ICS Dissolvable Agent for SafeGuard

Alcatel-Lucent Release 2.2
ICS Release 4.0

Administration Guide

PART NUMBER: 005-0030 REV A1
PUBLISHED: MARCH 2007

ALCATEL-LUCENT
26801 WEST AGOURA ROAD
CALABASAS, CA 91301 USA
(818) 880-3500
WWW.ALCATEL-LUCENT.COM

Alcatel-Lucent Proprietary

Contents

Chapter 4: Administering Security Scanner Policies

Chapter 5: Reports

Chapter 6: The ICSInfo Utility

Preface

In this preface:

About this Guide

This preface provides an overview of Integrity Clientless Security (ICS) documentation as implemented and integrated into the Alcatel-Lucent OmniAccess SafeGuard OS solution.

The ICS Dissolvable Agent for SafeGuard Administration Guide provides:

- Prerequisites
- Administration information, including background and task-oriented administrative procedures
- Information about using the various utilities included with Integrity Clientless Security

This guide is tailored for running ICS only under OmniAccess SafeGuard OS. If you are using a version of ICS available directly from Check Point Technologies, you should use the documentation available from their Web site.

Related Publications

For additional ICS information, see the *Online Help.* The online help provides the field-level information you need to understand the UI elements in the ICS Administrator Console. The online help includes detailed information about what each element does and what entries are valid. Use the online help after reading the procedural information in the ICS for SafeGuard Administrator Guide. You can access the help from any page in the ICS Administrator Console by clicking the help link.

For information about configuring and managing the OmniAccess SafeGuard Controller, refer to the following guides:

- *OmniAccess SafeGuard Controller Installation Guide*

  Describes the OmniAccess SafeGuard Controller. The guide provides detailed installation instructions and technical specifications for the OmniAccess SafeGuard Controller.

- *OmniVista SafeGuard Manager Administration Guide*

  Describes how to manage the OmniAccess SafeGuard Controller using the OmniVista SafeGuard Manager software.

- *OmniAccess SafeGuard OS Administration Guide*

  Provides concepts and configuration instructions for the major features of OmniAccess SafeGuard OS and its supported products, which includes End Point Validation (EPV) the integral component for using ICS.

This guide uses the following formats to highlight special messages in the text:

NOTE: This format highlights information that is important or that has special interest.

chapter

1 Introduction

In this chapter:

Check Point Integrity™ Clientless Security (ICS) protects your network by scanning end point computers. Use it to do the following:

- Check end point computers for known spyware, worms, and other potential threats
- Check that end point computers are compliant with your anti-virus, firewall, and other software policies
- Protect data on end point computers from keyloggers

Integrity Clientless Security Features

ICS consists of several features, each providing a unique type of security protection. You can choose which features to implement. This section provides an overview of these features.

Integrity Clientless Security Scanner

Use the Integrity Clientless Security Scanner policies to make sure that end point computers connecting to your network meet your security requirements. The Integrity Clientless Security Scanner checks end point computers for applications according to the enforcement rules you create. Enforcement rules either prohibit or require certain applications. If the end point computer does not meet the requirements of the enforcement rule, it is considered to be 'non-compliant'. You can choose to restrict or warn non-compliant users or simply log the event. For more detailed information about enforcement rules, see *Understanding Enforcement Rules on page 24*.

Reports

Use reports to monitor how ICS is protecting your network and to plan new policies. For more information about reports, see *Reports on page 36*.

ICSInfo Utility

ICS includes the ICSInfo Utility. The ICSInfo utility collects program and other information from end point computers that you can use when creating your policies or troubleshooting user issues. See *Troubleshooting End Point User Issues on page 40*.

Supported Features

The ICS Dissolvable Agent has the following features:

- Enforces software compliance
- Detects browser plugins for adware
- Tool for dialer hacking
- Detects keystroke Logging
- Detects undesirable software
- Remote administration tool
- Screen logging
- Cookie tracking
- Detects Trojans
- Detects worms
- Enforces anti-virus compliance for these vendors:
  - Computer Associates VET
  - Computer Associates eTrust InnoculateIT
  - Kaspersky Antivirus
  - McAfee VirusScan
  - Trend Micro PC-cillin/OfficeScan
  - Sophos AV
  - Symantec Norton Antivirus

Unsupported Features

The following ICS features display in the product, but are not supported in the ICS Dissolvable Agent for OmniAccess SafeGuard OS solution:

- While the spyware module does detect key-logging, the Advanced Anti-KeyLogger feature of ICS is not supported.
- Integrity Secure Workspace

chapter

2 Prerequisites

In this chapter:

End Point Prerequisites

Use this chapter to plan your ICS implementation by ensuring that you meet the requirements listed.

For end point computers to be successfully serviced by Integrity Clientless Security, they must meet the end point requirements outlined in this section. When a user tries to access your network without the proper browser or settings, an error message is displayed detailing the browser requirements. You can choose to allow access for end point computers that do not meet your requirements, however, those computers will not be serviced by ICS.

Supported Operating Systems

For information about allowing access for end point computers that are running unsupported operating systems see *Configuring ICS to Fail Open on page 21*.

For Integrity Security Scanner:

- Windows 98/ME
- Windows NT4 SP6
- Windows 2000
- Windows XP

Supported Browsers

- Internet Explorer 5.01 or later configured to allow cookies, run ActiveX components or Sun Java applets enabled or Microsoft Java VM enabled
- Mozilla Firefox 1.0 or later configured to allow cookies and Sun Java applets support enabled
- Netscape Navigator 8.0 or later configured to allow cookies and Sun Java applets support enabled

Java Requirements

ICS supports two Java implementations. End point computers must have one of the following to be serviced by ICS:

- Sun JRE version 1.4.2 or higher.
- Microsoft JVM version 5.5.3810.0 or higher.

chapter

3 General Administration Tasks

In this chapter:

Planning for Security

This chapter provides information about the general administration of ICS. Before you start to configure and administer ICS, you should consider which security features you want to use and how they will affect your users. You should balance security with the ability of your users to access your network. If you implement a large number of security requirements, then you will achieve high security; however, if the end point computers do not comply, then your users will not be able to access your network. This can cause a considerable support burden and negatively impact productivity. Alternatively, if you configure ICS to be too lenient, you might not achieve the level of security you need.

When planning your implementation, be sure to take into account your particular security situation. ICS provides a variety of features to suit different needs. Depending on your security goals and your users, you may use only a portion of those features. Use the information in *Security Scenario on page 16*, to determine which features are suitable for your implementation.

Even if you find that you need a very secure, very restrictive security implementation, it may not be a good idea to immediately impose it upon your users. The recommended way to achieve high security with lower user impact is to start with a less demanding configuration and then implement progressively more strict configurations in an iterative manner. The process you use to manage these iterative configurations is called a 'security lifecycle'. For more information, see *Understanding Security Lifecycles on page 17*.

Security Scenario

ICS is designed to provide flexible configuration options that allow you to tailor its protection to your security needs. When deciding which ICS security solutions to use you should consider the following:

- Security vulnerabilities
- Threats
- Type of end point users and disruption tolerance

Use the following full network access security scenario to help plan your implementation. In this scenario, you are providing end point users with unlimited access to your entire network.

Vulnerabilities

In this scenario, your entire network is vulnerable, including:

- Network resources
- File servers
- Application servers

- User accounts
- End point computers

Your security goals are to provide data protection, session confidentiality, and protection from network infection.

Risks

In this scenario, your organization's intellectual property is threatened by:

- Viruses
- Trojans
- Worms
- Hackers

End Point Users and Disruption Tolerance

Your end point users are usually employees but they can also be guests and contractors. Employees are professionals with a medium-to-high level of computer expertise. They are more likely to understand the need for security and to tolerate a higher degree of disruption while becoming compliant with your security implementation's demands.

Sample Solution

A recommended solution for full network access is to use the ICS Security Scanner. The Security Scanner protects against network infection and known spyware through the policy you configure. The Security Scanner policy should require an antivirus application and a firewall on each end point computer. The policy should also prohibit all types of spyware.

Although the final goal of this security solution is to have a rather demanding and restrictive policy, you can minimize end point user disruption through the use of security lifecycles. You can implement a limited number of security features at first and use more lenient options while your users become compliant. Once users have begun to comply, you can add more security features, and use the less permissive options. For more information see *Understanding Security Lifecycles*.

Understanding Security Lifecycles

Security lifecycles allow you to gradually increase your security while maintaining reasonable user access to your network. By using a security lifecycle, you can also keep your system up to date, by implementing changes according to changes in your systems security needs.

Consider starting out with a security configuration that is lenient. Strategies for creating more lenient security configurations include:

- Minimizing security features—Using only one or two features. To make these features less disruptive, allow end point computers to connect, even if the operating systems are not supported by the feature.
- Minimizing enforcement rules—Only using enforcement rules for the most important security requirements, such as requiring an antivirus application. To make these enforcement rules even less disruptive, set them to 'warn' or 'observe'.

Use the following steps in your security lifecycle:

1. Plan your security implementation.

   Use the sample security scenario to help plan your implementation. See *Security Scenario on page 16*. When planning your security implementation you should consider the following:

   — What applications do you want to prohibit?

   — Commonly prohibited application types include IM clients, file system indexers, games, and file sharing applications. For each prohibited application you should consider whether you want to deny access for users who have it or simply warn them that the application is prohibited. If you are unsure what the user impact would be, you can choose to allow access without a warning. This allows you to track incidents in your reports without troubling the user.

   — What applications do you want to require?

   — Commonly required applications include anti-virus applications and firewalls.

   — Do you want to protect against keyloggers?

   — Do you want to allow access for end points that have unsupported operating systems.

   — What remediation information do you need to provide to your users so they can become compliant with your policies?

2. Configure your security implementation.

   Use the Integrity Advanced Server Administrator Console to configure your security settings. See *Configuration Workflow on page 20*.

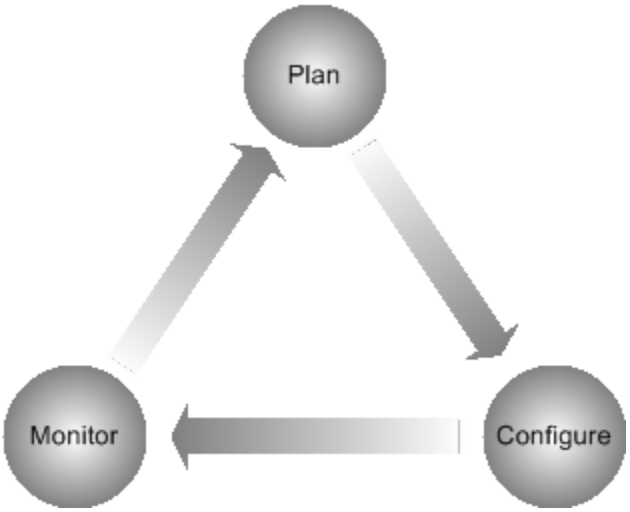
3. Monitor the results.

   Use the reports to see how well ICS is protecting your network and to see its impact on your end point users. See *Security Scan Results on page 37*.

4. Return to step 1.

   Use the information you obtain from the reports to plan your next configuration.

Figure 1 Security Lifecycle



Supporting the End Point User

In order to ensure that your users will be able to have the access they need and are not needlessly inconvenienced by your security policies, you should plan how to provide support and education for them.

One of the most important things you can do to make your ICS implementation run smoothly, is provide information to your users. If users understand your security rules and why they are being scanned, you will greatly reduce the volume of unnecessary help desk requests.

You can help your users to understand ICS and comply with your security requirements by doing the following:

- Providing remediation information—Always provide complete, clear remediation information and links if your enforcement rules are set to 'warn' or 'restrict. This allows users to deal with their own issues efficiently, without resorting to help desk requests. See *Understanding Enforcement Rules on page 24*.

Logging In

After you have finished installing ICS, you can log into the ICS Administrator Console. This is the Web-based graphical user interface that allows you to set your security configurations.

The ICS Administrator Console is located at:
`http://myIP:31862/ics/bin/ctool.cgi`.

The default username and password is 'icsadm/icsadm'. To add additional users and passwords to the Alcatel-Lucent system, use the optional EPV configuration commands described in the *OmniAccess SafeGuard OS Administration Guide*.

Configuration Workflow

After you plan your security configuration, you can begin to configure ICS. While you may perform some configuration functions at any time, the following is the recommended order for configuring your system:

1. Create enforcement rules.

   Enforcement rules determine what applications your users must or must not have on their computers. Enforcement rules are the basic building blocks of your policies. You can use the same enforcement rules in multiple policies. For more information, see *Understanding Enforcement Rules on page 24*.

2. Create policies.

   Policies provide a convenient way to specify which enforcement rules you want to use at the same time. For more information, see *Creating Policies on page 32*.

3. Activate your policy.

   Choose the policy that you want to use. You can create as many different policies as you want, but only one policy can be active at a time. See *Activating Policies on page 32*.

4. Save.

   After completing any configuration steps, you must always save to have your changes take effect.

5. (Optional) Back up your ICS policy and portal configurations on the Alcatel-Lucent device. See the section, *Backing Up and Restoring ICS Policies and Rules* in the EPV chapter of the *OmniAccess SafeGuard OS Administration Guide*.

General Administration Tasks

Use this section to perform general configuration tasks, including:

- *Configuring ICS to Fail Open*
- *Configuring Updates*

Configuring ICS to Fail Open

If you want to minimize disruption to your users, you should configure ICS to 'fail open.' This means that end point users that are not running a supported operating systems can still access your network, without being serviced by ICS.

1. Log into the ICS Administrator Console.
2. Go to the **Gateway Configuration** tab.
3. In the section **Settings for end points running a non-supported OS** select **Allow access to end points running a non-supported OS**.
4. Click **Save**.

   This procedure causes those unsupported users to bypass all the scans and security features of ICS. These unsupported end point users are not protected by ICS. Users with supported operating systems are still protected.

Configuring Updates

Check Point periodically releases updates to client components, such as support for new anti-virus providers. When updated versions of the client components are available, you can download them. Client components include the following:

- Security Scanner
- Enforcement agent
- Java and ActiveX launchers

It is recommended that you update your system once a week. If you do not update ICS, your system will be out-of-date and you will not have the best protection available.

How to Update Your ICS System:

1. Log into the ICS Administrator Console by supplying the default user ID and password.

   There are a number of methods to locating and logging into the ICS Administrator Console from within the OmniVista SafeGuard Manager. For example, you can select ICS Admin from the Other Actions pull-down menu. See the *OmniVista SafeGuard Manager Administration Guide* for details.

NOTE: You must have a DNS server configured in order to update ICS. See *Configuring for Domain Name Service (DNS) Server* in the *OmniAccess SafeGuard OS Administration Guide*.

2 Click **Update Client Components** at the bottom of the page.

If an update is available, a new window opens and displays the latest package.

3 Click the box, **Proceed to Update**.

A message appears to show the status of your update.

4 When the update is complete, click **Finish** to continue.

chapter

4 Administering Security Scanner Policies

In this chapter

This chapter contains information about how to administer your policies using the ICS Administrator Console. Policies control what the Integrity Clientless Security Scanner checks for on your end point computers. Policies consist of collections of enforcement rules, which specify whether to prohibit or require certain applications, and what action to take if the end point computer is out of compliance with the rule.

Understanding Integrity Clientless Security Scanner

Integrity Clientless Security Scanner requires no pre-installed software on end point computers, except a supported browser. The Security Scan is performed by a Java or ActiveX component that is deployed from your Web server to each end point computer that requests access.

Implementing Policies

This section describes all the steps you need in order to use policies to secure your end points. If you do not complete all these steps, your policies will not be enforced.

NOTE: If you do not want to create your own policies, you can use the sample policies included with ICS. ICS includes high, medium, and low sample policies that you can activate. You can also edit these rules to customize them.

To Implement policies

1. Create your enforcement rules. See *Understanding Enforcement Rules on page 24*.
2. Use the enforcement rules to create a policy. See *Creating Policies on page 32*.
3. Activate the policy. See *Activating Policies on page 32*.
4. Save your configuration.

Understanding Enforcement Rules

Use the Enforcement Rule page in the ICS Administrator Console to manage your enforcement rules. You must add an enforcement rule to a policy and make that policy the active policy for the rule to take effect. Any changes you make to an enforcement rule affects all the policies that contain that rule. When you delete an enforcement rule, it is removed from all your policies. You are warned when you delete an enforcement rule that is currently being used in a policy.

Each enforcement rule consists of the following parts:

- **Conditions**—Use the conditions area to indicate the criteria that the end point computer must meet. For instance, that it must have a certain file running.
- **Action**—Use the action area to indicate what ICS should do when the end point computer is out of compliance with the rule.

  Actions affect the user experience as described in *Table 1*.

Table 1 Action behaviors

Option	Behavior
Restrict	Prevents the users from logging on. ICS displays the scan report and any remediation information you have specified. Users must become compliant before being allowed to proceed.
Warn	Does not prevent users from logging on. ICS displays the scan report and any remediation information you have specified. Users may proceed without becoming compliant. Users are asked to become compliant every time they are scanned by ICS.
Observe	Does not prevent users from logging on. ICS records the violation in the log. This option does not display the scan report to end users but is useful for gathering information about potential issues with your network before you restrict end point connections.
Allow	ICS does not check for spyware you have set to 'allow'. This action is only available for Anti-spyware scan rules.

- **Remediation** — Use the remediation area to specify resources and information that the end point users need to become compliant with the enforcement rule. For example, if the rule requires an anti-virus program, you should provide a link to a location where the end point user can download the application and instructions on how to install it. Because users might be repeatedly warned, or even denied access if they do not comply, it is important to make sure you provide sufficient and clear remediation resources.

  In Alcatel-Lucent's End Point Validation (EPV) feature, a bypass policy is required to perform remediation. See the section, *Creating Global Bypass Policies*, in the *End Point Validation* chapter of the *OmniAccess SafeGuard OS Administration Guide* for further details.

Enforcement Rule Types

Use enforcement rules to control which applications your users must, or must not have on their computer when they connect to your network. There are the following types of enforcement rules:

- **Firewall Application** — Use firewall application rules to require a certain firewall application. See *Firewall Application Rules on page 26*.
- **Anti-Virus Application** — Use anti-virus application rules to require a supported anti-virus application. If you want to require an anti-virus application that is not supported, use the custom application rule. See *Anti-virus Application Rules on page 27*.
- **Anti-Spyware Scan** — Use anti-spyware scan rules to prohibit certain spyware types. See *Anti-Spyware Scan Rules on page 29*.
- **Custom Application** — Use custom application rules to prohibit or require any application. See *Custom Application Rules on page 30*.
- **Custom Group** — Use Custom Group rules to bundle custom application enforcement rules into one rule. When you put enforcement rules in a group, the end point computer must meet at least one of the conditions in order to be in compliance. See *Custom Group Rules on page 31*.

Firewall Application Rules

Firewall application rules determine which firewall applications end point computers must have when they are logged onto your network. You can use this feature to require that end point users obtain the latest version of an Integrity client when they connect to your gateway.

Creating a Firewall Application Rule

The steps below give an overview of creating a firewall application rule. For detailed information about individual user interface elements, and how to complete the page, see the online help.

To Create a Firewall Application Rule:

1. Log into the ICS Administrator Console and click **Enforcement Rules**.
2. On the Enforcement Rules page click **New Rule** and choose **Firewall Application**.
3. Select the firewalls you want to require.

   This sets the conditions for the rule. If end point computers violate these conditions they are considered to be out of compliance.
4. Select the action you want ICS to take if the end point user is not in compliance with this rule.
5. Use the remediation area to specify any information or resources you want to provide to end point users to help them to become compliant with this rule.

6 Click **Save Rule**.

Anti-virus Application Rules

It is important to protect your network from viruses. Every time an end point user logs in, your network is exposed to any viruses that the end point computer is infected with. Users who access your network through a gateway are particularly likely to be infected, since they are more likely to use their computers for personal uses, which put them at risk for viruses.

In order to protect your organization from viruses, you should require your users to have anti-virus protection. Effective anti-virus protection requires not only having the correct anti-virus software on your end point computers, but also having a recent version of that software and up-to-date software definitions. If end point users have out-of-date software definitions, they will not be protected against the latest viruses.

Anti-virus application rules determine which anti-virus applications your end point computers must have when they are logged into your network. Since users can sometimes disable their anti-virus software, all anti-virus applications rules require that the application be running. For your convenience, anti-virus enforcement rules are pre-configured with supported anti-virus providers.

NOTE: If you want to create an enforcement rule for an anti-virus provider not supported by the anti-virus applications rules, you can do so by creating a custom software rule to require the application. See *Custom Application Rules on page 30*.

If you want to require that your end point computers have a supported form of anti-virus protection, create an anti-virus enforcement rule for your policy. It is recommended that you require an anti-virus application with a DAT file no older than 14 days. In the case of a virus outbreak, you should require that the DAT file be no more than 24 hours old.

Creating an Anti-virus Application Rule

The steps below give an overview of creating an anti-virus application rule. For detailed information about individual user interface elements, and how to complete the page, see the online help.

To create an anti-virus application rule:

1 Log into the ICS Administrator Console and click **Enforcement Rules**.

2 On the Enforcement Rules page click **New Rule** and choose **Anti-Virus Application**.

3 Select the anti-virus applications you want to require.

The end point computer must have at least one of these anti-virus applications to be in compliance with the rule.

4 You can optionally edit the conditions for each application.

For each anti-virus application you can specify more detailed criteria and remediation information that is specific to the application.

A Click **Edit**.

The Anti-Virus Application Details page appears.

B Specify the operating system that this anti-virus application is required for.

C Specify the application conditions.

It is recommended that you require a recent version of the application and a DAT file no older than 14 days. This ensures that your end point computers have up-to-date protection against viruses.

NOTE: The format of these entries is important and formats vary from one anti-virus provider to another. To obtain the engine version, DAT file version, and DAT age information for your supported anti-virus software in the correct format, run the ICSInfo utility included with Integrity Clientless Security on your reference computer. For more information, see *Obtaining Anti-virus Application Information on page 41*.

D Specify the remediation information and resources.

This remediation information is specific to the application.

E Click **Save Rule**.

You return to the Anti-Virus Enforcement Rule Settings page.

5 Select the action you want ICS to take if the end point user is not in compliance with this rule.

6 Use the remediation area to specify any information or resources you want to provide to end point users to help them to become compliant with this rule.

This remediation information is for all the anti-virus applications and should be more generic than the remediation information you provided for the specific applications.

7 Click **Save Rule**.

Anti-Spyware Scan Rules

The term 'spyware' refers to applications that collect user data on host computers for either commercial or malicious purposes.

Spyware may do any of the following:

- Aid hackers in circumventing your security and spreading malicious code. Spyware can introduce worms, dial out to toll lines, and introduce other serious security breaches.
- Send information about a user, the user's behavior, the computer system or the computer system's use without requesting permission from the user to do so. This can be a serious breach of security for your users and your organization.
- Present advertising, often without notification, to the users without any additional benefit. This is a less serious threat, but is annoying to users and can have a serious impact on productivity.

For more information about types of spyware and the risks they present, see the online help for the Anti-Spyware Enforcement rules.

Use anti-spyware scan rules to protect your end points from spyware. Anti-spyware scan rules allow you to control gateway access for users who have spyware software on their end point computers. ICS comes preconfigured with software definitions for many types of known spyware, organized by type. Through anti-spyware enforcement rules you can protect your organization, and encourage or require your users to remove spyware residing on their computers.

For each type of spyware, you can set the action you would like ICS to take when that spyware type is detected on an end point computer. You can also create exceptions for specific spyware programs you consider benign and want to allow.

If you want to protect your Gateway and your end point users from spyware, create an anti-spyware enforcement rule for your policy. You can only use one Anti-spyware scan rule for each policy, though you may wish to use different rules in different policies. Only the rule included in your active policy will be enforced for your users.

Creating an Anti-spyware Rule

The steps below give an overview of creating an Anti-spyware scan rule. For detailed information about individual user interface elements, and how to complete the page, see the online help.

To Create an Anti-spyware Rule:

1. Log into the ICS Administrator Console and click **Enforcement Rules**.
2. On the Enforcement Rules page click **New Rule** and choose **Anti-Spyware Scan**.

3 Enter a **Name** and **Description** for the rule.

4 For each screened software type, choose the action you want ICS to take when it detects this kind of spyware.

If you warn or restrict the end point computer, it is recommended that you include a **Remedy Message**, informing the user of what they need to do to treat the spyware.

5 If you want ICS to ignore certain spyware applications, add them to the exclusions list.

6 Optionally, you can select **Display SmartDefense Advisor article link**.

Selecting this option will display a Check Point article to the end point users that will explain what the spyware is and offer treatment advice. It is highly recommended that you select this option.

SECURITY: If you elect to present this information to end users, you must configure an EPV bypass policy to allow the users access to smartdefense.checkpoint.com. Configuration of bypass policies are discussed in the *EPV* chapter of the *OmniAccess SafeGuard OS Administration Guide*.

7 Click **Save Rule**.

Custom Application Rules

While most of the common applications that you might want to control are governed by the other types of rules, you might wish to prohibit or require other applications.

If you wish to prohibit or require an application not covered by any of the other rule types, use a custom application rule. A typical use of a custom application rule is to create a rule requiring an anti-virus application that is not supported by the preconfigured antivirus application rules.

To Create a Custom Application Rule:

1 Log into the ICS Administrator Console and click **Enforcement Rules**.

2 On the Enforcement Rules page click **New Rule** and choose **Custom Application**.

3 Enter a **Name** and a **Description** for the rule.

4 Choose the end point computer operating system you want this rule to apply to.

5 Specify the conditions for this rule.

If you are creating a rule requiring an anti-virus application, it is recommended that you require that the application be running, to prevent users from disabling the application. You should also require that it be modified no more than a week ago, to ensure that end point computers are getting virus definition updates regularly. During a virus outbreak, you will want to require that the file be modified no more than 24 hours ago.

NOTE: To obtain the checksum for your custom application, run the ICSInfo utility included with Integrity Clientless Security on your reference computer. For more information, see *Obtaining Application Checksums on page 41*.

6 Select the action you want ICS to take if the end point user is not in compliance with this rule.

7 Use the remediation area to specify any information or resources you want to provide to end point users to help them to become compliant with this rule.

8 Click **Save Rule**.

Custom Group Rules

Use custom group rules to group together custom application enforcement rules. End point computers have to be compliant with at least one rule in the group. For example, you may want to make a rule group that requires a certain security patch or a certain service pack, if having either one would fulfill your organization's security requirements.

Creating Custom Group Rules

To Create a Custom Group:

1 Log into the ICS Administrator Console and click **Enforcement Rules**.

2 On the Enforcement Rules page click **New Rule** and choose **Custom Group**.

3 Enter a **Name** and a **Description** for the rule.

4 Choose the enforcement rules you want to include in the group.

End point users will have to be compliant with at least one of these rules. You can only add custom application rules to a group rule.

5 Select the action you want ICS to take if the end point user is not in compliance with this rule.

6 Use the remediation area to specify any information or resources you want to provide to end point users to help them to become compliant with this rule.

This remediation information is for all the enforcement rules in the group and should be more generic than the remediation information you provided for specific enforcement rules.

7 Click **Save Rule**.

Creating Policies

Policies are made up of Enforcement rules. When an end point computer is scanned, its state is compared to all the enforcement rules in the currently active policy. If you have more than one enforcement rule in a policy, the end point users must comply with all of the rules. If you need to enforce compliance with just one rule out of a group, create a custom group rule out of the rules.

To Create a Policy:

1 Log into the ICS Administrator Console and click **Policies**.

2 On the Policies page, click **New Policy**.

3 Enter a **Name** and **Description** for the policy.

4 In the **Rules selected for this policy** table, select the enforcement rules you want in this policy.

5 Click **Save Policy**.

NOTE: This policy will not be enforced until you activate it.

Activating Policies

You can create as many policies as you need, but only one is enforced at a time. You must activate your policy in order to have it be enforced. You may also set the scan interval.

To Activate a Policy:

1 Log into the ICS Administrator Console and click **Gateway Configuration**.

2 Select your policy in the **Integrity Security Scanner Policy** drop down list.

3 Optionally, you can select to enforce a scan interval.

Use a scan interval to require that the end point computers be re-scanned while they are connected to your network. If a user is connected to your network, and then directs a browser to another location, they may become infected with spyware after the original scan. Use the scan interval to trigger a periodic re-scan to help ensure that your end point users remain free of spyware while connected.

The re-scans are silent to the user and are performed in the background. If the enforcement rule's action is set to warn or observe and the user becomes contaminated, the user remains compliant until aged-out of the posture table. However, if the enforcement rule's action is set to restrict and the user become contaminated, the user falls out of compliance and should follow the remediation action. Depending on your trigger policy and remediation action, the user's network access might be disrupted.

NOTE: The recommended scan interval is 15 minutes.

4 Click **Save**.

chapter

5 Reports

In this chapter:

Use this chapter to understand how to use reports to enhance your implementation.

Reports

Use the ICS reports to monitor security events occurring on your network. Use the information in these reports to improve your policies, provide better remediation for users, and observe how ICS is protecting your network.

ICS includes the following major reports, you can also drill down to detail-level reports:

Generating Reports

All ICS report pages use the same method to generate reports. Use the following instructions to generate reports, then see the section on that report.

To Generate a Report:

1. Log into the ICS Administrator Console.
2. Click **Reports**.
3. Choose your report.
4. Set the date range for the report and click **Generate Report**.

   The report is generated for the time period you specify.

NOTE: The reports database holds a maximum of two days data, after which the data is rotated.

Access Statistics

Use the Access Statistics report to see what the results were for all the users who attempted to connect to your gateway. Attempted user connections are counted per session, with the session determined by the persistence of the cookie. If a user connects to your gateway, disconnects and reconnects again, that is counted as one connection attempt, unless the cookie has expired.

This report shows how many users were compliant with your security rules and what happened to those who were not compliant. Use the legend to see details about the users in each category.

You can use the information in this report to refine your policies. If an excessive amount of users are being warned, or even restricted, your rules may be too strict or you may not be providing enough remediation information. Use the Rules Broken report to see which rules your end point users are having the most trouble with. Once most users are compliant, you can increase your security requirements.

Security Scan Results

The Security Scan Results report shows the total numbers of enforcement rules broken and the total amount of spyware found for each user's scan. You can use this report to find out why a user was warned or restricted. Using this information, you can then provide remediation information to the user.

Spyware Found

Use the Spyware Found report to see how often particular spyware applications were found on your end point computers. If you find that ICS is scanning for a particular spyware application that you want to allow, you can add it to the ignore list. See *Anti-Spyware Scan Rules on page 29*.

Rules Broken

Use the Rules Broken report to determine which rules are causing your end point users the most trouble. This report includes rules that are set to 'observe'. If a rule is consistently being broken at a high rate, that may indicate the rule is too strict or that you are not providing enough remediation information for that rule.

Anti-Keylogger

The Anti-Keylogger report shows processes that were flagged by ICS as potentially being keyloggers. This reports shows you how ICS protects your network and end point users from keyloggers.

Errors

Use the Errors report to view the ICS errors that end point users are experiencing when they attempt to connect to your gateway. This report only shows errors when the user connects to the ICS server. To diagnose connection issues due to end point configuration, use the ICSInfo utility. See *Troubleshooting End Point User Issues on page 40*.

chapter

6 The ICSInfo Utility

In this chapter:

The ICSInfo utility collects program and other information from end point computers that you can use when creating your policies or troubleshooting user issues.

Troubleshooting End Point User Issues

If your users are unable to connect to your network, you may need to help them to become compliant. Have your users run the ICSInfo utility to determine what is wrong.

The ICSInfo utility provides the following information for supported operating systems:

- Host—Processor, Memory, OS
- User—User Name, Profile location, Groups
- Java—MS-JVM and Sun-JRE versions (and if they are installed)
- Browser—IE version (and if JRE is enabled), current default browser location and version
- Internet Options—The options set in the Internet Options of Internet Explorer (per zone).
- ICS Component—The ICS components currently on the end point computer
- Anti-Virus—The anti-virus application information
- Applications/Modules—The applications currently found on the end point computer
- Network Preferences—The settings for the installed network adapters

How to Troubleshoot End Point User Issues:

1. Have your end point user obtain the ICSinfo.exe file.

   The ICSInfo utility is available at:
   `http://myIP:31862/ics/components/icsinfo.exe`

   You might want to make this utility accessible to your users from your remediation server. To do so, save the file locally and hosting it on the remediation server.

2. Have your end point user run the ICSinfo.exe file.

3. Have your end point user perform the following steps to obtain the icsinfo.xml file:

   A Run the ICSinfo.exe file.

   B When prompted, click **Browse** and select a location to save the icsinfo.xml file.

C Click **Run**.

The ICSInfo utility runs and the file is saved to the specified location.

4 Have the end point user send the icsinfo.xml file to you for analysis.

Obtaining Anti-virus Application Information

When creating anti-virus enforcement rules, you need to use the correct format for your anti-virus provider information. This format varies from provider to provider. Use the ICSinfo utility to scan a reference computer to obtain the information for all the installed anti-virus programs in the correct format.

To Obtain Anti-virus Application Information:

1 Set up a reference computer with your anti-virus applications installed.

Be sure to obtain the updates for your anti-virus providers.

2 Obtain the ICSinfo.exe file and copy it to your reference computer.

The ICSInfo utility is available at:

`http://myIP:31862/ics/components/icsinfo.exe`

3 Run the ICSInfo.exe file

Using a command prompt run `ICSInfo.exe -avinfo`. When you run the ICSInfo utility using this parameter, the ICSInfo utility produces an icsinfo.xml file that contains only anti-virus application information.

4 Check the icsinfo.xml file for the application information.

Obtaining Application Checksums

Use the ICSInfo utility to obtain checksums for applications. Use these checksums when creating custom application enforcement rules. Since checksum are unique, verifying a file by checksum prevents another file from masquerading as that file.

To Obtain Application Checksums:

1 Set up a reference computer with a trusted copy of the application.

2 Obtain the ICSinfo.exe file and copy it to your reference computer, to the same location as your application.

The ICSInfo utility is available at:

`http://myIP:31862/ics/components/icsinfo.exe`

3 Run the ICSInfo.exe file

Using a command prompt run `ICSInfo.exe -fileinfo`. When you run the ICSInfo.exe file using this parameter the ICSInfo utility produces an icsinfo.xml file that contains the version, size, checksum and vendor information for each dll and exe file in the folder.

4 Open the icsinfo.xml file and use the information to create your custom application enforcement rules.

Index

R

S

T

U

W