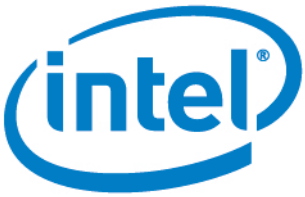


Intel® Setup and Configuration Software (Intel® SCS)

Intel® Enterprise Digital Fence Plugin

Version 1.1 Document

Release Date: Monday, September 21, 2015

Legal Information

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer.

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® Solid State Drives may require additional software, hardware, services and/or an Internet connection. Results may vary depending upon configuration. Consult your system manufacturer for more details.

Intel and the Intel logo, are trademarks of Intel Corporation in the U.S. and/or other countries.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the U.S. and/or other countries.

* Other names and brands may be claimed as the property of others.

Table of Contents

Glossary of Terms

Term	Description
AES	Advanced Encryption Standard
BSS	Basic Service Set
CCMP	Counter-Mode Cipher Block Chaining (CBC) Message Authentication Code (MAC) Protocol
DLL	Dynamic Link Library
GUID	Globally Unique Identifier
IEEE	Institute of Electrical and Electronics Engineers
Intel® SSD Pro Family	An entire Intel solid-state drive product line focused on security and manageability features
PSK	Pre-Shared Key
RSNA	Robust Security Network Association
SSD	Solid-State Drive
SSID	Server Set Identifier
WEP	Wired Equivalent Privacy
WMI	Windows Management Instrumentation
WPA	WiFi Protected Access
TKIP	Temporal Key Integrity Protocol

1 Introduction

This document describes the Intel® Enterprise Digital Fence Plugin and how to use it.

1.1 What is the Intel Enterprise Digital Fence Plugin?

The Intel® Enterprise Digital Fence Plugin is management software for Intel® Enterprise Digital Fence. You can use the plugin to manage all the configuration settings of Intel Enterprise Digital Fence.

The Intel Enterprise Digital Fence Plugin is fully integrated with Intel® Setup and Configuration Software (Intel® SCS). This integration lets you take advantage of the Intel SCS infrastructure to run operations on multiple platforms using scripts. This also makes it possible to run operations remotely and integrate them with your management console.

Note:

The Intel Enterprise Digital Fence Plugin integrates with Intel SCS via "Solution Plugins" and the Solutions Framework component of Intel SCS. This document contains specific information about how the Intel Enterprise Digital Fence Plugin has implemented features and capabilities made available by the Solutions Framework. For detailed information about the Solutions Framework, refer to the `Intel(R)_Solutions_Framework.pdf`. (The PDF is located in the `Solutions_Framework` folder of the Intel SCS download package.)

1.2 What Features are Supported?

This version of the Intel Enterprise Digital Fence Plugin supports remote configuration of the settings required to enable and manage Intel Enterprise Digital Fence. For more information, see Configuring Intel Enterprise Digital Fence on page 7.

1.3 What Do I Need to Install?

Before you can use the Intel Enterprise Digital Fence Plugin, you must make sure that the Solutions Framework is setup correctly on the host platforms. For information about the prerequisites and how to prepare the host platforms, refer to the `Intel(R)_Solutions_Framework.pdf`.

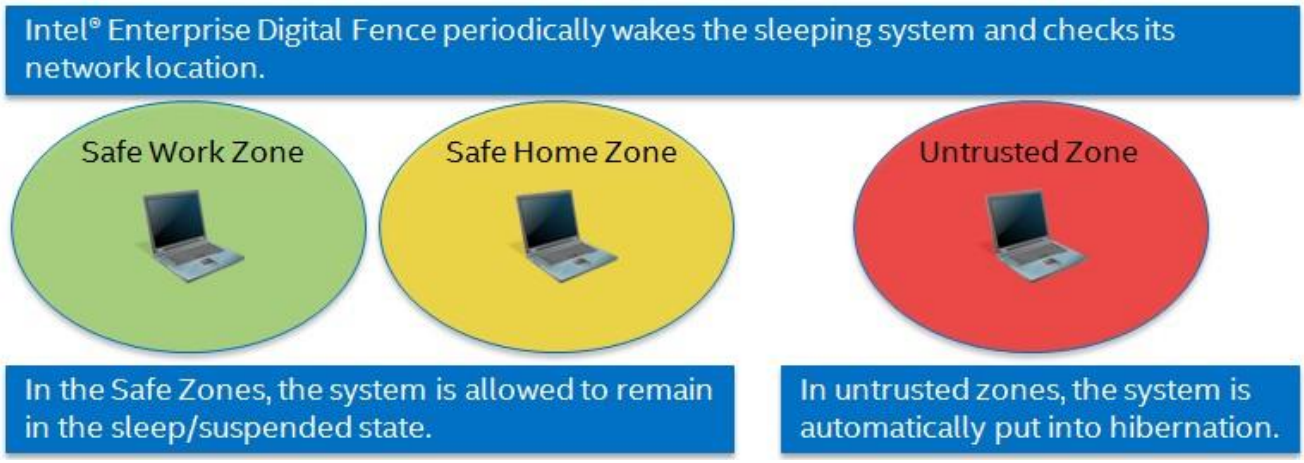
This table describes the "Solution Plugins" of Intel Enterprise Digital Fence.

Solution Plugin Type	Details
Host Plugin	**Name:** `DigitalFencePlugin.dll` This plugin is mandatory and must be installed on each of the host platforms where you want to use the Intel Enterprise Digital Fence Plugin features. The installer included in this download package is an MSI installation file that automatically installs both Intel Enterprise Digital Fence and the host plugin. The download package also includes a batch file named `DigitalFenceInstaller-silent-install.bat`. You can use this file to silently install when you deploy the installer using your software deployment mechanism. **Note:** • For the prerequisites of the installer, see What are the Prerequisites for the Installer? on the next page. • To identify the platforms on which to run the installer, see How Can I Find Platforms that Support Intel Enterprise Digital Fence? on page 5. • The Host solution Manager searches for the plugins by looking in the registry. The Intel Enterprise Digital Fence installer automatically adds the registry key for you during installation. (The location of the registry key is documented in the `Intel(R)_Solutions_Framework.pdf`.)
Profile Editor Plugin	**Name:** `DigitalFenceProfileEditor.dll` This plugin is used to create the configuration profiles for Intel Enterprise Digital Fence. This plugin is located in the DigitalFenceProfileEditor folder. To install this plugin: 1. Login to the computer running the Console component of Intel SCS. 2. Locate the Console Plugins folder. For example, the default installation folder of SCS 11.0 is: C:\Program Files\Intel\SCS11\Console\Plugins 3. Place the DigitalFenceProfileEditor folder in the Plugins folder. 4. Close and then open the Console again. **Note:** • The plugin includes help with information about the settings available in Intel Enterprise Fence configuration profiles. To open the help, click the help icon of the plugin (in the Console or the Profile Editor). • The plugin is supported only from version 10.0 of Intel SCS. You cannot use the plugin with Intel SCS 9.x.

1.4 How Does Intel Enterprise Digital Fence Work?

Intel Enterprise Digital Fence is a capability to enable location-oriented enforcement of a data protection policy for a system with encrypted storage. Many mobile computer users do not want the inconvenience of putting their system into a hibernation state. They prefer to simply close the laptop lid and let the system go into a suspend/sleep state. Since they know that their data is encrypted, they believe that their systems are safe in any situation. What they do not realize is that when a system goes into a suspend/sleep state, the disk is still encrypted, but the encryption keys remain in the system's RAM. This leaves the system in a vulnerable state to potential attacks. For example, malware can capture the encryption keys using Direct Memory Access (DMA) techniques and access the protected data. Until now, this meant that you could either trust your users to behave responsibly, or force them to use only the hibernation option.

With Intel Enterprise Digital Fence you can now define "Safe Zones" where the computer is allowed to remain in the sleep/suspend state. These are network configurations that you define and consider as trusted. You can include in the Safe Zone workplace networks (Work Zone Detection) and networks outside the workplace (Home Zone Detection). When the system is in a sleep/suspended state, the Windows-based service of Intel Enterprise Digital Fence periodically wakes the system to check if it is located in a Safe Zone. If the system is not located in a Safe Zone, the system is automatically forced into a hibernation state.



1.5 What are the Prerequisites for the Installer?

These are the prerequisites required to install and use Intel Enterprise Digital Fence:

- Version 4.0 of Microsoft .NET Framework
- The presence of an Intel SSD Pro 1500 Series or an Intel SSD Pro 2500 Series drive
- The sleep and hibernate power options must not be disabled. If they are disabled, there is no point installing and using Intel Enterprise Digital Fence. (Intel Enterprise Digital Fence uses the advanced power options "Allow Wake Timers" in the Windows operating system.)

Note:

The Intel Enterprise Digital Fence installer checks for these prerequisites and will not install if any of them are missing.

1.6 How Can I Find Platforms that Support Intel Enterprise Digital Fence?

The Solutions Framework includes "Platform Discovery" options that you can use to identify and locate Intel Enterprise Digital Fence in your organization. You can use these options to identify where you need to install the host plugin (`DigitalFencePlugin.dll`). For information about Platform Discovery, refer to the "Discovering and Publishing Data" section of the `Intel(R)_Solutions_Framework.pdf`.

The ID of Intel Enterprise Digital Fence (shown in the uuid attribute) is e8c6bb4d-eda0-4859-bc7a-197cf252cf88.

This is an example of the data returned when a platform does not support Intel Enterprise Digital Fence.

```
<Solution     uuid="e8c6bb4d-eda0-4859-bc7a-197cf252cf88"
          name="Intel(R) Enterprise Digital Fence" exist="false" state="not supported">
</Solution>
```

This is an example of the data returned when a platform supports Intel Enterprise Digital Fence, but the required software and host plugin are not installed. These are the platforms on which you should run the installer for Intel Enterprise Digital Fence. (The installer will install the service and the host plugin.)

```
<Solution     uuid="e8c6bb4d-eda0-4859-bc7a-197cf252cf88"
          name="Intel(R) Enterprise Digital Fence" exist="true" managed="false" state="supported">
     <Hardware version="INTEL SSDSC2BF180A4L- LSTi"/>
     <Software name="Intel(R) Enterprise Digital Fence Service" required="true" available="false" />
     <FrameworkPlugin available="false"/>
</Solution>
```

This is an example of the data returned when the Intel Enterprise Digital Fence Service and the host plugin are already installed on the platform.

```
<Solution     uuid="e8c6bb4d-eda0-4859-bc7a-197cf252cf88"
          name="Intel(R) Enterprise Digital Fence" exist="true" managed="true" state="enabled">
     <Hardware version="INTEL SSDSC2BF180A4L- LSTi"/>
     <Software name="Intel(R) Enterprise Digital Fence Service" required="true"
          available="true" version="1.1.0.42"/>
     <FrameworkPlugin available="true" version="1.0.0.1"/>
</Solution>
```

Element	Description

<Solution>	Possible attributes of the start tag of this element for Intel Enterprise Digital Fence:
	• uuid – The Globally Unique Identifier (GUID) of Intel Enterprise Digital Fence
	• name – The descriptive name of Intel Enterprise Digital Fence
	• exist – Indicates if the platform includes all the necessary hardware and firmware required to support Intel Enterprise Digital Fence (true or false)
	• managed – Indicates if the Solutions Framework is capable of managing the solution (true or false). This value will only be true if the host plugin of Intel Enterprise Digital Fence is installed and working correctly.
	• state – The state of Intel Enterprise Digital Fence . Possible values:
	  • not supported – The platform does not support Intel Enterprise Digital Fence
	  • supported – The platform supports Intel Enterprise Digital Fence
	  • enabled – Intel Enterprise Digital Fence is enabled
	  • disabled – Intel Enterprise Digital Fence is disabled

<Hardware>	Intel Enterprise Digital Fence requires an Intel SSD Pro 1500 Series or Intel SSD Pro 2500 Series drive. If the platform includes an SSD Pro Series drive, this element will show the version of drive.
<Software>	Possible attributes of this element for Intel Enterprise Digital Fence: • name – The name of the software • required – Whether the software is required (true or false) • available – Whether the software is installed on the platform (true or false) • version – The version of the software (if the software is installed)
<FrameworkPlugin>	A void element containing attributes describing the host plugin: • available – Whether the host plugin is installed on the platform (true or false) • version – The version of the host plugin (if the host plugin is installed)

2 Using the Intel Enterprise Digital Fence Plugin

This section describes how to use the features and options supported by the Intel Enterprise Digital Fence Plugin. For version 1.0 of the host plugin this means configuration using profiles (the other Solutions Framework capabilities were not implemented)

2.1 Configuring Intel Enterprise Digital Fence

Configuration profiles contain the configuration settings that will be put in the solution during configuration. Profiles for Intel Enterprise Digital Fence are created using the profile editor plugin of Intel Enterprise Digital Fence. This plugin can be loaded by the Console or Profile Editor components of Intel SCS. When loaded, the profile editor plugin of Intel Enterprise Digital Fence shows the settings that it supports. For descriptions of these settings, click the help icon of the plugin (in the Console or Profile Editor).

To help you decide which component to use to create the profile, and for instructions how to use them, refer to these sections in the `Intel(R)_Solutions_Framework.pdf`:

- Which Component Should I use to Create Profiles?
- Using the Console to Create Profiles
- Using the Profile Editor to Create Profiles

You can then use the profile with the `SCS-Configure.ps1` script or the `Configure` method. These examples show how to use the `SCS-Configure.ps1` script to configure Intel Enterprise Digital Fence.

Example #1: To configure using a profile created in the Console:

```
.\SCS-Configure.ps1 -ComputerName MyHost.Domain.com
  -Component e8c6bb4d-eda0-4859-bc7a-197cf252cf88
  -RCS rcs.domain.com -ProfileName "ProfileinRCS"
```

Example #2: To configure using a profile created using the Profile Editor:

```
.\SCS-Configure.ps1 -ComputerName MyHost.Domain.com
  -Component e8c6bb4d-eda0-4859-bc7a-197cf252cf88
  -ProfileFile "MyDigitalFenceProfile.xml"
```

3 Supported Methods and Scripts

This section includes information that is specific to how some of the Solutions Framework methods and scripts were implemented by the Intel Enterprise Digital Fence Plugin.

> **Note:**
>
> For a full description of the methods, syntax, and prerequisites, refer to the `Intel(R)_Solutions_Framework.pdf`.

3.1 Supported Solutions Framework API Methods

The Solutions Framework API is a Windows Management Instrumentation (WMI) provider that exposes classes and methods used by the Host Solution Manager of the Solutions Framework.

This version of the Intel Enterprise Digital Fence Plugin supports these methods:

- PlatformDiscovery (see How Can I Find Platforms that Support Intel Enterprise Digital Fence? on page 5)
- Recalculate
- RefreshSolutions
- GetConfiguration
- Configure (see Configuring Intel Enterprise Digital Fence on the previous page)
- EnumeratePermissions
- AddPermissions
- RemovePermissions

This version of the Intel Enterprise Digital Fence Plugin does not support these methods:

- SolutionDiscovery
- UnConfigure
- GetKPIs
- GetAndResetKPIs
- ResetKPIs
- GetAttribute
- SetAttribute
- ApplyCommandSync
- BackupSolutionSettings
- RestoreSolutionSettings
- CountEvents
- ClearAllEvents

3.2 Supported Scripts

The Solutions Framework contains example Windows PowerShell scripts (in the `Scripts` subfolder in the `Solutions_Framework` folder). The scripts are ready to use as they are, or you can edit and tailor them to your specific requirements.

For information about running PowerShell scripts, refer to this page in the Microsoft Technet site: http://technet.microsoft.com/en-us/library/ee176949.aspx.

The scripts include command line help. To open the help, from the PowerShell command line, type this:

```
get-help .\script-name.ps1 -full
```

This version of the Intel Enterprise Digital Fence Plugin supports these scripts:

- SCS-Permissions.ps1
- SCS-PlatformDiscovery.ps1
- SCS-GetConfiguration.ps1
- SCS-Configure.ps1

This version of the Intel Enterprise Digital Fence Plugin does not support these scripts:

- SCS-SolutionDiscovery.ps1
- SCS-ReadKPI.ps1
- SCS-ResetKPI.ps1
- SCS-GetAttribute.ps1
- SCS-SetAttribute.ps1
- SCS-ApplyCommand.ps1
- SCS-GetEvents.ps1
- SCS-ClearEvents.ps1
- SCS-Unconfigure.ps1

3.3 Error Codes

This table describes the possible error codes returned by the Intel Enterprise Digital Fence Plugin when running the Configure API.

Code	Description
1000	At least one of the Boolean values defined in the configuration profile is spelled incorrectly. Valid values: • true • false
1001	At least one of the security types defined in the configuration profile is invalid. Check that the values in the <Int32> child elements of <AllowedAuthenticationAlgorithms> are all valid values (see Authentication Algorithms on page 17).
1002	At least one of the encryption types defined in the configuration profile is invalid. Check that the values in the <Int32> child elements of <AllowedCipherAlgorithms> are all valid values (see Encryption Algorithms on page 17).
1003	The sleep period defined in the configuration profile is invalid. Check that the value in the <S3SleepDurationSeconds> is a value between 300 seconds and 3600 seconds.
1004	Failed to serialize the Wireless Work Networks defined in the configuration profile in the <WirelessData> elements.
1005	Failed to serialize the IP Subnets defined in the configuration profile in the <Subnet> elements.
1006	Failed to write and save the configuration values in the registry.

4 XML Reference

This section describes the format and content of the XML documents created and used specifically by the host plugin of Intel Enterprise Digital Fence. For version 1.0 of the host plugin this means configuration profiles (the other Solutions Framework capabilities were not implemented).

4.1 Configuration Profile

This is an example of a configuration profile.

```
<Management version="1.0.0.13">
    <ManagedElement     component-id="e8c6bb4d-eda0-4859-bc7a-197cf252cf88">
        <Profile>
            <Network>
                <WorkZoneDetectionEnabled>true</WorkZoneDetectionEnabled>
                <HomeZoneDetectionEnabled>true</HomeZoneDetectionEnabled>
                <AllowOnlySecureNetworks>true</AllowOnlySecureNetworks>
                <AllowWiredNetwork>true</AllowWiredNetwork>
                <CheckDomainController>true</CheckDomainController>
                <SSIDBlacklist>linksys|NETGEAR|dlink|default|hpsetup|wireless</SSIDBlacklist>
                <AllowedAuthenticationAlgorithms>
                    <Int32>6</Int32>
                    <Int32>7</Int32>
                </AllowedAuthenticationAlgorithms>
                <AllowedCipherAlgorithms>
                    <Int32>2</Int32>
                    <Int32>4</Int32>
                </AllowedCipherAlgorithms>
                <WorkWirelessNetwork>
                    <WirelessData>
                        <SSID>WorkNetwork1</SSID>
                        <Name>Primary Network</Name>
                        <AuthenticationAlgorithm>6</AuthenticationAlgorithm>
                        <CipherAlgorithm>4</CipherAlgorithm>
                        <SecurityEnabled>true</SecurityEnabled>
                    </WirelessData>
                    <WirelessData>
                        <SSID>WorkNetwork2</SSID>
                        <Name>Secondary Network</Name>
                        <AuthenticationAlgorithm>6</AuthenticationAlgorithm>
                        <CipherAlgorithm>4</CipherAlgorithm>
                        <SecurityEnabled>true</SecurityEnabled>
                    </WirelessData>
                </WorkWirelessNetwork>
                <DomainSuffix>
                    <AllowCheck>true</AllowCheck>
                    <SuffixList>
                        <Suffix>example1.com</Suffix>
```

```
                        <Suffix>example2.com</Suffix>
                    </SuffixList>
                </DomainSuffix>
                <DNSServers>
                    <AllowCheck>true</AllowCheck>
                    <DNSList>
                        <DNS>10.247.2.1</DNS>
                        <DNS>10.3.80.100</DNS>
                        <DNS>10.19.1.2</DNS>
                    </DNSList>
                </DNSServers>
                <IPSubnets>
                    <AllowCheck>true</AllowCheck>
                    <SubnetsList>
                        <Subnet>
                            <NetworkAddress>10.217.75.0</NetworkAddress>
                            <Mask>255.255.252.0</Mask>
                        </Subnet>
                    </SubnetsList>
                </IPSubnets>
            </Network>
            <CustomAction>
                <LibrariesPath>
                    <Path>C:\fullpath\customplugin.dll</Path>
                </LibrariesPath>
            </CustomAction>
            <Time>
                <PeriodicWakeEnabled>true</PeriodicWakeEnabled>
                <S3SleepDurationSeconds>900</S3SleepDurationSeconds>
            </Time>
        </Profile>
    </ManagedElement>
</Management>
```

Element	Description
<Management>	A normal (root) element containing all the child elements of the XML document. Possible attributes of the start tag of this element: • version - The version of the profile. In profiles created by the profile editor plugin of Intel Enterprise Digital Fence, this is the version of the plugin DLL (`DigitalFenceProfileEditor.dll`) used to create the profile.

Element	Description
<ManagedElement>	A normal element containing attributes and child elements describing a specific solution component. Possible attributes of the start tag of this element: • component-id - The GUID of Intel Enterprise Digital Fence **Note:** Profiles created by the profile editor plugin of Intel Enterprise Digital Fence will also include attributes with references to the XML schema. These attributes are not mandatory and are only included to improve XML parsing of the file.
<Profile>	A normal element containing all the child elements of the configuration profile.
<Network>	The child elements of <Network> contain settings that define how Intel Enterprise Digital Fence will check and decide if a computer is located in the safe zone.
<WorkZoneDetectionEnabled>	Defines if work zone detection is enabled. Valid values: • true – Enable work zone detection • false – Disable work zone detection
<HomeZoneDetectionEnabled>	Defines if home zone detection is enabled. Valid values: • true – Enable home zone detection • false – Disable home zone detection
<AllowOnlySecureNetworks>	Defines if their are any restrictions to the networks that the user can add to the safe zone. • true – The user will only be allowed to add networks that are configured with the security types and encryption types that you define in the <AllowedAuthenticationAlgorithms> and <AllowedCipherAlgorithms> elements. When this value is true, you must define at least one security type and one encryption type. • false – The user will be allowed to add any wireless network to the safe zone, regardless of its security settings
<AllowWiredNetwork>	Defines if wired connections are allowed in the safe zone. • true – Wired connections will be included in the safe zone if they comply with the security restrictions you define in the <CheckDomainController>, <DomainSuffix>, <DNSServers>, and <IPSubnets> elements. When this value is true, you must define at least one of these security restrictions. • false – All wired connections will be considered unsafe. When this value is false, you must define at least one work wireless network in the <WorkWirelessNetwork> element.

Element	Description
<CheckDomainController>	Defines if Intel Enterprise Digital Fence will check will check for the presence of an Active Directory domain controller. • true – Check for the presence of an Active Directory domain controller. The network will only be included in the safe zone if this check is successful. • false – Do not perform this check
<SSIDBlacklist>	A Server Set Identifier (SSID) is the name that is broadcasted by a wireless network to enable computers to connect to the network. Routers and access points include built-in factory default SSIDs. When a wireless network uses the default SSID it is an indication that the network is not secure. (For example, if the name was not changed then maybe the default password was also not changed.) You can define a blacklist of the most common SSIDs that your users might use. If an SSID is included in this blacklist, the user will not be allowed to add that network to the safe zone. **Note:** Make sure that each SSID is separated with a | character, as shown in the example.
<AllowedAuthenticationAlgorithms>	The security type of a network defines the authentication algorithm that the network is configured to use (see Authentication Algorithms on page 17). Create an <Int32> element for each of the security types that you consider are safe. The user will only be allowed to add networks that use one of the security types defined in this list of <Int32> elements. **Note:** If the value of <AllowOnlySecureNetworks> is true, this element must contain at least one child <Int32> element.
<AllowedCipherAlgorithms>	The encryption type of a network defines the encryption algorithm that the network is configured to use (see Encryption Algorithms on page 17). Create an <Int32> element for each of the encryption types that you consider are safe. The user will only be allowed to add networks that use one of the encryption types defined in this list of <Int32> elements. **Note:** If the value of <AllowOnlySecureNetworks> is true, this element must contain at least one child <Int32> element.
<WorkWirelessNetwork>	The child elements of <WorkWirelessNetwork> define which wireless networks in the workplace will be included in the safe zone.
<WirelessData>	Create a <WirelessData> element for each wireless work network that you want to include in the safe zone. When a user is connected to any of these networks during sleep periods, Intel Enterprise Digital Fence will also perform other checks, depending on the configuration of the <CheckDomainController>, <DomainSuffix>, <DNSServers>, and <IPSubnets> elements.
<SSID>	The network's SSID

Element	Description
<Name>	The network's profile name
<AuthenticationAlgorithm>	The network's security type (see Authentication Algorithms on page 17)
<CipherAlgorithm>	The network's encryption type (see Encryption Algorithms on page 17)
<SecurityEnabled>	Defines if the network has it's security enabled. Valid values: • true • false
<DomainSuffix>	The child elements of <DomainSuffix> define if Intel Enterprise Digital Fence will check to which domain the computer is currently associated.
<AllowCheck>	Valid values: • true – Check to which domain the computer is currently associated. The computer will only be considered to be in the safe zone if it is associated to one of the domains defined in the <SuffixList>. • false – Do not perform this check (any entries in the <SuffixList> will be ignored) **Note:** When enabled, this check is done on both wired and wireless networks.
<SuffixList>	The list of domain suffixes
<Suffix>	Create a <Suffix> element for each domain suffix
<DNSServers>	The child elements of <DNSServers> define if Intel Enterprise Digital Fence will check to which IP subnet the computer is currently associated.
<AllowCheck>	Valid values: • true – Check to which DNS server the computer is currently associated. The computer will only be considered to be in the safe zone if it is associated to one of the DNS servers defined in the <DNSList>. • false – Do not perform this check (any entries in the <DNSList> will be ignored) **Note:** When enabled, this check is done on both wired and wireless networks.
<DNSList>	The list of DNS servers
<DNS>	Create a <DNS> element for the IP address of each DNS server
<IPSubnets>	The child elements of <IPSubnets> define if Intel Enterprise Digital Fence will check to which IP subnet the computer is currently associated.

Element	Description
<AllowCheck>	Valid values: • true – Check to which IP subnet the computer is currently associated. The computer will only be considered to be in the safe zone if it is associated to one of the IP subnets defined in the in the <SubnetsList>. • false – Do not perform this check (any entries in the <SubnetsList> will be ignored) **Note:** When enabled, this check is done on both wired and wireless networks.
<SubnetsList>	The list of IP subnets
<Subnet>	Create a <Subnet> element for each IP subnet
<NetworkAddress>	The network's IP address
<Mask>	The network's mask
<CustomAction>	The child elements of <CustomAction> contain settings that define customizations of Intel Enterprise Digital Fence.
<LibrariesPath>	The capabilities of Intel Enterprise Digital Fence can be extended and customized using a third-party plugin. If you have a plugin and want to use it, specify the path to the plugin DLL file in the <Path> element. (Only one plugin is supported.)
<Path>	The full path (including the DLL filename) to the location of the custom plugin DLL
<Time>	The child elements of <Time> contain settings that define how often Intel Enterprise Digital Fence will wake up the computer.
<PeriodicWakeEnabled>	Defines if Intel Enterprise Digital Fence is allowed to wake up the computer from sleep and active standby modes. Valid values: • true • false – Only use this setting when you want to disable Intel Enterprise Digital Fence
<S3SleepDurationSeconds>	Defines the frequency (in seconds) at which Intel Enterprise Digital Fence will wake up the computer from sleep and active standby modes to check if the computer is in a safe zone. Minimum: 300 seconds (5 minutes). Maximum: 3600 seconds (60 minutes).

Authentication Algorithms

Value	Security Type	Description
1	Open	802.11 open system authentication algorithm
2	Shared Key	802.11 shared key authentication algorithm that requires the use of a pre-shared Wired Equivalent Privacy (WEP) key for 802.11 authentication
3	WPA	WiFi Protected Access (WPA) algorithm
4	WPA-Personal	WPA algorithm that uses Pre-Shared Keys (PSK). This algorithm is valid only for Basic Service Set (BSS) of the infrastructure type.
6	WPA2-Enterprise	802.11i Robust Security Network Association (RSNA) algorithms. For example, WPA2. These algorithms are valid only for BSS of the infrastructure type.
7	WPA2-Personal	The 802.11i RSNA algorithm that uses PSK. This algorithm is valid only for BSS of the infrastructure type.

Encryption Algorithms

Value	Encryption Type	Description
0	None	No encryption algorithm is enabled or supported
1	WEP 40	Wired Equivalent Privacy (WEP) encryption algorithm with a 40-bit encryption key. (WEP is the RC4-based algorithm that is specified in the 802.11-1999 standard.)
2	TKIP	Temporal Key Integrity Protocol (TKIP) algorithm. (TKIP is the RC4-based algorithm suite that is based on the algorithms that are defined in the WPA specification and IEEE 802.11i-2004 standard.)
4	AES CCMP	AES-CCMP algorithm, as specified in the IEEE 802.11i-2004 standard and RFC 3610
5	WEP 104	Wired Equivalent Privacy (WEP) encryption algorithm with a 104-bit encryption key
256	WPA or RNS Use Group	WiFi Protected Access (WPA) or a Robust Security Network (RSN) Use Group Key cipher suite. (For more information about the Use Group Key cipher suite, refer to clause 7.3.2.25.1 of the IEEE 802.11i-2004 standard.)
257	WEP	WEP encryption algorithm with an encryption key of any length

5 Integration with Microsoft SCCM

You can also integrate the Intel Enterprise Digital Fence installer (and plugin) with Microsoft System Center Configuration Manager (SCCM). You can do this using the Intel® SCS Add-on for Microsoft* SCCM (referred to in this document as "the Add-on"). The Add-on is a configuration wizard that you can use to integrate Intel SCS with SCCM. For each Add-on component that you select to install, the Add-on creates collections, advertisements, packages, and task sequences for you in SCCM. Each of the items that the Add-on creates in SCCM is automatically pre-configured for you. When you run the Add-on, in the Select Components window, simply click **Add** and then browse and select the installer for Intel Enterprise Digital Fence.

The Add-on is available as a separate download package on the Intel SCS website. For information about how to use the Add-on, refer to the documentation supplied with the Add-on.

Unsupported Capabilities

Currently, the Add-on cannot query the plugin installer to find out which capabilities it supports. The same list of capabilities are displayed for all solutions. When you reach the window to select the capabilities of Intel Enterprise Digital Fence, do not select these check boxes:

- **Discover** (because the `SolutionDiscovery` method is not supported)
- **Unconfigure** (because the `Unconfigure` method is not supported)

If you select these check boxes, the Add-on will create SCCM objects for these operations, even though they are not supported (for example task sequences).

Incorrect Solution GUID in Add-on

Version 2.1.5 and earlier of the Add-on had a known issue where an incorrect GUID for the solution was inserted in some of the collections and task sequences.

This issue has been fixed in version 2.1.6 of the Add-on.

If you used version 2.1.5 to add Intel Enterprise Digital Fence to SCCM, you have two options:

1. Run version 2.1.6 of the Add-on, and in the Select Components window, select **Change** for the Intel Enterprise Digital Fence component. This will re-install the Intel Enterprise Digital Fence component with the correct GUID in the objects created by the Add-on.

- OR -

2. Manually correct the GUID in these locations:

- The queries of these collections:
  - Intel Enterprise Digital Fence: Managed
  - Intel Enterprise Digital Fence: Plugin Available
  - Intel Enterprise Digital Fence: Plugin Not Installed
- The command line of this task sequence: Intel Enterprise Digital Fence: Configuration

Note:

The correct GUID for Intel Enterprise Digital Fence is `e8c6bb4d-eda0-4859-bc7a-197cf252cf88`.