efficient iP®

Datasheet

Identity Manager

Enrich your DDI Automation with Identity Information

Highlights:

- Provide visibility on who is using the network/apps from where and when
- Enrich central repository with user information (complement IP, devices, applications, VLAN ...)
- Bring visibility on main identity information to network teams
- Offer a simple and easy way to find user associated with an IP address (plus device, DHCP lease, reverse DNS record...)
- Enable automation based on identity info in addition to technical attributes like IP or MAC address
- Integrate seamlessly to Microsoft Active Directory with real time notifications for single view of all active network sessions

SOLIDserver IPAM is used for managing IP addresses and subnets. With Identity Manager, the EfficientIP solution brings the application users as a new facet.

By collecting real-time events on user sessions with additional metadata through directory synchronization, and linking this information to the IP source of truth, Identity Manager provides visibility for each user session associated with its duration and device location answering the questions:

- WHO is using the network?
- From WHERE?
- WHEN?

Global Visibility on User Activity

Infrastructure visibility is mandatory for I&O personnel. Having the ability to easily link the application users to the rest of the infrastructure assets offers a real advantage in global operations and especially in troubleshooting and forensic activities. By which user is this IP address being used? Does this device belong to the user using it on a regular basis? Who is currently on the network from this department? From this branch office? Finding answers quickly to these questions is not so easy, and is further complicated for large networks with vast numbers of users.

Identity Manager collects information on the users of the IT system and on their network and application sessions. All this information is available in a specific SOLIDserver manager section in order to provide quick access to both identities and their respective parameters, as well as the flow of network sessions. With a link between the user session and the IP address where it is used, the IPAM is automatically enriched and can provide a new session facet to DDI activities. This enables the simplification of numerous I&O activities.

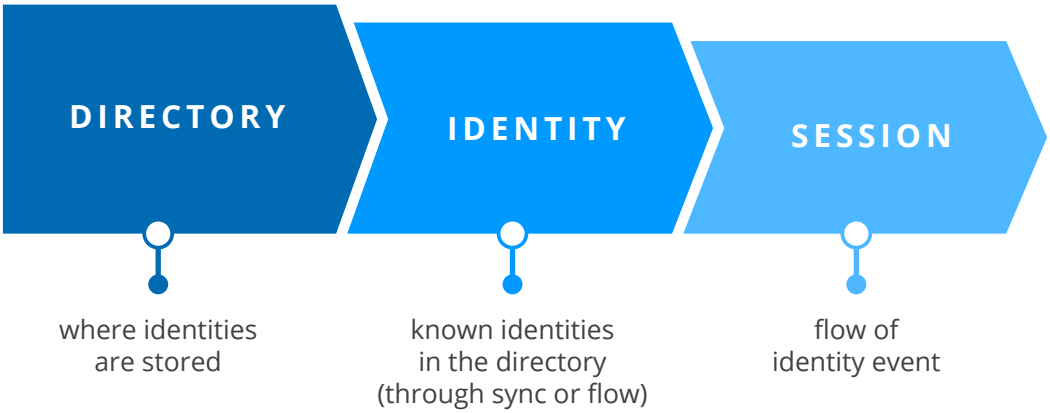
Identity Objects Expand the IPAM Coverage

SOLIDserver Identity Manager is a complete module with its own object topology. It presents information about users' identity and their sessions on the network. The manager presents information at 3 different levels: the directory, the identity and the session.

First, the directory view stores all the known sources of information about identities and sessions. With Microsoft Active Directory, one entry is listed per domain, allowing to focus only on the identities and sessions belonging to it.

The second level contains all the identities belonging to the directories. Depending on the activation of the synchronization each identity may be augmented with its associated parameters like name, phone number or job department. By default, only the identity of the user is available, corresponding most of the time to its login credential. This view allows quick access to the identities on the IT system, very easy to use with all the search and filter facilities offered by the listing in SOLIDserver. It also exposes this information through the API to authorized applications.

The third level is dedicated to the sessions. Each authentication or authorization of a user on the IT system - either at network level or application level - is automatically pushed towards the Identity Manager module as session information. A session is associated with an identity and a directory, the listing associated to this third level displays the technical source of the messenger - for Active Directory this is the Domain Controller. It also displays the start and stop date, as well as the last event received for the session, which can be either termination or session continuation information. Most importantly, each session is associated with the IP address from where it is used. This view is very powerful as it offers a backward link between an IP address and an identity. The IP address is pivotal and therefore links automatically in the DDI to a lot of information such as the device in Device Manager, a DHCP lease or a switch port in NetChange. Combining this valuable information can bring value for troubleshooting activities and security forensic researches where time to access information is vital.

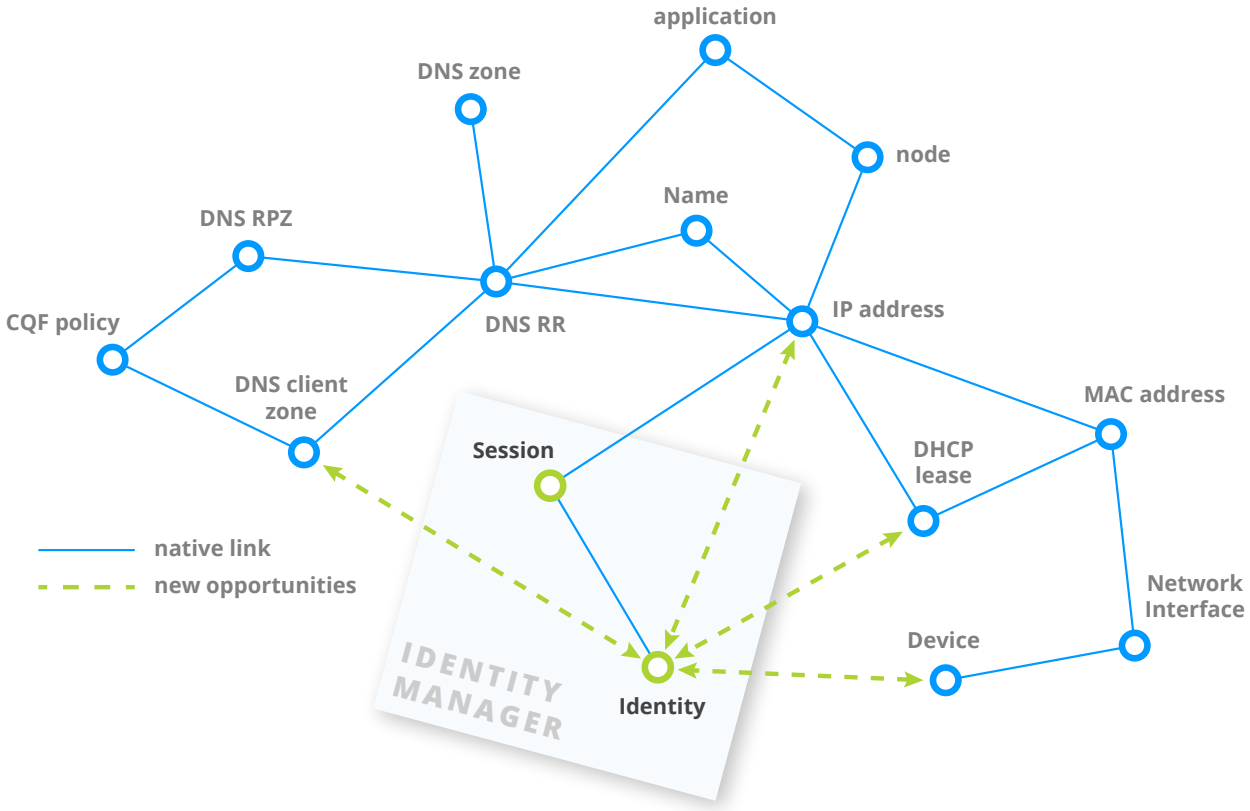


Rich DDI Automation with Identity Information

The IPAM web interface integrates search for identity and sessions through the Global Search feature. It also integrates the manager itself with the standard alerting system of the SOLIDserver to be automatically informed whenever a specified situation is reached. For example, a user connected from a specific subnet at night time or an administrator session from an IP address which is not allowed to perform such an operation can raise a trigger and send an alarm to the SOC.

The Identity Manager expands the possible use cases with a DDI solution. Having user information linked to the IP address of their device is very powerful and expands the topology of the DDI objects to a new extent. For example, at a specific operation time, it is possible to link the IP addresses and identity sessions active on the network in order to validate that nobody is still connected on a site on which the network will be under maintenance. If any users are connected on the site at maintenance time, it will be possible to easily contact them through information in the inventory. Another interesting use case concerns use of Device Manager, which inventories devices and not only the IP addresses. Device Manager therefore is a nice location of identity information. It is possible to perform an automatic inventory of which user is using which device and provide plenty of reporting and alerts on specific situations like the change of a user using a device or filtering devices without a known user.

As a specific module, Identity Manager brings a dedicated set of API calls helping external IT tools to automate actions and analysis. The 3 element types are available to list and search through the API: directory, identity and session. Session listing is helpful for a dynamic visualization of the user connected to the network or the IT services, for searching active sessions and the association between an identity and an IP address.

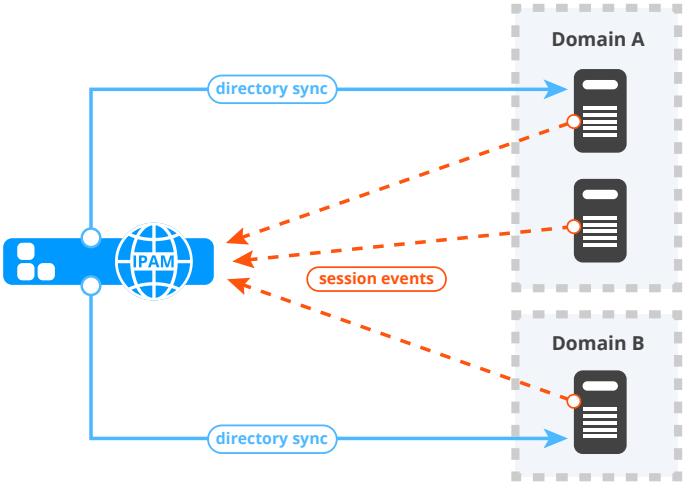


Automatic Collection of Microsoft Active Directory Session Events

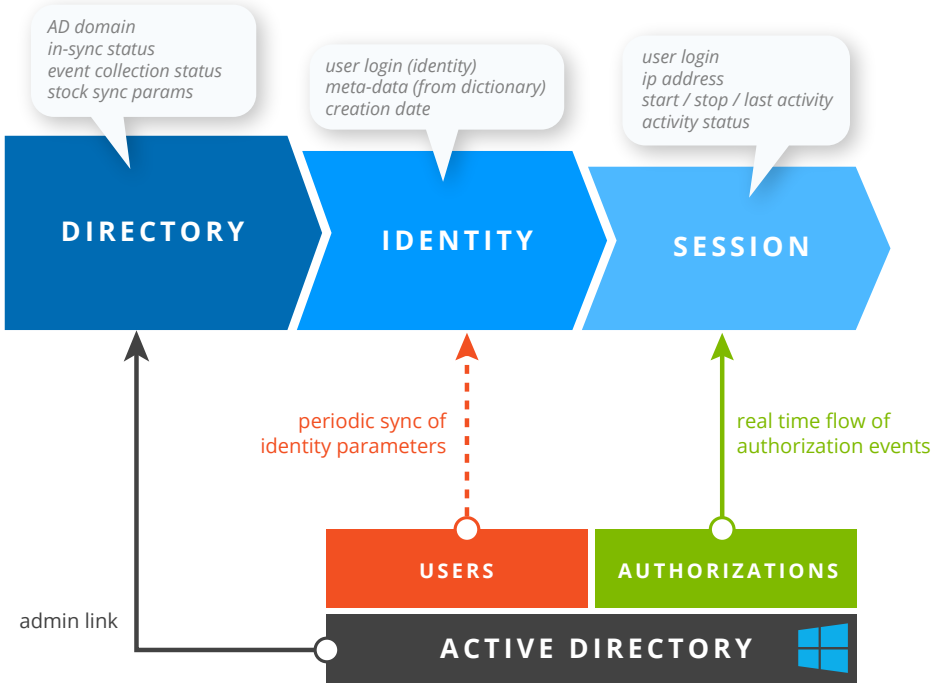
Microsoft Active Directory is available as a standard directory in the Identity Manager module. Therefore any Active Directory Domain Controller can be configured to push its events to the SOLIDserver, providing valuable information through user sessions. As soon as a Domain Controller is configured, any new user activity requiring an authentication or an authorization using the SSO (Single Sign On) mechanism will be directly forwarded to the SOLIDserver. Upon analysis, each authorization event received by the Identity Manager automatically updates the identity session list. Sessions expire automatically in the Domain Controller as well as in the Identity Manager. The directory list is automatically maintained through discovered domains in the identity sessions, providing a very easy way to configure the Identity Manager module.

Communication between the Active Directory Domain Controller and the SOLIDserver is highly secured through mutual authentication based on digital certificates. The events filtering and forwarding facility is authorized at the Domain Controller level, it therefore can be enabled and disabled easily and more importantly can be audited with regards to security and data protection to remain compliant with corporate policies. Only the valuable events required to get information from sessions are utilized by the Identity Manager module, this guarantees data protection and allows scalability of the service.

In order to enrich the identities information, it is possible to configure Identity Manager to perform at regular intervals a synchronization of some user parameters from the Active Directory. The list of standard parameters is tunable, in order to comply with regulatory requirements and with the visibility I&O teams would like to provide through the IPAM interface and API to the IT ecosystem. This synchronization is not mandatory, the Active Directory manager may control the level of information shared with the DDI solution without providing any security credentials. Security and confidentiality of user information is therefore ensured.

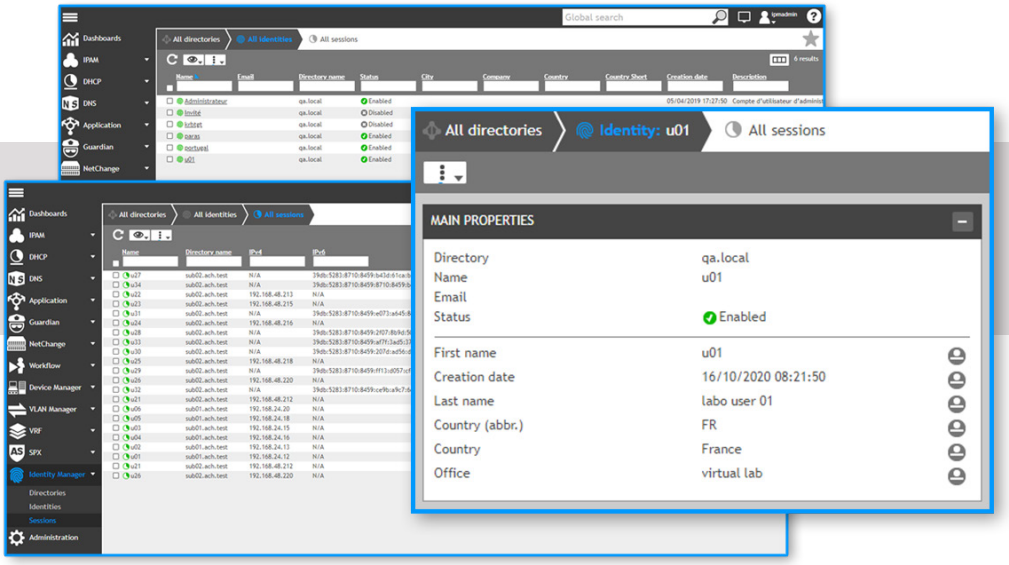


Traffic flows between the DCs & SOLIDserver



Better Collaboration Between I&O Teams

Identity Manager brings some visibility to the network team about each user logged onto the network, and various information about them contained in the central directory. By enabling this visibility about identities, even restricted to some parameters that can be shared with various teams and tools through automation, the immediate result is better communication between the teams and less siloed information. Where it is complex for network and security administrators to easily obtain information about who is using an IP address (even more complex when behind a MAC address), it becomes smoother with Identity Manager. By eliminating the need to develop a complex enterprise directory software, leveraging the information contained in the Active Directory and all the rich parameters that are already available can be a source of workflow efficiency. And where the information contained in the directory is already easily accessible, the information on sessions and the rich link between an IP address and an identity will bring multiple benefits.



SOLIDserver Sizing

Each SOLIDserver appliance has the ability to handle a specific identity amount with optimal performances, the limits per model are indicated in the table below:

Model	SDS-270	SDS-570	SDS-1170	SDS-2270	SDS-3370	SDS-7070
Maximum Identities managed	500	1 500	5 000	10 000	25 000	50 000

Note: the service only series (SDS-50 and BLAST) are not supporting any IPAM feature.

efficient iP®

REV: C-201028

As one of the world's fastest growing DDI vendors, EfficientIP helps organizations drive business efficiency through agile, secure and reliable network infrastructures. Our unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, our unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on us to help control the risks and reduce the complexity of challenges they face with modern key IT initiatives such as cloud applications, virtualization, and mobility. Institutions across a variety of industries and government sectors worldwide rely on our offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams.

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752