Microsoft

Citrix NetScaler and Microsoft Intune integrate to provide access to on-premises apps with a secure, seamless experience for end users

Users have one URL and single sign-on across all apps, while IT improves protection of the corporate network

Employees expect the freedom to access their email and documents from anywhere, on any device—and they expect the experience to be seamless and modern. With an integrated solution from Citrix and Microsoft, IT departments can make this a reality and boost employee productivity as a result.

Now more than ever, people are connected

With smartphones, tablets, laptops, and PCs, people have an increasing number of options for getting and staying connected at any time. Today's employees expect the freedom to access their corporate email and documents from anywhere, on any device—and they expect the experience to be seamless and modern. To meet the needs of this highly mobile workforce, IT must work to enable maximum employee productivity, while ensuring that corporate data is secure. One of the core challenges of IT today is making sure that only the right users, under the appropriate conditions, have access to corporate resources—while enabling users to do their best work from anywhere.

IT is looking for a solution that enables them to define access-control and security policies that limit access to corporate data based on not only the user credentials but also the state of the end-user device. And, they need a dynamic policy framework for using multi-factor authentication, to ensure that only trusted and authorized users on policy-compliant devices can access sensitive corporate data.

For an end user looking to access corporate data from any device and location, the solution should offer minimum end-user involvement in setting up and configuring their end user devices; a seamless user experience; and support for any device they are using.

Citrix NetScaler Unified Gateway

Citrix NetScaler Unified Gateway is an SSL VPN–based remote access solution that integrates with industry-leading MDM and MAM solutions to provide an ability to scan the end-user device, authenticate an end user, and create a device-level and/or an application-level VPN tunnel into a datacenter. Using this tunnel, an end user can securely access on-premises resources.

Microsoft Enterprise Mobility + Security (EMS)

Microsoft EMS is a comprehensive mobility solution designed to help manage and protect users, devices, apps, and data in a mobile-first, cloud-first world. EMS gives you the control and protection your business requires, without compromising the familiar mobile and desktop experiences that employees expect.
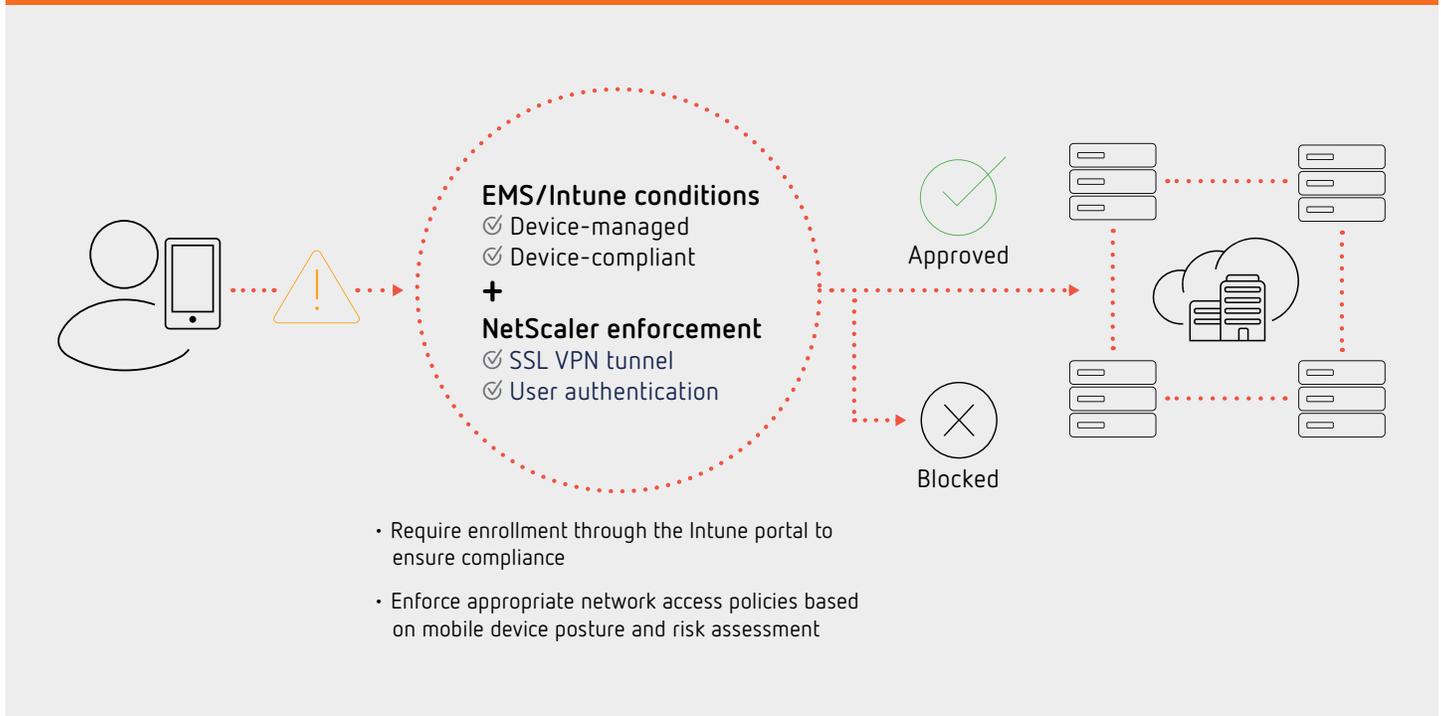
Microsoft EMS and Citrix NetScaler

Today Citrix and EMS have integrated, harnessing the power of Citrix NetScaler and Microsoft Intune to help IT control access to on-premises data and resources, while still enabling people to do their best work from any device.

This integration gives you on-premises conditional access—allowing you to set policies to ensure that only managed and compliant devices can connect to your on-premises corporate network (see Diagram 1).

You can use compliance policy settings in Microsoft Intune to evaluate the compliance of employee devices against a set of rules you create. As a first check, NetScaler Unified Gateway captures the device ID to check if the device is enrolled and compliant with Microsoft Intune. If the end-user device is not enrolled or in compliant status, NetScaler Unified Gateway redirects the user to the Intune enrollment process. An Intune agent will guide the user to complete the enrollment process and maintain the end-user device status with Intune. When the user comes to NetScaler Unified Gateway

---

Diagram 1   Intune and NetScaler provide conditional access to on-premises corporate network

EMS/Intune conditions
☑ Device-managed
☑ Device-compliant

+

NetScaler enforcement
☑ SSL VPN tunnel
☑ User authentication

Approved

Blocked

· Require enrollment through the Intune portal to ensure compliance

· Enforce appropriate network access policies based on mobile device posture and risk assessment

again, device state will be verified before access is granted, thereby enforcing the conditional access policies.

When you combine a device-compliance policy with conditional access, only authorized users will gain access, and only from compliant devices (see Diagram 2).

Key customer benefits of the integration include:

A cost effective solution
While other vendors charge a per-user license fee on top of appliance and softwhere costs, there is no per-user license for creating an SSL VPN tunnel with NetScaler Platinum edition.

Conditional access
The integration provides an added level of security, as IT admins can now define access-control policies for on-premises resources like MS Exchange, SharePoint, or any other application, based on the state of the end-user mobile device. For a mobile device to get access to on-premises resources, it must be enrolled with Microsoft Intune, and it must be compliant.

Improved end-user device security
In addition to conditional access to corporate resources based on Microsoft Intune enrollment, this solution provides policies for additional checks of end-user devices. For a list of policies that can be applied at Microsoft Intune, please check here: compliance policy settings.

Additionally, NetScaler Unified Gateway provides an adaptive multi-factor authentication framework that supports all commonly used authentication options, including digital certificates, smart cards, one-time passwords, and third-party SAML IDP integrations.

A better user experience
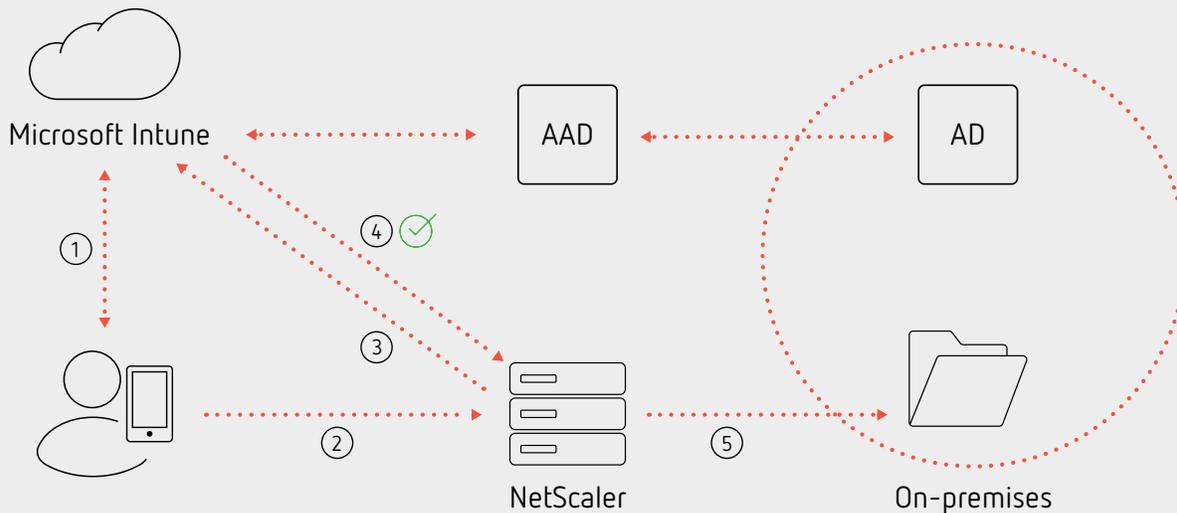Users on compliant devices have easy access to on-premises data and resources.

End-to-end visibility
NetScaler Unified Gateway, with Gateway Insight, provides complete end-to-end visibility and monitoring of any issues related to user access to on-premises applications, allowing faster resolution of these issues.

If you plan on using Microsoft Intune, use NetScaler Unified Gateway for providing user authentication and conditional access to on-premises resources. NetScaler Unified Gateway helps consolidate your remote-access/gateway infrastructure, and provides a single solution for secure access to all applications.

Diagram 2   Intune and NetScaler user-authentication process

1. Device enrollment to Intune
2. User attempts access to on-prem server
3. Gateway checks "conditional access policies"
   -Device ID is used for identification
4. Intune provides device status
   -Enrollment
   -Compliance
5. User receives success/failure response

How to order Microsoft Intune
Visit https://www.microsoft.com/Intune.

How to order NetScaler Unified Gateway
For more information or a free trial, go to
https://www.citrix.com/gateway.