

Managing Different Devices and Network Access Policy Safely



One of Europe's largest Cisco ISE deployments enables Kela to secure flexible working practices and simplify IT management

EXECUTIVE SUMMARY

Customer Name: Kela

Industry: Government

Location: Finland

Number of Employees: 7500

Challenge

- Introduce BYOD-enabled flexible working while maintaining data security
- Reduce consequent workload on IT team

Solution

- Cisco Smart Security solution, providing policy-based access control, identity-aware networking, and data integrity and confidentiality
- Cisco products and services include TrustSec, Identity Services Engine, and Prime Infrastructure Manager

Results

- Provided secure authentication for 7500+ users
- Cut phone configuration time to zero
- Improved network troubleshooting

Challenge

Kela is the national social security provider for Finland, processing more than four million benefit applications and over €13.5 billion in benefit payments annually. Like many public sector organizations, it is constantly looking to improve the efficiency and quality of citizen services. Employee mobility is an intrinsic part of this plan. With a highly distributed workforce of 7500 employees spread across 400 locations, the agency introduced flexible working practices over a decade ago.

At that time, the main IT focus was on securing corporate devices and vast amounts of confidential data across wired and virtual private networks. This approach used RADIUS access control servers and, more recently, a Cisco Secure Access Control System. However, things changed when Kela deployed wireless networking. With employees increasingly seeking to connect personal devices, the agency was forced to rethink IT strategy.

"A powerful and flexible unified access security system was needed, one that could enforce a safe bring-your-own-device policy and manage different devices like Samsung GalaxyTabs, Nokia Lumia phones, Apple iPhones and iPads, and so on," says Juha Lappalainen, development manager at Kela.

Solution

Kela issued a significant public sector tender for WAN, LAN, and fixed and mobile voice services. Elisa, a Cisco® Gold Certified Partner and already the agency's WAN provider, won the tender, which included security services with a Cisco Smart Security proposal.

"In addition to the advanced security functionalities of Cisco switches, Elisa has strong knowledge of Cisco solutions and experience of running Cisco-based business-critical networks," says Lappalainen. "The Cisco team actively offers new ideas and helps us if and when needed."



“ISE and Prime are very good: secure, flexible, and offering greater network visibility. With ISE, we can also apply a posture health check for workstations, to ensure end devices are compliant with our security policy.”

Juha Lappalainen
Development Manager
Kela

Elisa installed the new solution following a Cisco TrustSec® Validated Design, and now operates it on behalf of Kela. At the solution's center is the Cisco Identity Services Engine (ISE), which forms a security policy management and control platform. It enforces usage policies in conjunction with Cisco TrustSec across wired and wireless networks and potentially VPNs. Kela also uses ISE for a range of other functions, including access control, profiling, and security posture policies on endpoints.

This holistic approach also incorporates Cisco Prime™ Infrastructure Manager, which is used for gaining insight into the network, troubleshooting, and in-depth reporting. Completing the Cisco Smart Security solution, Cisco Mobility Services Engine forms a wireless intrusion prevention system for solving connectivity problems and capturing network events that can be used to create a knowledge base.

These integrated components protect a vast IT infrastructure comprising around 900 Cisco Catalyst® 2960-S, 3750-X, and 6509 Series Switches, with more than 300 Cisco Aironet® 2600 Series Access Points and two Cisco 5508 Series Wireless Controllers. For redundancy, Kela has an ISE server at both of its main data centers, along with fully redundant Active Directory and application servers. RADIUS server load-balancing is implemented as a feature on the Cisco Catalyst switches, along with Cisco AutoQoS to help ensure prioritization for IP telephony and video data traffic.

The organization has different access policies and mechanisms for different devices. Extensible Authentication Protocol (EAP)-Transport Layer Security machine certificates are used for Kela assets. Meanwhile, EAP-Protected Extensible Authentication Protocol is used for bring-your-own-device (BYOD) endpoints. For IP phones, Kela uses MAC Authentication Bypass (MAB) to provide limited access for endpoints that the network does not recognize. “Machine certificates are our preferred authentication method. They offer strong authentication and best automation for device access control,” adds Lappalainen.

Results

The Cisco Smart Security solution provides authentication for around 7500 users and some 8000 workstations and laptops, 3000 BYOD endpoints (mainly Apple iPads), 5000 IP phones, and more than 2000 smartphones. In addition, ISE grants access to around 1000 multipurpose devices and printers along with 300 other assorted network devices.

The Kela Cisco ISE deployment is one of the largest in Europe. Importantly, Kela is able to deal with the BYOD trend easily and securely. “ISE has the intelligence to handle the access policy for different devices and user needs,” says Lappalainen.

Furthermore, the four-strong IT team saves time whenever a new company phone is handed out because there is no longer any need to carry out a manual port configuration. Instead users download their phone configuration from a Trivial FTP server and have the device registered on the system.

“ISE has automated and simplified access control for network devices such as printers, IP phones, and thin-clients and now we have enhanced visibility of our network,” says Ilari Saikkonen, senior IT specialist, Kela.

Pre-known phones connect via a separate VLAN with authentication through EAP-Message Digest 5 (MD5). The advantage of this access policy is that Kela can provision new phones with zero administration effort. Similarly printer management has been greatly simplified. Previously they had to be authenticated using MAB with Active Directory group and location information. Now they can be added on a plug-and-play basis using a centralized access policy over 802.1X with EAP-MD5.

“ISE has automated and simplified access control for network devices such as printers, IP phones, and thin-clients and now we have enhanced visibility of our network.”

Ilari Saikkonen,
Senior IT Specialist
Kela

User experience has also improved. “With Cisco Prime we can easily see, for example, the wireless network status, and quickly troubleshoot if users have problems on accessing network services,” Lappalainen says. “ISE and Prime are very good: secure, flexible, and offering greater network visibility. With ISE, we can also apply a posture health check for workstations, to ensure end devices are compliant with our security policy.”

Next Steps

Further benefit is foreseen from implementing new features such as Cisco EnergyWise™ and new products such as Catalyst 2960-X, 3850, and 4500 Series Switches and Cisco Aironet 600 Series OfficeExtend Access Points for remote users. This next phase of network evolution could help boost video collaboration across the organization.

“Internet videos and video calls are common nowadays, and increasing,” Lappalainen says. “This trend brings new demands for the LAN but especially for the wireless LAN. More application visibility and quality of service may be needed. Because of continuous feature development, we see the Cisco solutions as providing good investment protection.”

For More Information

To learn more about the Cisco architectures and solutions featured in this case study go to:

www.cisco.com/go/trustsec

www.cisco.com/go/ise

www.cisco.com/go/wireless

Product List

Wireless

- Cisco Aironet 2600 Series Access Points
- Cisco 5508 Series Wireless Controller

Routing and Switching

- Cisco Catalyst 2960-S Series Switches
- Cisco Catalyst 3750-X Series Switches
- Cisco Catalyst 6509 Series Switches

Security

- Cisco TrustSec
- Cisco Identity Services Engine
- Cisco Prime Infrastructure Manager
- Cisco Mobility Services Engine
- Cisco Wireless Intrusion Prevention System



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)