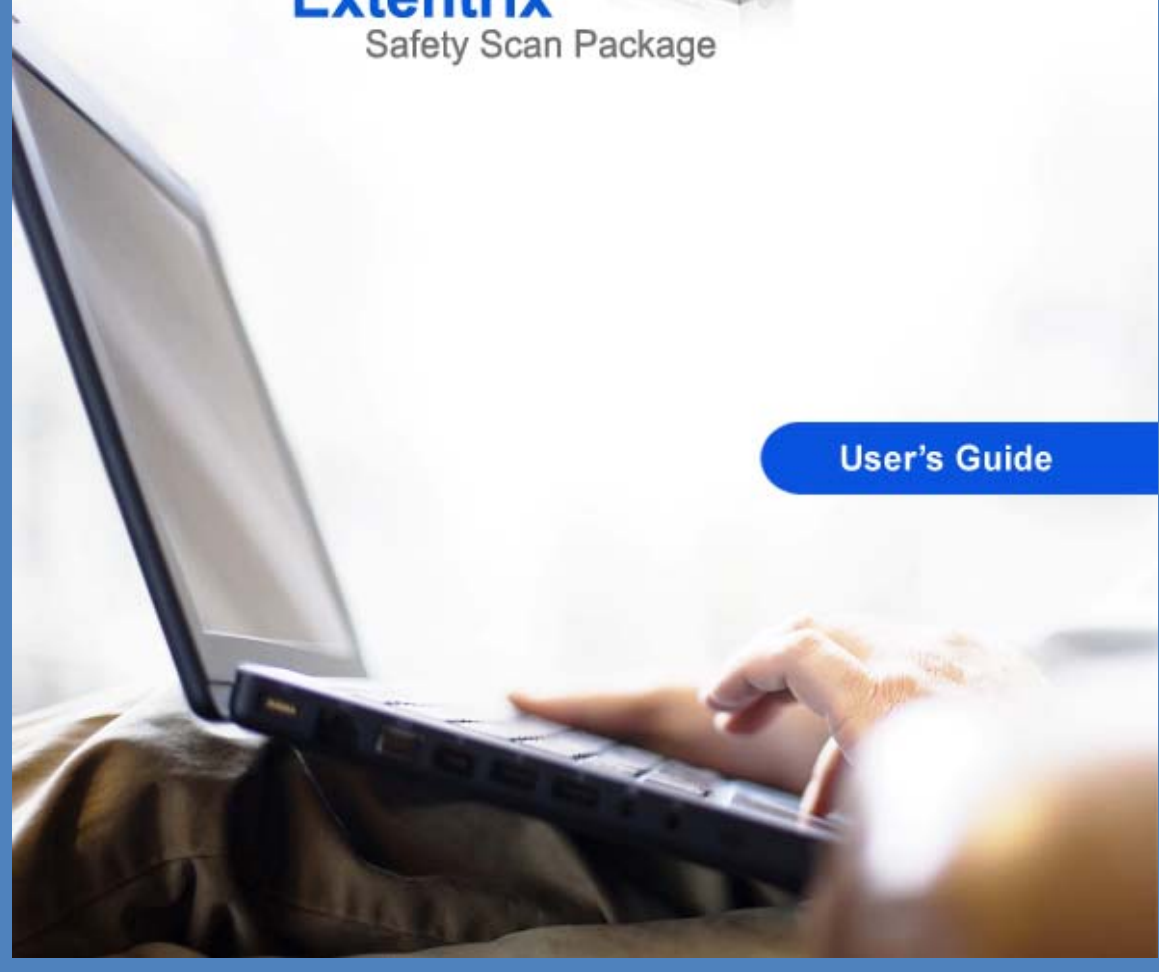


extentrix



Extentrix
Safety 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	3
SCANS INCLUDED INSIDE EXTENTRIX SAFETY SCAN PACKAGE.....	4
1. EXTENTRIX SAFETY SCAN	4
<i>Scan description</i>	<i>4</i>
<i>Installation and configuration.....</i>	<i>5</i>
2. EXTENTRIX SMART BROWSER SCAN- FOR IE	16
<i>Scan description</i>	<i>16</i>
<i>Installation and configuration.....</i>	<i>17</i>
SUPPORT.....	32
GLOSSARY	33
INDEX.....	34
ABOUT EXTENTRIX	35

INTRODUCTION

Extentrix Safety Scan Package supports the Citrix Access Gateway™ SSL VPN technology, a key feature of Citrix Presentation Server™ Platinum Edition. Extentrix works with Citrix Access Gateway to provide end-to-end security and safeguarding for users accessing system resources from Internet cafes and kiosks, ensuring that the data accessed is not inadvertently left behind for someone else to view or use.

Through safety scan package, Extentrix worked on raising the security level for users accessing system resources and made sure that every temporary data will be deleted after logging out and is not inadvertently left behind for someone else to view or use.

After logging out, Extentrix Safety Scan Package provides an ActiveX Control to ensure that the data accessed is not inadvertently left behind for someone else to view or use. It deletes all the important data as history, cached pages, forms data, and any sensitive data there. Extentrix Safety Scan Package consists of:

1. Distributed Files:

- EPAClient.exe
- Append.txt
- Extentrix IE Cleanup ActiveX.ocx

2. Scans:

- Extentrix Safety Scan
- Extentrix Smart Browser Scan- for IE

SCANS INCLUDED INSIDE EXTENTRIX SAFETY SCAN PACKAGE

Extentrix Safety Scan Package contains the following Scan inside:

1. EXTENTRIX SAFETY SCAN**SCAN DESCRIPTION**

Scan Name: Extentrix Safety Scan.

Description: Extentrix Safety Scan is produced to ensure a highly secure access environment for administrators whom system resources are accessed. It is an end-to-end security Scan that includes safeguards for users accessing system resources from internet cafes and kiosks. It has control over Internet Explorer cache, history, and cookies for it deletes any important data left behind by users who access corporate resources.

Parameters: None.

Scan Output:

- Deletion Status- a Boolean output which indicates whether the Temporary Internet Explorer Files, History files, and Cookies are deleted completely or not.

TRUE – indicates that all Temporary Internet, History, and Cookies files are deleted from the client's machine.

FALSE – indicates that at least one of Temporary Internet, History, and Cookies files is not deleted from the client's machine.
- License Status- a String output which indicates whether the scan is licensed or not.

TRIAL LICENSE – Indicates that the scan still in 30 days trial period.

INVALID LICENSE – Indicates that the scan is not licensed.

VALID LICENSE – Indicates that the scan is licensed.

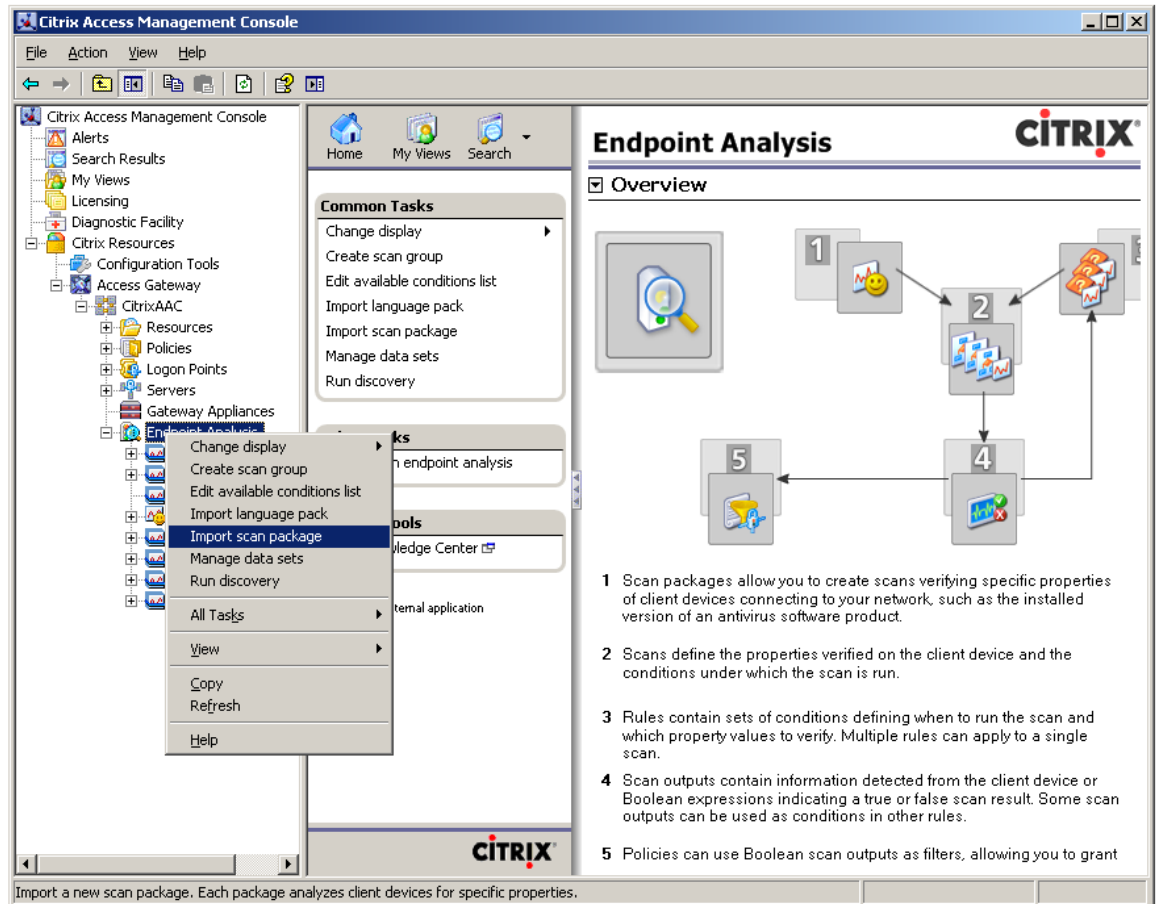
Note: If the License Status has an Invalid License value, the Deletion Status will be false.

INSTALLATION AND CONFIGURATION

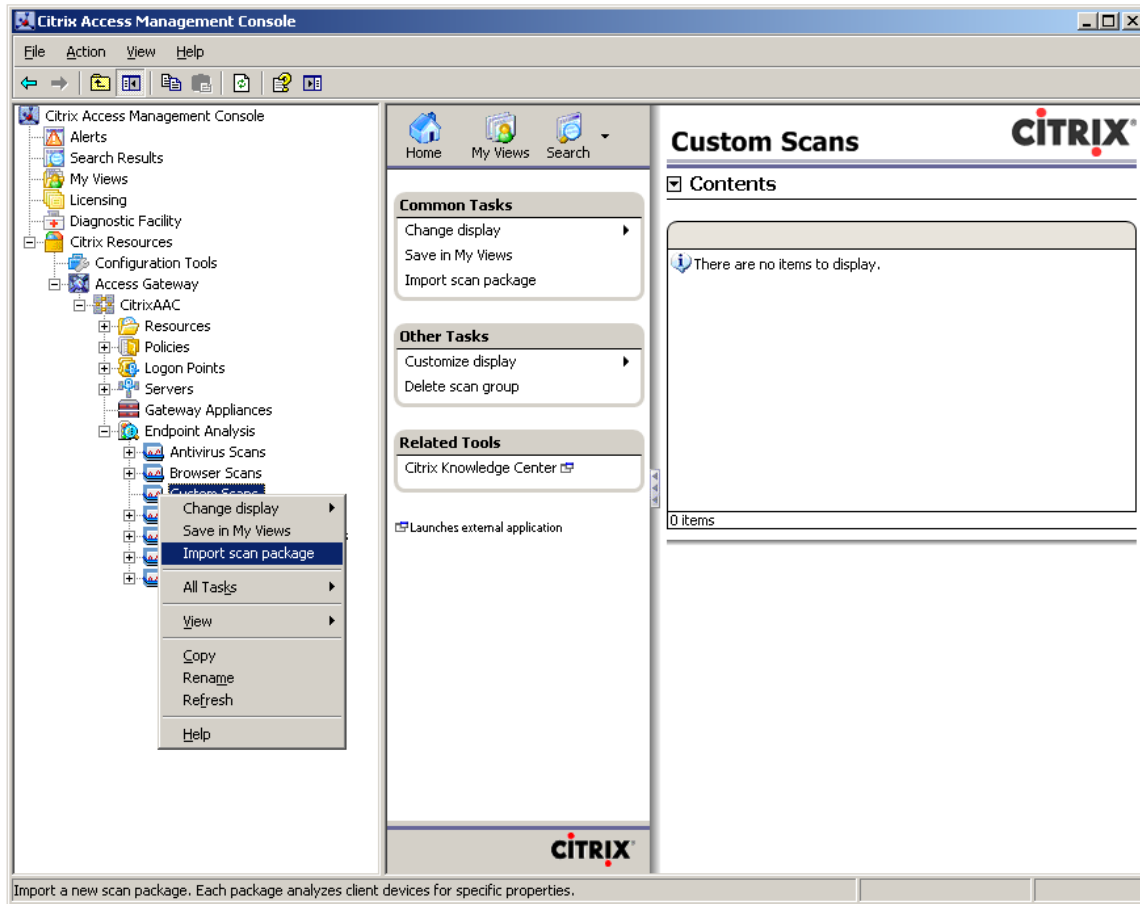
IMPORTING SCAN PACKAGES

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

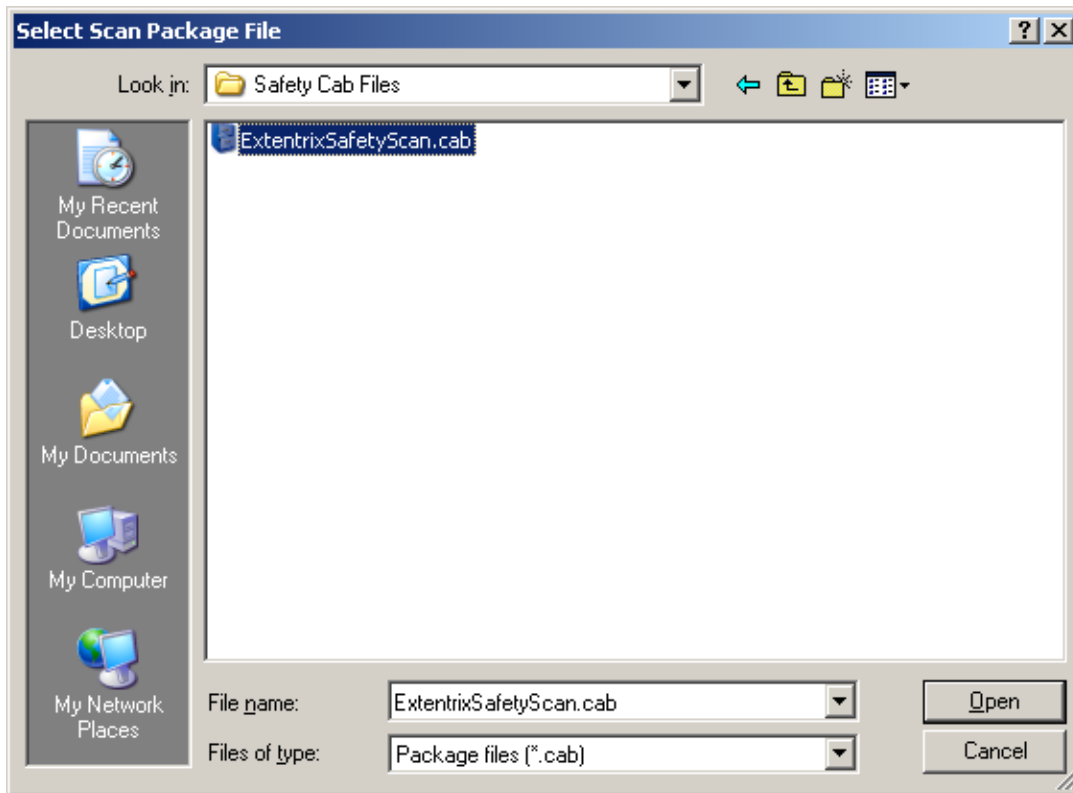
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



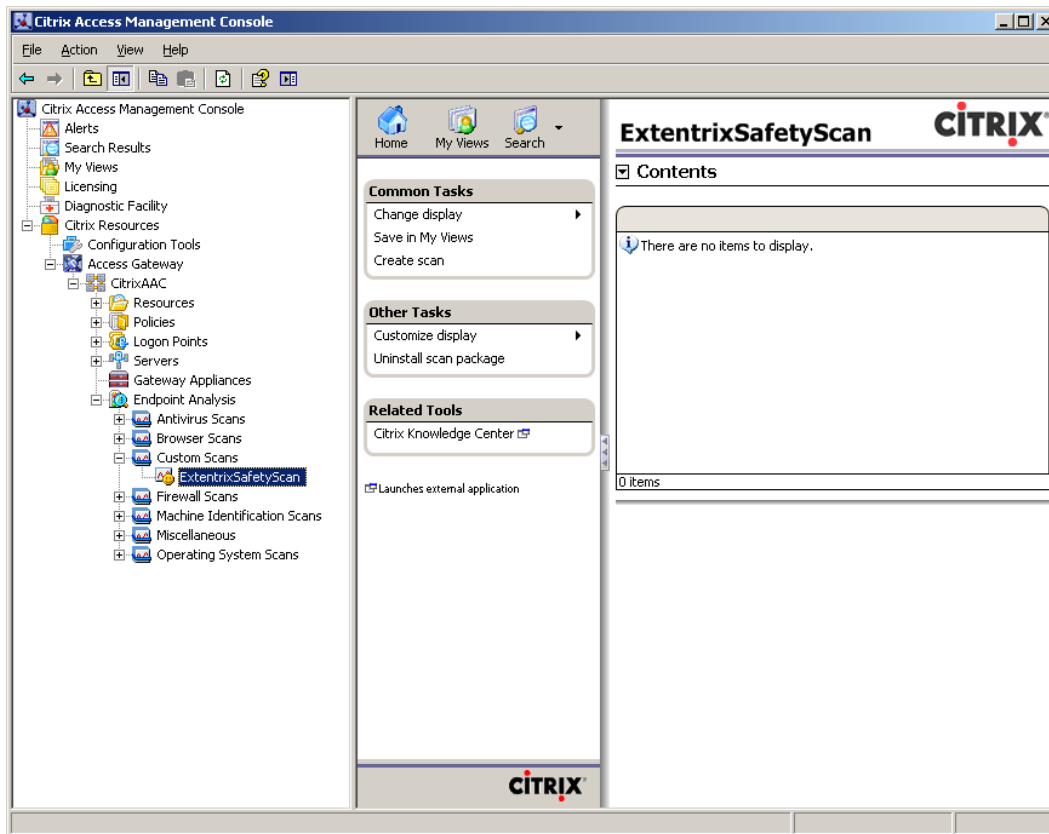
Also you can choose to insert the scan to a specific scan package group as shown in the following picture:



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



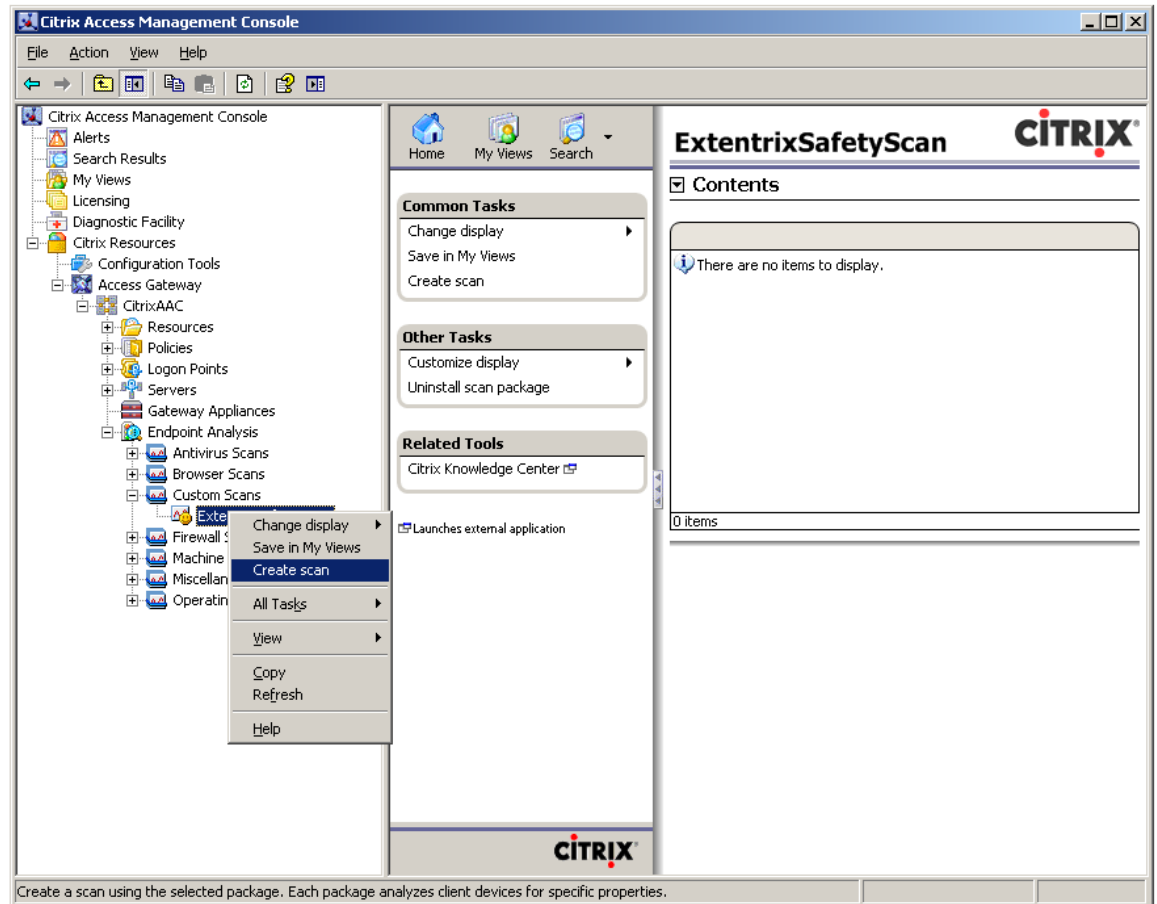
The Scan is displayed in the console as in the following picture:



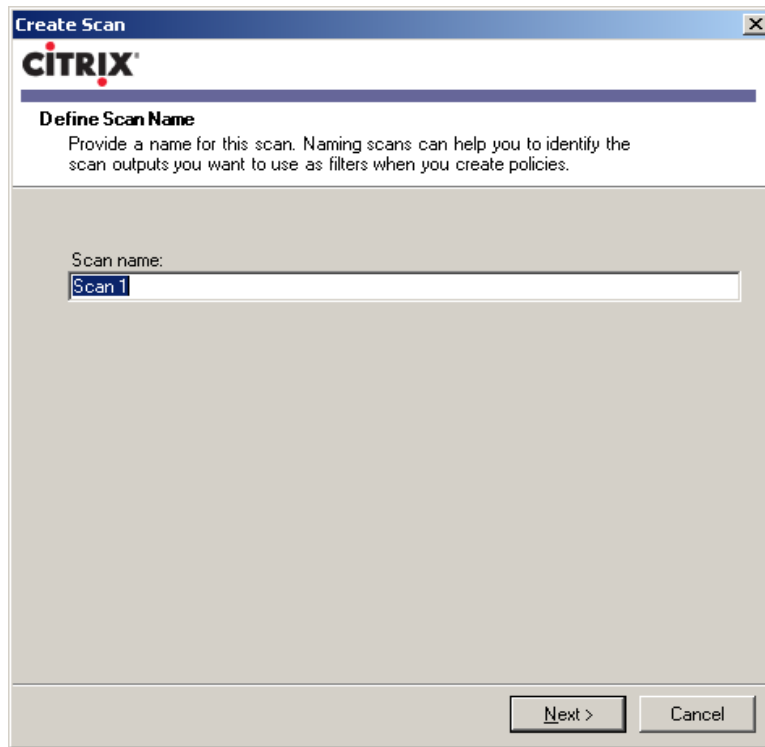
INSTALLING THE SCAN PACKAGE

Please follow the steps below to create scans and rules for the **Extentrrix Safety Scan**.

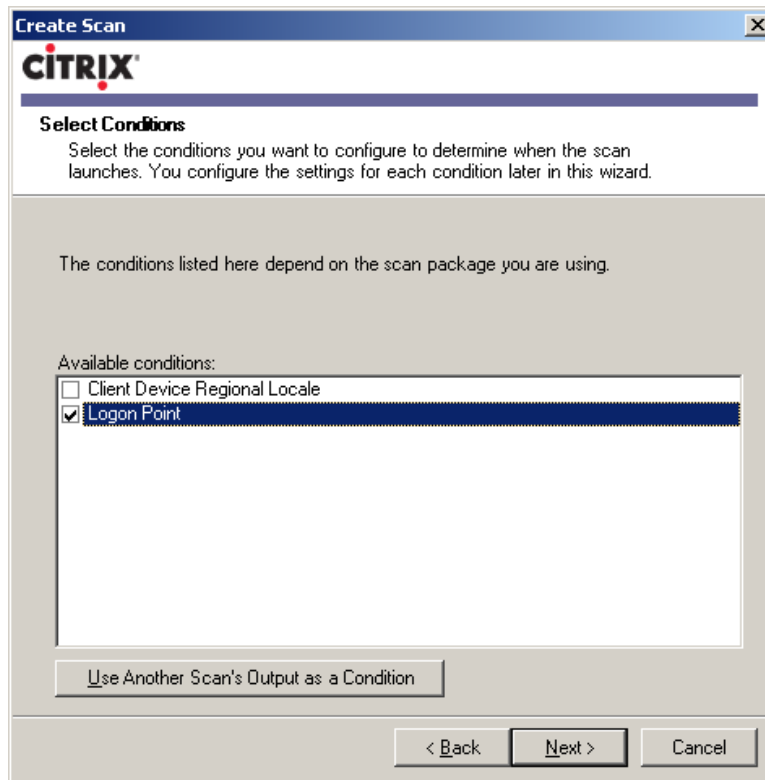
1. Select **Extentrrix Safety Scan** to create scan for it, right click the icon and choose **Create Scan**.



2. Type a name for the scan:



3. Set the scan conditions:



4. Type rule name and set rule conditions:

Create Scan

CITRIX

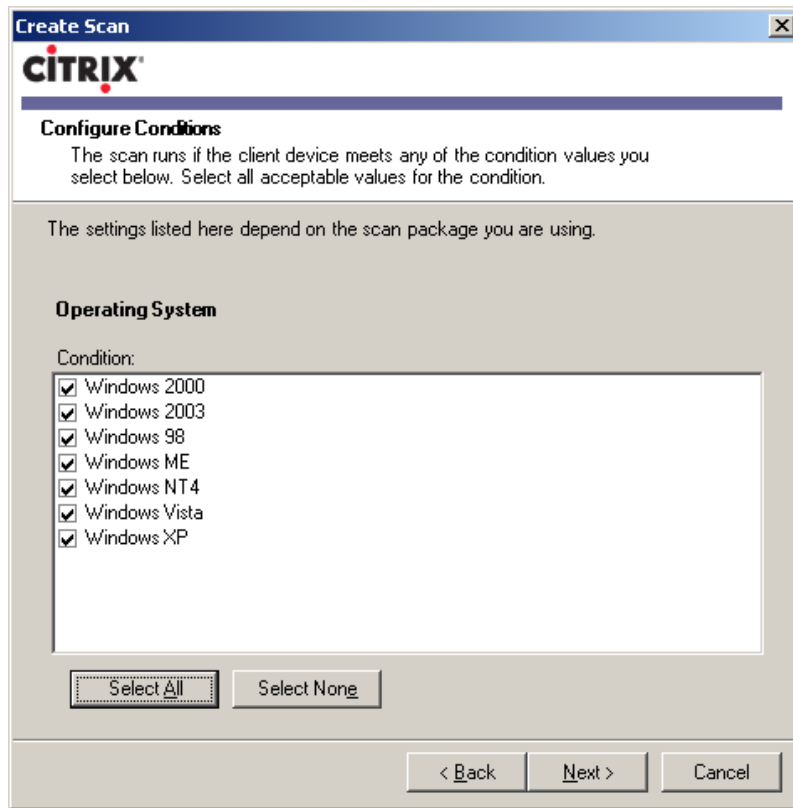
Define Rule
Rules are a combined set of conditions under which a scan is run.

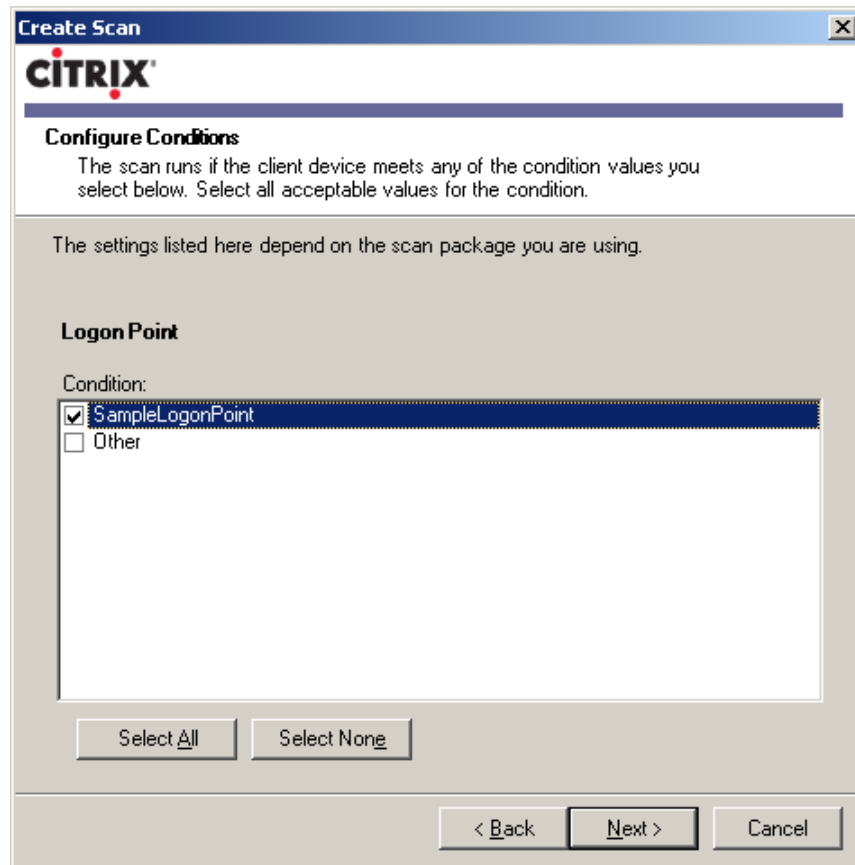
For example, your rule might be to use Scan X when the client device is running Operating System Y and Browser Version Z.

You can create multiple rules for any scan.

Rule name:
Rule 1

< Back Next > Cancel





5. A notification message will appear to tell you that this rule needs no further configuration to run.



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

2. EXTENTRIX SMART BROWSER SCAN- FOR IE

SCAN DESCRIPTION

Scan Name: Extentrix Smart Browser Scan-ForIE.

Description: Scans for IE version, security options settings and ensures that they meet the conditions specified by administrators before allowing the client to access the corporate network.

Parameters:

- IE minor version: a string specifies the minor version of IE that is allowed to be granted access to the server.
- IE options map: a map that contains security options with required values from administrator.

Scan Output:

- Allow Access- a Boolean output which indicates whether the IE version and security options meet administrator conditions or not.
 - TRUE – indicates that IE version and security options meet administrator conditions.
 - FALSE – indicates that IE version or security options or both don't meet administrator condition to be granted access to the server.
- 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.

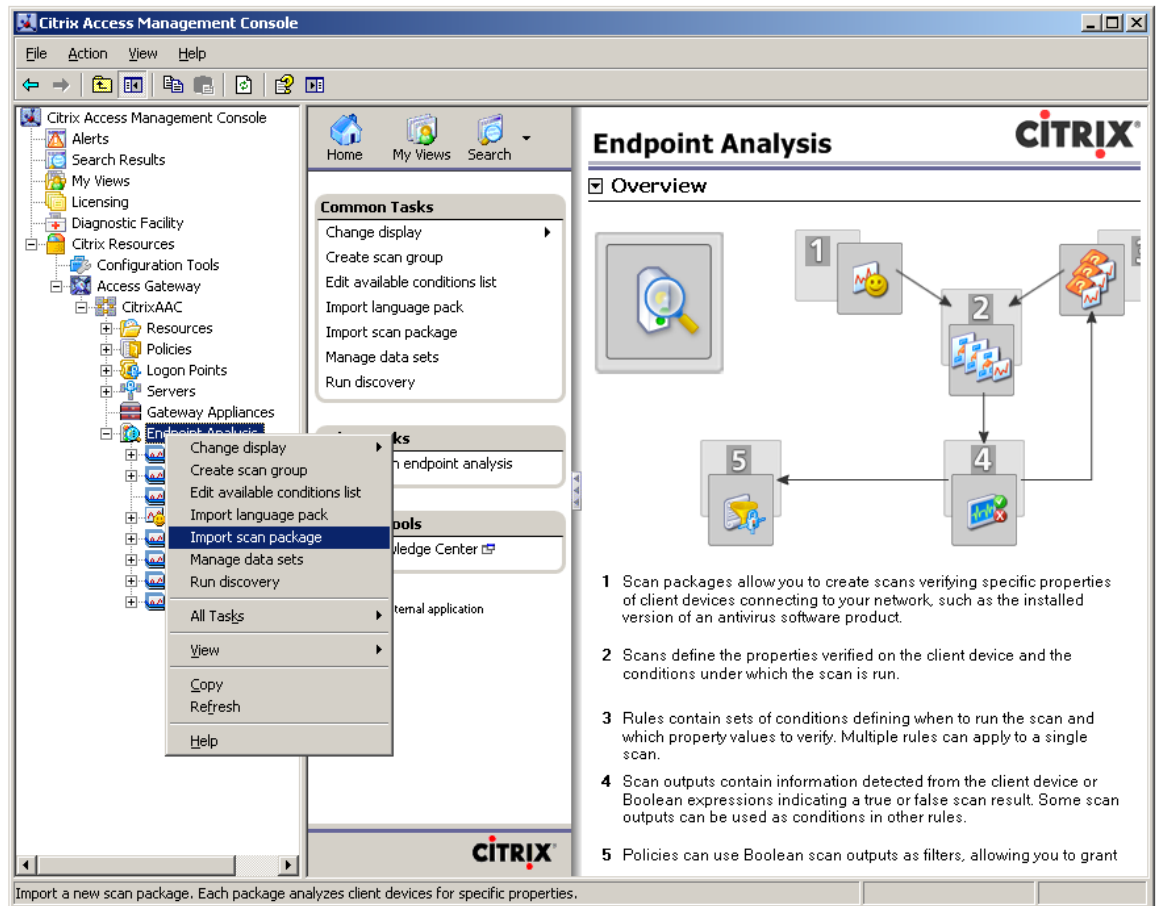
Note: If the License Status has an Invalid License value, the Allow Access will be false.

INSTALLATION AND CONFIGURATION

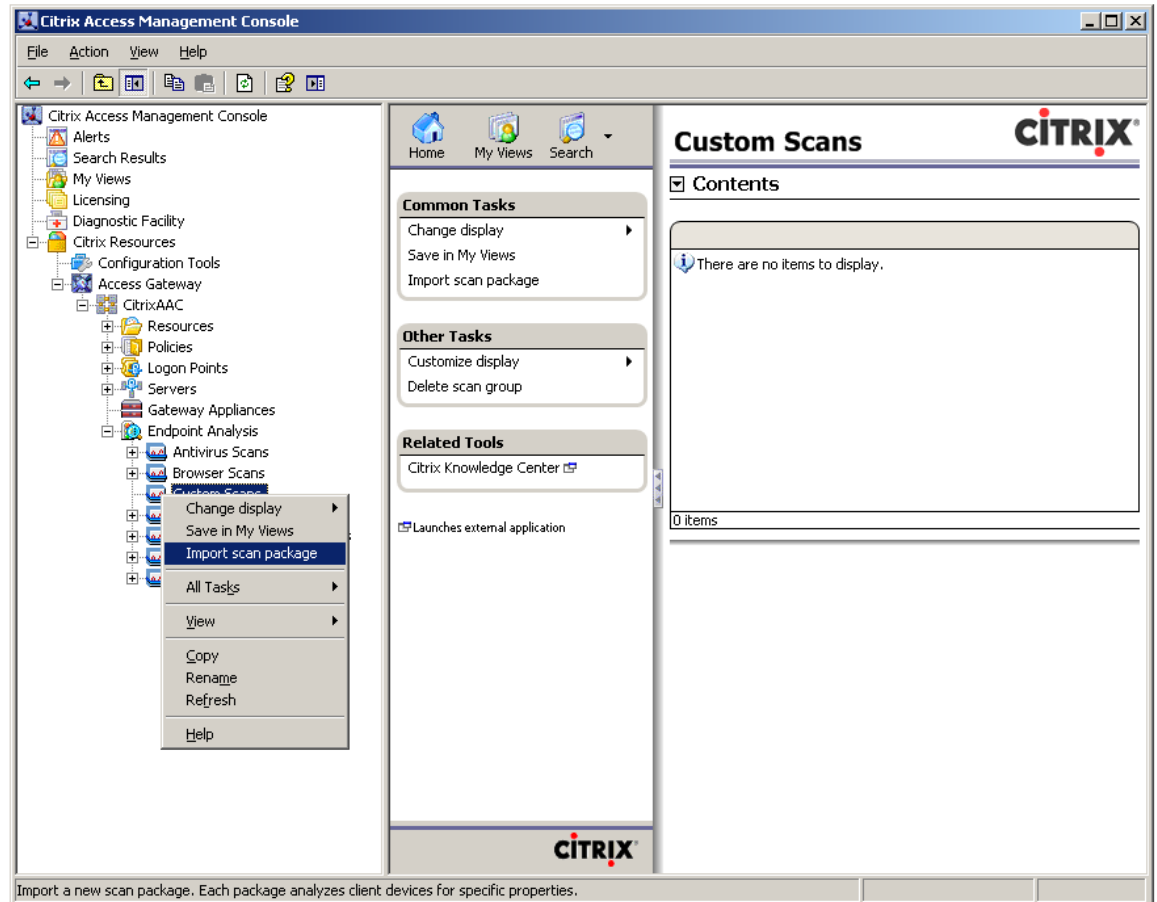
IMPORTING SCAN PACKAGES

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

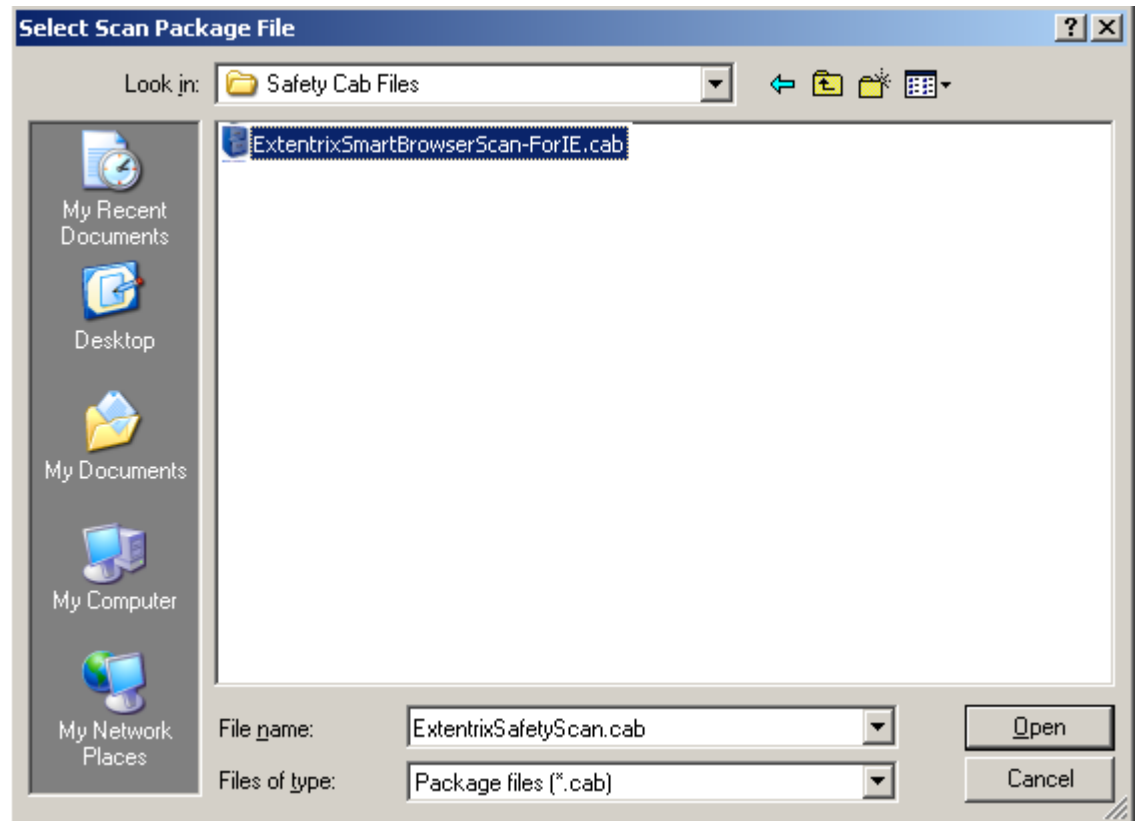
1. After opening Citrix Access Management Console, in the console tree select the **Endpoint Analysis** node.
2. Right click any of the displayed scan packages categories and select **Import scan package** from the drop down menu list.



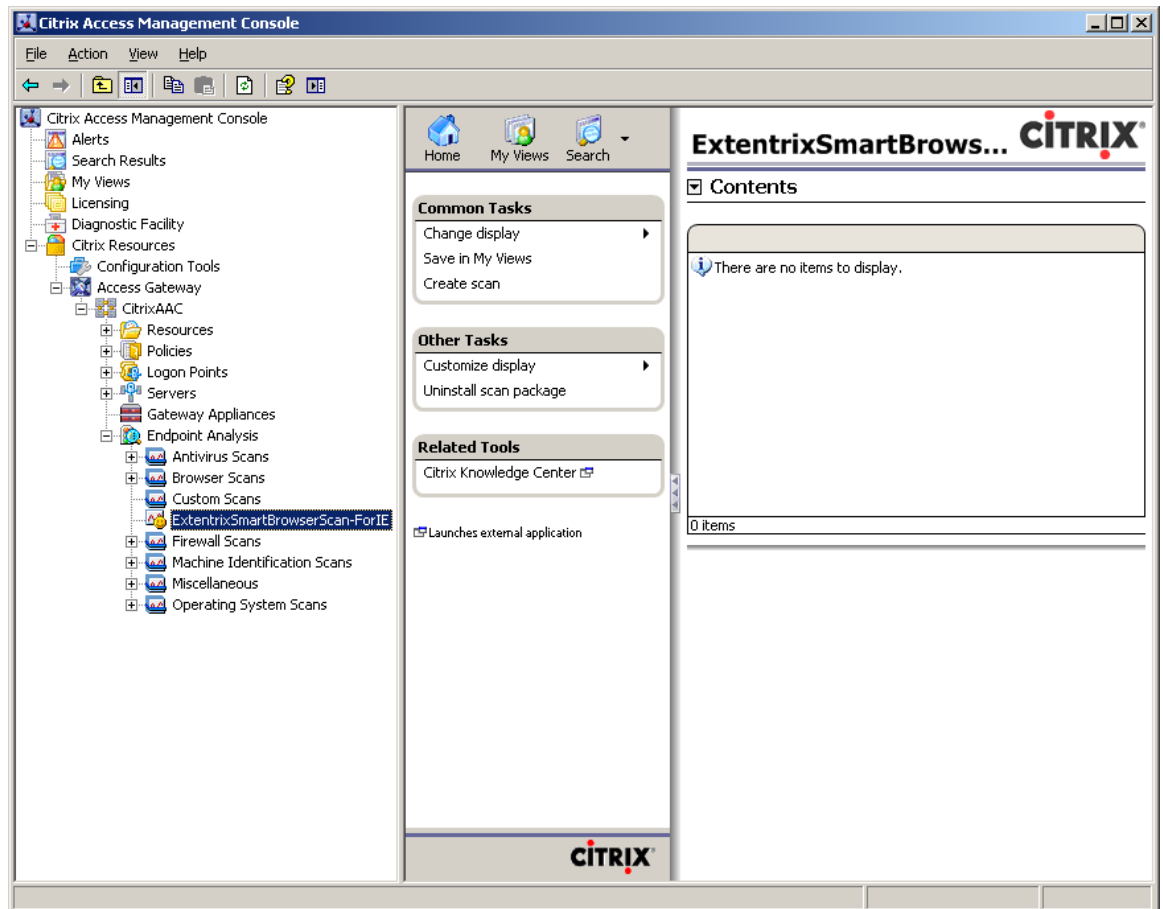
Also you can choose to insert the scan package to a specific scan package group as shown in the following picture:



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



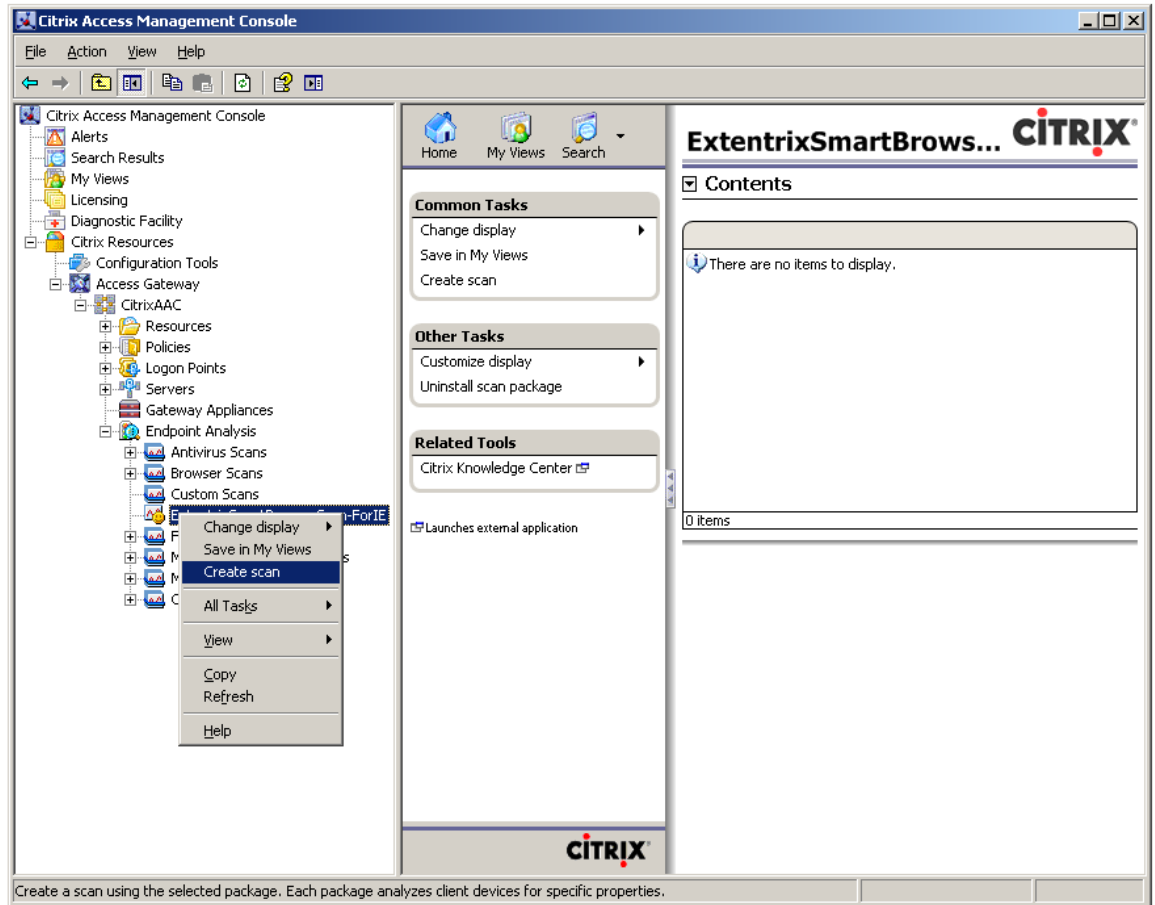
The package will be displayed in the console as shown in the following picture:



INSTALLING THE SCAN PACKAGE

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

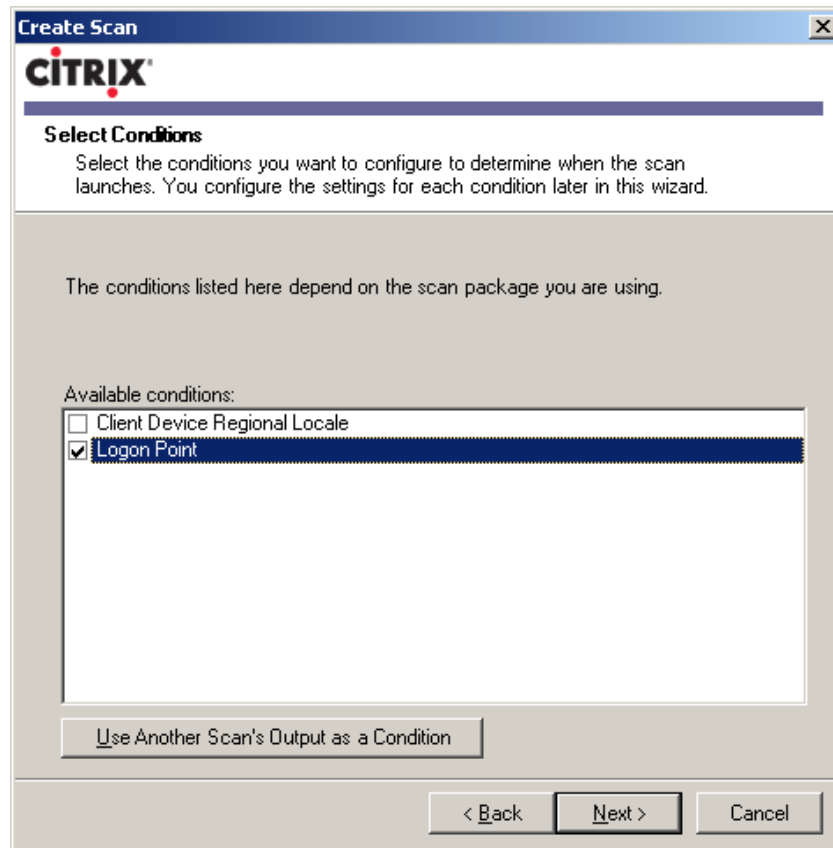
1. Select **ExtentrixSmartBrowserScan-ForIE** to create scan for it, right click the icon and choose **Create Scan**.



2. Type a name for the scan:



3. Set the scan conditions:



4. Type rule name and set rule conditions:

Create Scan

CITRIX

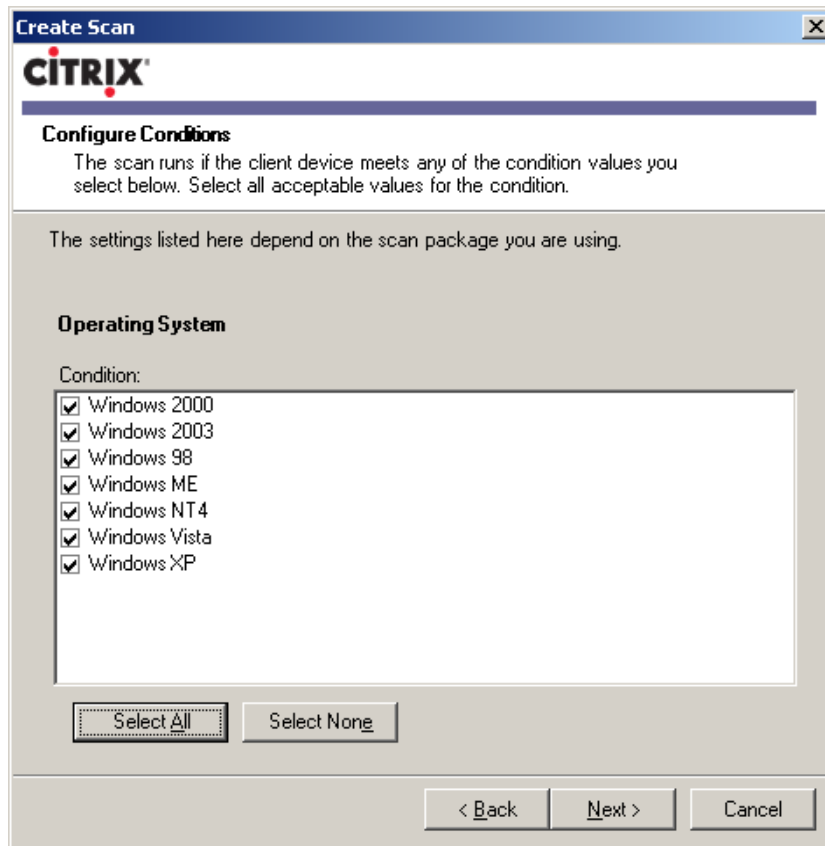
Define Rule
Rules are a combined set of conditions under which a scan is run.

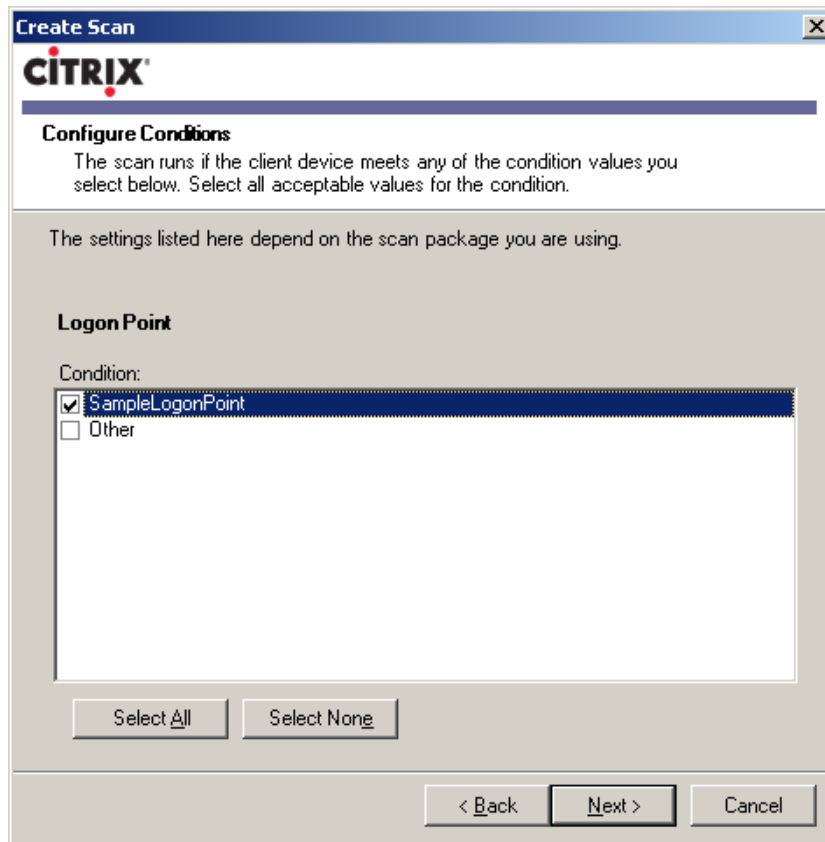
For example, your rule might be to use Scan X when the client device is running Operating System Y and Browser Version Z.

You can create multiple rules for any scan.

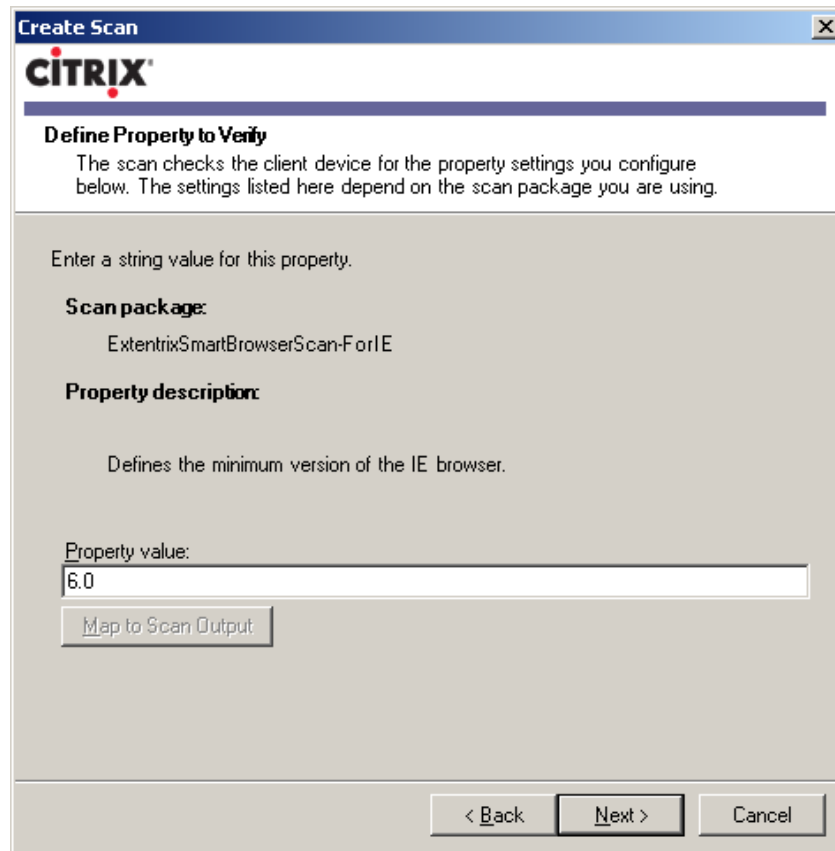
Rule name:

< Back Next > Cancel

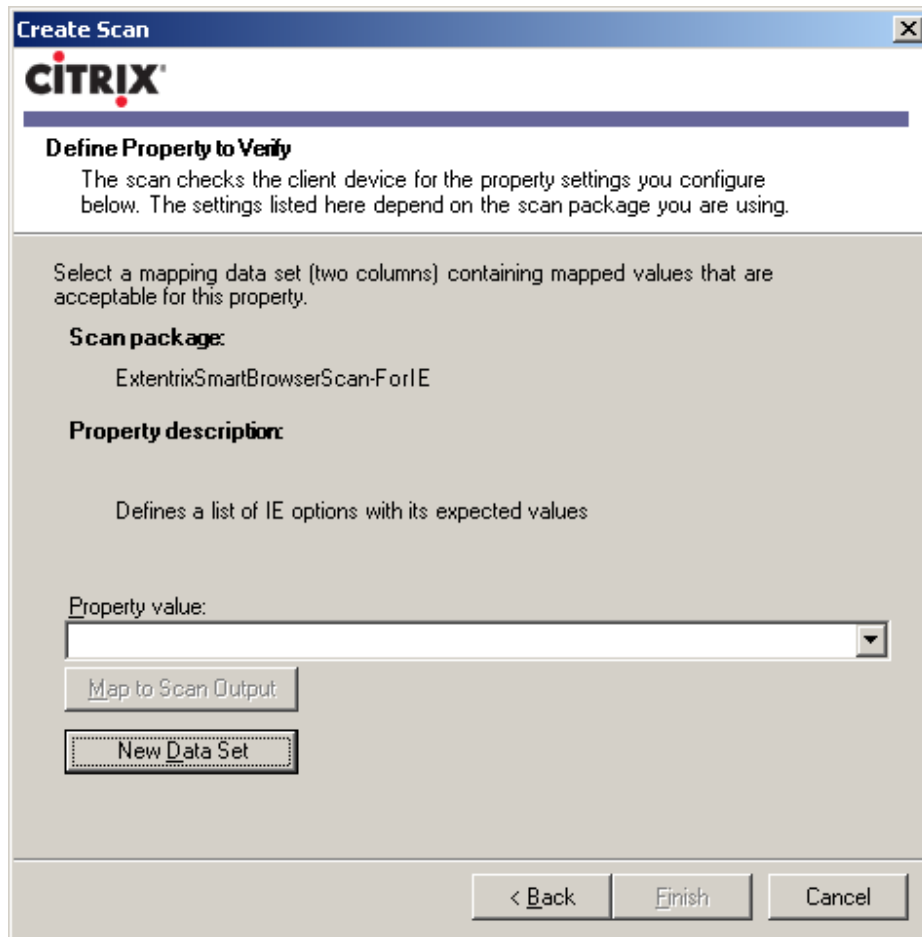




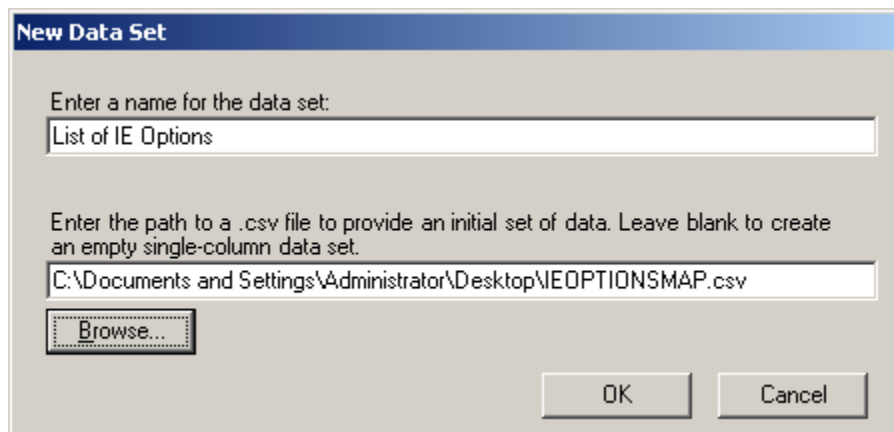
5. Type the minor value of the Internet explorer version you want as integer value.



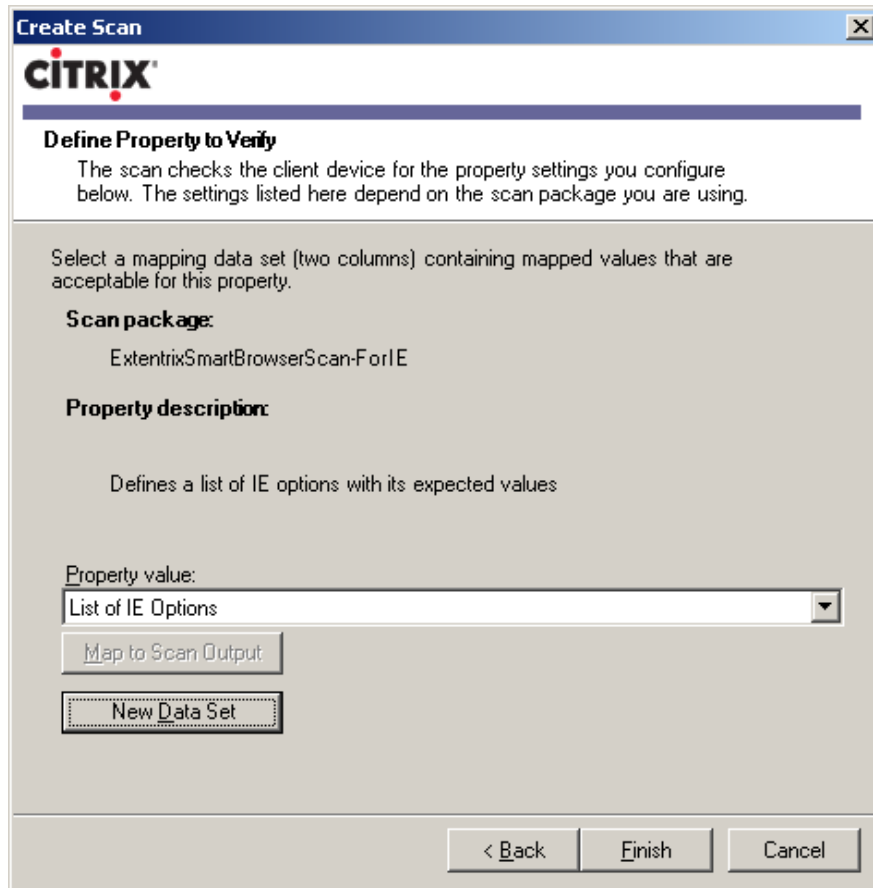
6. Define a data set (map) using a comma delimited .csv file. To do that, click on **New Data Set** to import the file. The file will have a list of all the internet security options with their conditions.



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.

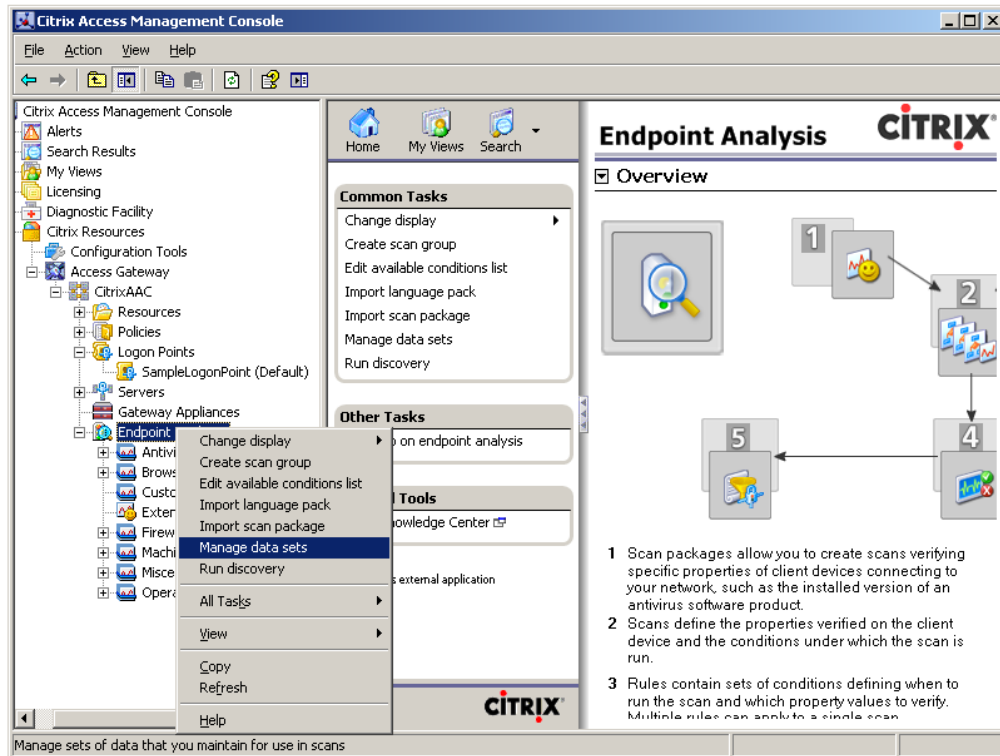


8. When you are done, click **Finish**.

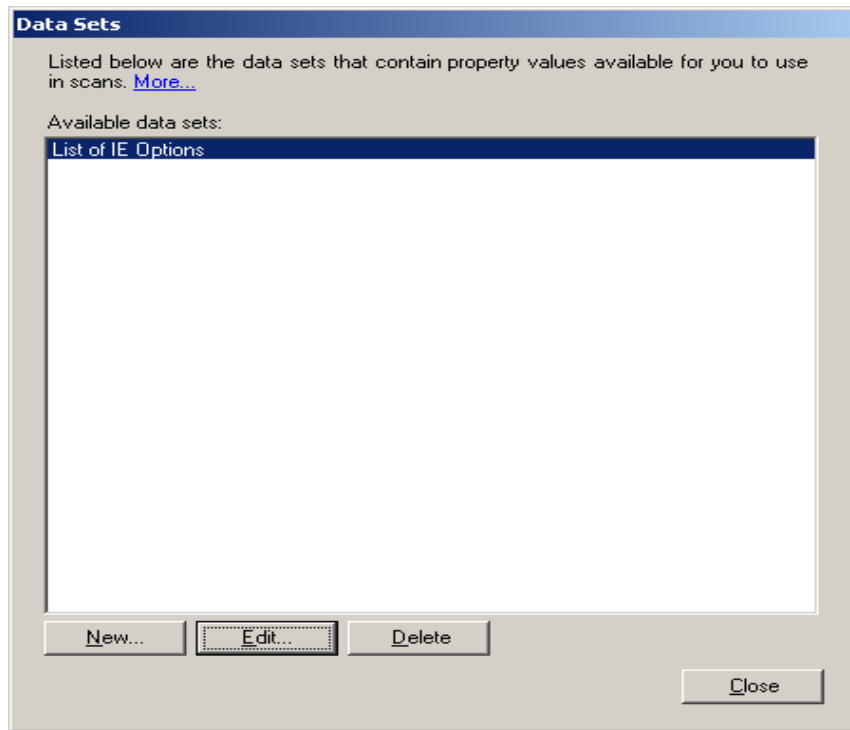


Note: You can leave the path of the file empty to create an empty single-column data set. You can edit the value later after you create the data set. To edit the data set:

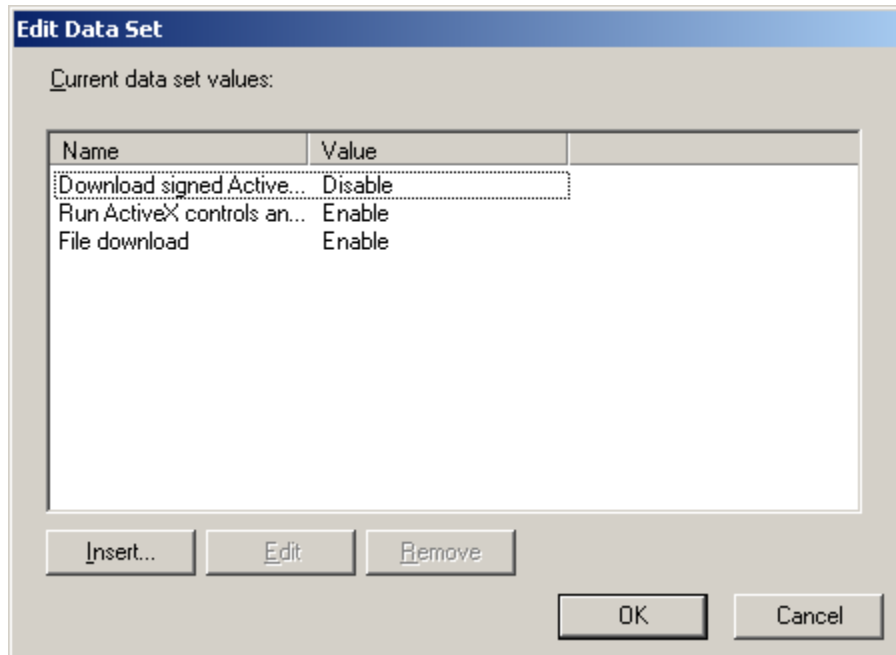
- Right click **Endpoint Analysis** in the console tree and select **Manage Data Set** from the action menu.



- 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**.

SUPPORT

Support for Extentrix Safety 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, 34

Endpoint Analysis Client, 34

Extentrix Safety Scan, 4

Extentrix Smart Browser Scan-ForIE, 17

I

Importing scan packages, 18

Importing Scan Packages, 6

Installing the scan package, 9, 22

Introduction, 3

P

Parameters, 4, 17

S

Scan Output, 4, 17

support, 33

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/>.