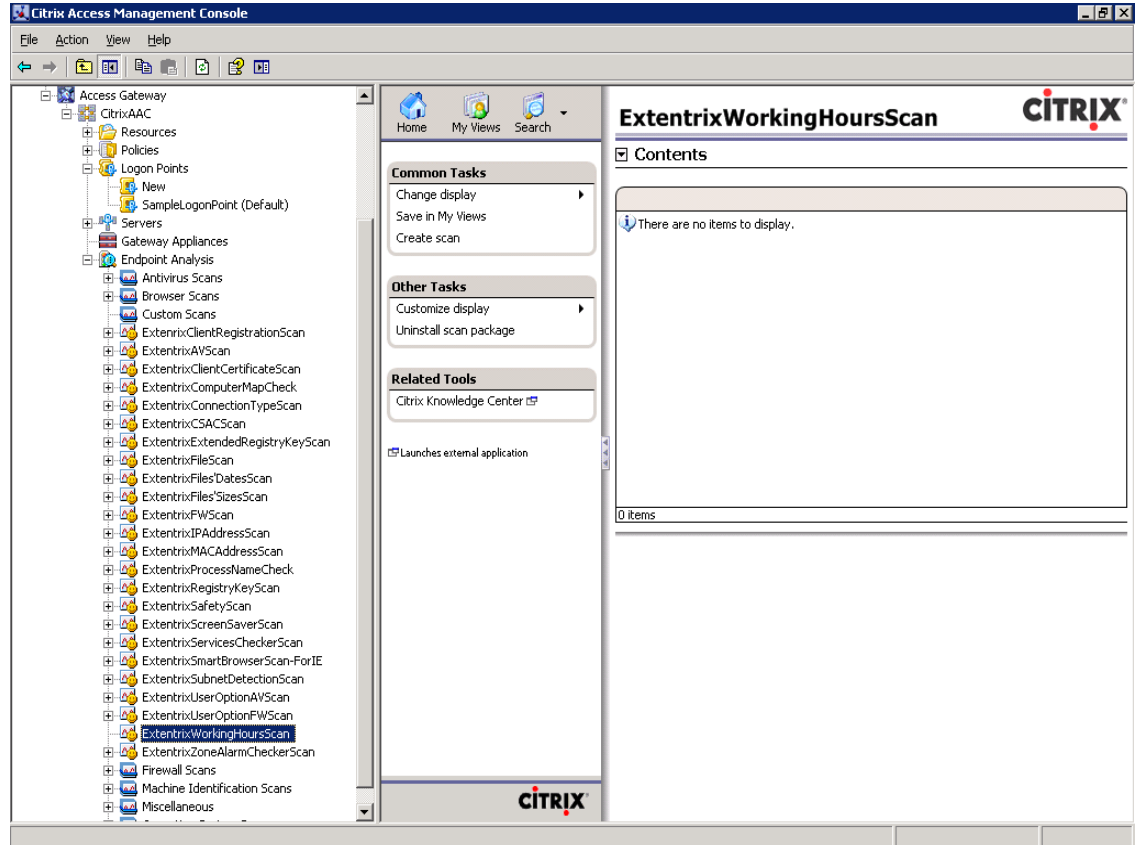
Also you can choose?? to insert the scan package to a specific scan package group as shown in the following picture:



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



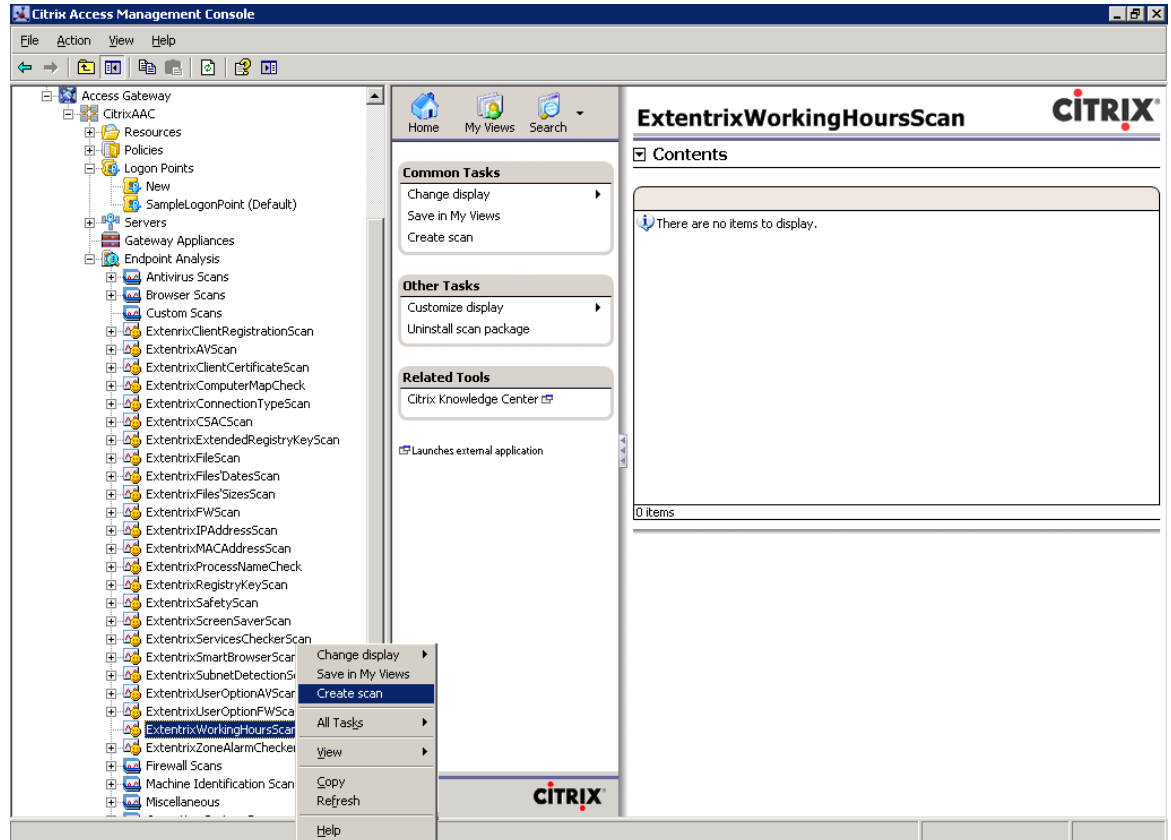
The package will be displayed in the console as shown in the following picture:



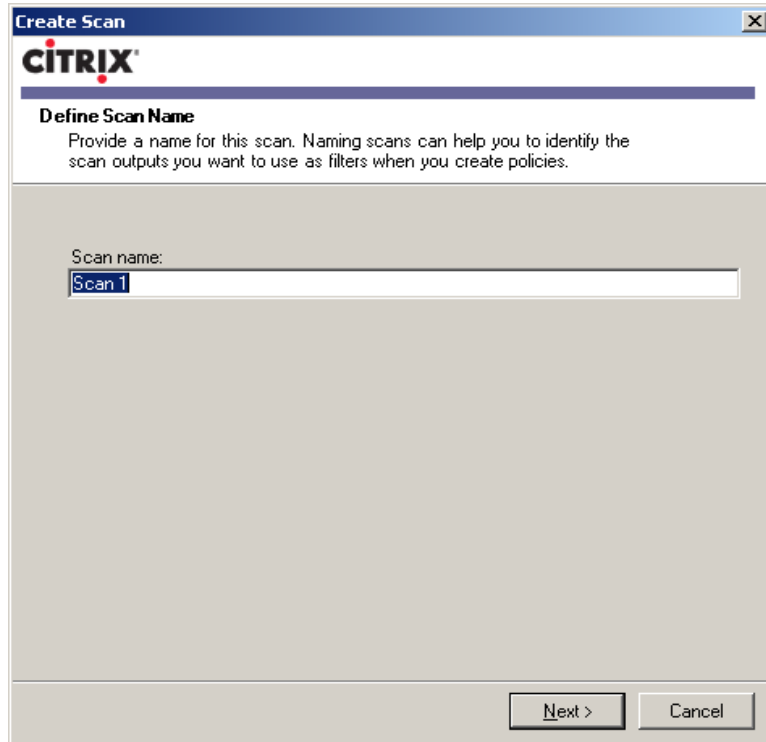
INSTALLING THE SCAN PACKAGE

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

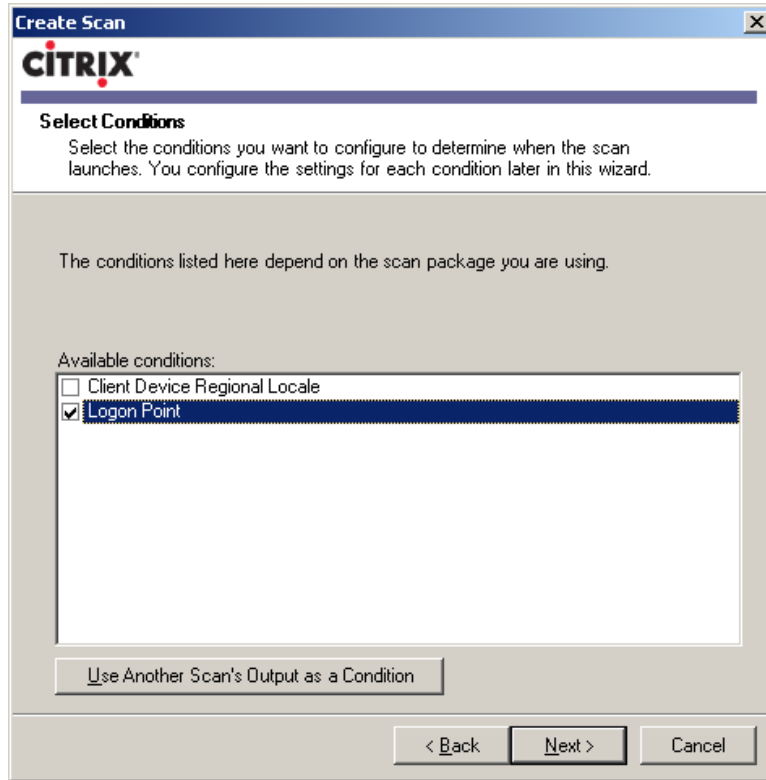
1. Select **Extentrix Working Hours Scan** to create scan for it, right click the icon and choose **Create scan**.



2. Type a name for the scan:



3. Set the scan conditions:



4. Type rule name and set rule conditions:

Create Scan

CITRIX

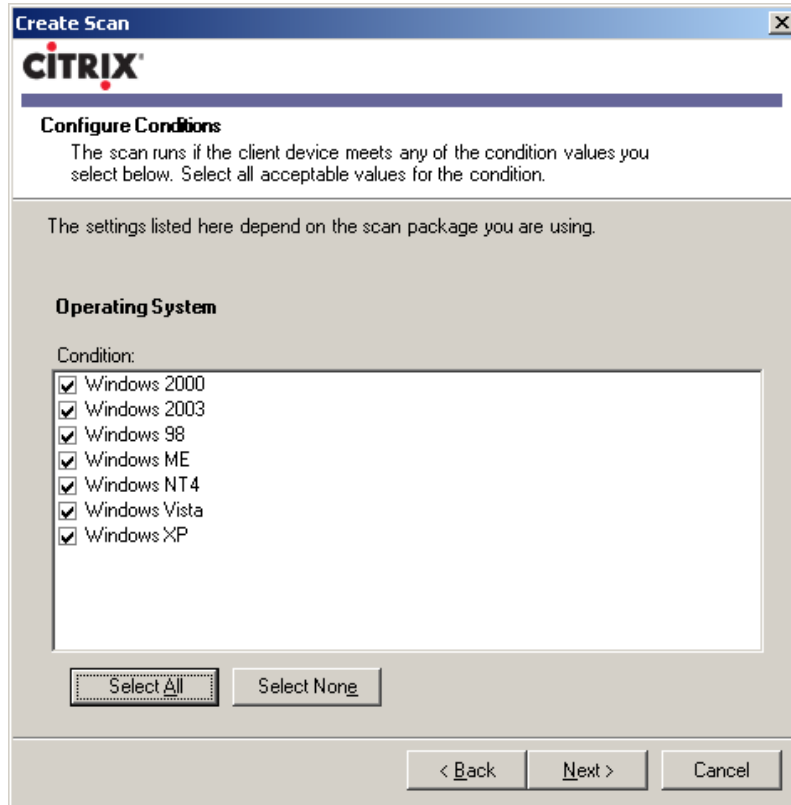
Define Rule
Rules are a combined set of conditions under which a scan is run.

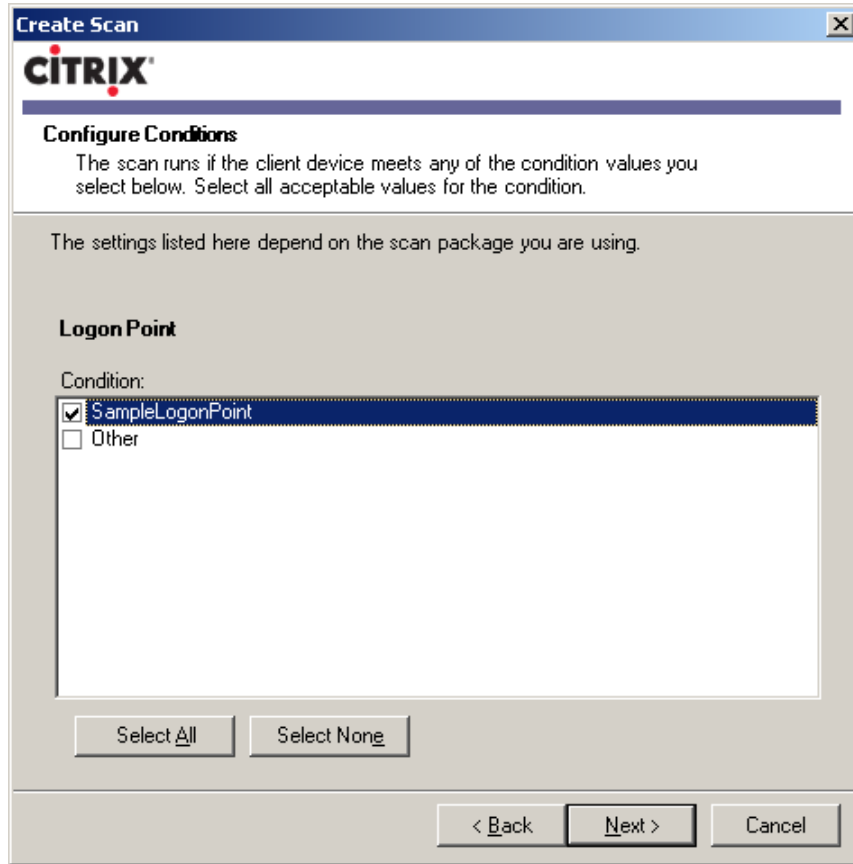
For example, your rule might be to use Scan X when the client device is running Operating System Y and Browser Version Z.

You can create multiple rules for any scan.

Rule name:

< Back Next > Cancel





5. Type the Working Hours Start at (in 24 Format HH:MM).

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 string value for this property.

Scan package:
 ExtentrixWorkingHoursScan

Property description:
 Defines the Start time in 24 format (HH:MM)

Property value:

< Back Next > Cancel

6. Type the Working Hours Finish at (in 24 Format HH:MM).

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 string value for this property.


Scan package:
 ExtentrixWorkingHoursScan

Property description:
 Defines the Finish time in 24 format (HH:MM)

Property value:

7. Type Warning Message.

Create Scan
✕



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 string value for this property.

Scan package:
ExtentrixWorkingHoursScan

Property description:

A string value represents a warning message that will be displayed if user had accessed the company's web site outside predefined working hours.

Property value:

SUPPORT

Support for Extentrix Essentials 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, 158

Endpoint Analysis Client, 158

Extentrix File Scan, 104

Extentrix Files' Dates Scan, 70

Extentrix Files' Size Scan, 87

Extentrix Process Name Check, 6

Extentrix Registry Key Scan, 24, 121

Extentrix Screen Saver Scan, 41

Extentrix Services Checker Scan, 54

I

Importing scan packages, 7, 26, 42, 55, 71, 88, 105, 123, 143

Installing the scan package, 12, 30, 46, 59, 75, 93, 110, 127, 148

Introduction, 5

P

Parameters, 6, 24, 41, 54, 70, 87, 104, 121, 142

S

Scan Output, 6, 24, 41, 54, 70, 87, 104, 121, 142

support, 157

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/>.